



Junos[®] OS

Attack Detection and Prevention Library for Security Devices

Release
12.1X47-D10



Published: 2014-06-02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] OS Attack Detection and Prevention Library for Security Devices
12.1X47-D10
Copyright © 2014, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xiii
	Documentation and Release Notes	xiii
	Supported Platforms	xiii
	Using the Examples in This Manual	xiii
	Merging a Full Example	xiv
	Merging a Snippet	xiv
	Documentation Conventions	xv
	Documentation Feedback	xvii
	Requesting Technical Support	xvii
	Self-Help Online Tools and Resources	xvii
	Opening a Case with JTAC	xviii
Part 1	Denial-of-Service Attacks Feature Guide for Security Devices	
Chapter 1	Overview	3
	Attack Detection and Prevention	3
	Attack Detection and Prevention Overview	3
	DoS Attack Overview	4
	Understanding Screen Options on the SRX5000 Module Port	
	Concentrator	4
	Statistics-Based Screens	5
	Signature-Based Screens	6
	Firewall DoS Attacks	7
	Firewall DoS Attacks Overview	7
	Understanding Session Table Flood Attacks	7
	Understanding Source-Based Session Limits	8
	Understanding Destination-Based Session Limits	9
	Understanding SYN-ACK-ACK Proxy Flood Attacks	10
	Understanding Firewall Filters on the SRX5000 Module Port	
	Concentrator	10
	Network DoS Attacks	11
	Network DoS Attacks Overview	11
	Understanding SYN Flood Attacks	12
	SYN Flood Protection	13
	SYN Flood Options	15
	Understanding Whitelists for SYN Flood Screens	17
	Understanding SYN Cookie Protection	17
	Understanding ICMP Flood Attacks	19
	Understanding UDP Flood Attacks	20
	Understanding Land Attacks	21

	OS-Specific DoS Attacks	22
	OS-Specific DoS Attacks Overview	22
	Understanding Ping of Death Attacks	23
	Understanding Teardrop Attacks	24
	Understanding WinNuke Attacks	25
Chapter 2	Configuration	27
	Firewall DoS Attacks	27
	Example: Setting Source-Based Session Limits	27
	Example: Setting Destination-Based Session Limits	29
	Example: Protecting Against a SYN-ACK-ACK Proxy Flood Attack	31
	Network DoS Attacks	33
	Example: Configuring Multiple Screening Options	33
	Example: Enabling SYN Flood Protection	38
	Example: Enabling SYN Flood Protection for Webservers in the DMZ	40
	Example: Configuring Whitelists for SYN Flood Screens	46
	Example: Enabling SYN Cookie Protection	48
	Example: Enabling ICMP Flood Protection	50
	Example: Enabling UDP Flood Protection	52
	Example: Protecting Against a Land Attack	54
	OS-Specific DoS Attacks	56
	Example: Protecting Against a Ping of Death Attack	56
	Example: Protecting Against a Teardrop Attack	57
	Example: Protecting Against a WinNuke Attack	58
	Configuration Statements	59
	[edit security screen] Hierarchy Level	60
	attack-threshold	62
	description (Security Screen)	63
	destination-ip-based	64
	destination-threshold	65
	fin-no-ack	66
	flood (Security ICMP)	67
	flood (Security UDP)	68
	icmp (Security Screen)	69
	ids-option	70
	ip (Security Screen)	73
	ip-sweep	75
	land	76
	limit-session	76
	ping-death	77
	port-scan	78
	screen (Security Zones)	79
	source-ip-based	79
	source-threshold	80
	syn-ack-ack-proxy	81
	syn-check-required	81
	syn-fin	82
	syn-flood	83
	syn-flood-protection-mode	84

	syn-frag	84
	tcp (Security Screen)	85
	tcp-no-flag	86
	tcp-sweep	87
	timeout (Security Screen)	88
	traceoptions (Security Screen)	89
	udp (Security Screen)	91
	udp-sweep	92
	white-list	93
	winnuke	94
Chapter 3	Administration	95
	Operational Commands	95
	clear security screen statistics	96
	clear security screen statistics interface	97
	clear security screen statistics zone	99
	show security screen ids-option	101
	show security screen statistics	106
Part 2	Reconnaissance Deterrence Feature Guide for Security Devices	
Chapter 4	Overview	117
	Attack Detection and Prevention	117
	Attack Detection and Prevention Overview	117
	IP Address and Port Options	118
	Reconnaissance Deterrence Overview	118
	Understanding IP Address Sweeps	118
	Understanding TCP Port Scanning	119
	Understanding UDP Port Scanning	120
	Understanding Network Reconnaissance Using IP Options	121
	Uses for IP Packet Header Options	122
	Screen Options for Detecting IP Options Used for Reconnaissance	124
	Understanding Domain Name System Resolve	124
	System Probes and Flag Set	125
	Reconnaissance Deterrence Overview	125
	Understanding Operating System Probes	125
	Understanding TCP Headers with SYN and FIN Flags Set	126
	Understanding TCP Headers With FIN Flag Set and Without ACK Flag Set	126
	Understanding TCP Header with No Flags Set	127
	Attacker Evasion Techniques	128
	Reconnaissance Deterrence Overview	128
	Understanding Attacker Evasion Techniques	129
	Understanding FIN Scans	129
	Understanding TCP SYN Checking	129
	Understanding IP Spoofing	131
	Understanding IP Spoofing in Layer 2 Transparent Mode	132
	Understanding IP Source Route Options	133

Chapter 5	Configuration	137
	IP Address and Port Options	137
	Example: Blocking IP Address Sweeps	137
	Example: Blocking Port Scans	139
	Example: Detecting Packets That Use IP Screen Options for Reconnaissance	141
	Operating System Probes	143
	Example: Blocking Packets with SYN and FIN Flags Set	144
	Example: Blocking Packets With FIN Flag Set and Without ACK Flag Set	145
	Example: Blocking Packets with No Flags Set	147
	Attacker Evasion Techniques	148
	Thwarting a FIN Scan (CLI Procedure)	149
	Setting TCP SYN Checking (CLI Procedure)	149
	Setting Strict SYN Checking (CLI Procedure)	149
	Configuring IP Spoofing in Layer 2 Transparent Mode	150
	Example: Blocking IP Spoofing	151
	Example: Blocking Packets with Either a Loose or a Strict Source Route Option Set	152
	Example: Detecting Packets with Either a Loose or a Strict Source Route Option Set	154
	Configuration Statements	156
	[edit security screen] Hierarchy Level	157
	attack-threshold	160
	description (Security Screen)	161
	destination-ip-based	162
	destination-threshold	163
	fin-no-ack	164
	flood (Security ICMP)	165
	flood (Security UDP)	166
	icmp (Security Screen)	167
	ids-option	168
	ip (Security Screen)	171
	ip-sweep	173
	land	174
	large	174
	limit-session	175
	no-syn-check	175
	no-syn-check-in-tunnel	176
	ping-death	176
	port-scan	177
	screen (Security Zones)	178
	source-ip-based	178
	source-threshold	179
	strict-syn-check	179
	syn-ack-ack-proxy	180
	syn-check-required	180
	syn-fin	181
	syn-flood	182
	syn-flood-protection-mode	183

	syn-frag	183
	tcp (Security Screen)	184
	tcp-no-flag	185
	tcp-sweep	186
	timeout (Security Screen)	187
	traceoptions (Security Screen)	188
	udp (Security Screen)	190
	udp-sweep	191
	white-list	192
	winnuke	193
Chapter 6	Administration	195
	Operational Commands	195
	clear security screen statistics	196
	clear security screen statistics interface	197
	clear security screen statistics zone	199
	show security screen ids-option	201
	show security screen statistics	206
Part 3	Suspicious Packet Attributes Feature Guide for Security Devices	
Chapter 7	Overview	217
	Attack Detection and Prevention	217
	Attack Detection and Prevention Overview	217
	ICMP and SYN Fragment Protection	218
	Suspicious Packet Attributes Overview	218
	Understanding ICMP Fragment Protection	218
	Understanding Large ICMP Packet Protection	219
	Understanding SYN Fragment Protection	220
	IP Protection	221
	Suspicious Packet Attributes Overview	222
	Understanding Bad IP Option Protection	222
	Understanding Unknown Protocol Protection	223
	Understanding IP Packet Fragment Protection	224
Chapter 8	Configuration	227
	ICMP and SYN Fragment Protection	227
	Example: Blocking Fragmented ICMP Packets	227
	Example: Blocking Large ICMP Packets	228
	Example: Dropping IP Packets Containing SYN Fragments	229
	IP Protection	230
	Example: Blocking IP Packets with Incorrectly Formatted Options	230
	Example: Dropping Packets Using an Unknown Protocol	231
	Example: Dropping Fragmented IP Packets	231
	Configuration Statements	232
	[edit security screen] Hierarchy Level	233
	attack-threshold	236
	description (Security Screen)	237
	destination-ip-based	238
	destination-threshold	239

	fin-no-ack	240
	flood (Security ICMP)	241
	flood (Security UDP)	242
	icmp	243
	icmp (Security Screen)	243
	ids-option	244
	ip (Security Screen)	247
	ip-sweep	249
	land	250
	limit-session	250
	ping-death	251
	port-scan	252
	screen (Security Zones)	253
	source-ip-based	253
	source-threshold	254
	syn-ack-ack-proxy	255
	syn-check-required	255
	syn-fin	256
	syn-flood	257
	syn-flood-protection-mode	258
	syn-frag	258
	tcp (Security Screen)	259
	tcp-no-flag	260
	tcp-sweep	261
	timeout (Security Screen)	262
	traceoptions (Security Screen)	263
	udp (Security Screen)	265
	udp-sweep	266
	white-list	267
	winnuke	268
Chapter 9	Administration	269
	Operational Commands	269
	clear security screen statistics	270
	clear security screen statistics interface	271
	clear security screen statistics zone	273
	show security screen ids-option	275
	show security screen statistics	280
Part 4	Index	291

List of Figures

Part 1	Denial-of-Service Attacks Feature Guide for Security Devices
Chapter 1	Overview 3
	Figure 1: Limiting Sessions Based on Source IP Address 8
	Figure 2: Distributed DOS Attack 9
	Figure 3: SYN Flood Attack 13
	Figure 4: Proxying SYN Segments 14
	Figure 5: Rejecting New SYN Segments 15
	Figure 6: Establishing a Connection with SYN Cookie Active 18
	Figure 7: ICMP Flooding 19
	Figure 8: UDP Flooding 21
	Figure 9: Land Attack 22
	Figure 10: Ping of Death 23
	Figure 11: Teardrop Attacks 24
	Figure 12: Fragment Discrepancy 25
	Figure 13: WinNuke Attack Indicators 26
Chapter 2	Configuration 27
	Figure 14: Device-Level SYN Flood Protection 41
Part 2	Reconnaissance Deterrence Feature Guide for Security Devices
Chapter 4	Overview 117
	Figure 15: Address Sweep 119
	Figure 16: Port Scan 120
	Figure 17: UDP Port Scan 121
	Figure 18: Routing Options 122
	Figure 19: TCP Header with SYN and FIN Flags Set 126
	Figure 20: TCP Header with FIN Flag Set 127
	Figure 21: TCP Header with No Flags Set 128
	Figure 22: SYN Flag Checking 130
	Figure 23: IP Source Routing 134
	Figure 24: Loose IP Source Route Option for Deception 134
Part 3	Suspicious Packet Attributes Feature Guide for Security Devices
Chapter 7	Overview 217
	Figure 25: Blocking ICMP Fragments 219
	Figure 26: Blocking Large ICMP Packets 220
	Figure 27: SYN Fragments 221
	Figure 28: Incorrectly Formatted IP Options 223
	Figure 29: Unknown Protocols 224

Figure 30: IP Packet Fragments	225
Figure 31: IPv6 Packet	225
Figure 32: Fragment Extension Header	225

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xv
	Table 2: Text and Syntax Conventions	xv
Part 1	Denial-of-Service Attacks Feature Guide for Security Devices	
Chapter 2	Configuration	27
	Table 3: SYN Flood Protection Parameters	42
Chapter 3	Administration	95
	Table 4: show security screen ids-option Output Fields	101
	Table 5: show security screen statistics Output Fields	107
Part 2	Reconnaissance Deterrence Feature Guide for Security Devices	
Chapter 4	Overview	117
	Table 6: IP Options and Attributes	122
Chapter 6	Administration	195
	Table 7: show security screen ids-option Output Fields	201
	Table 8: show security screen statistics Output Fields	207
Part 3	Suspicious Packet Attributes Feature Guide for Security Devices	
Chapter 9	Administration	269
	Table 9: show security screen ids-option Output Fields	275
	Table 10: show security screen statistics Output Fields	281

About the Documentation

- Documentation and Release Notes on page xiii
- Supported Platforms on page xiii
- Using the Examples in This Manual on page xiii
- Documentation Conventions on page xv
- Documentation Feedback on page xvii
- Requesting Technical Support on page xvii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- [LN Series](#)
- [SRX Series](#)

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xv defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Denial-of-Service Attacks Feature Guide for Security Devices

- [Overview on page 3](#)
- [Configuration on page 27](#)
- [Administration on page 95](#)

CHAPTER 1

Overview

- [Attack Detection and Prevention on page 3](#)
- [Firewall DoS Attacks on page 7](#)
- [Network DoS Attacks on page 11](#)
- [OS-Specific DoS Attacks on page 22](#)

Attack Detection and Prevention

- [Attack Detection and Prevention Overview on page 3](#)
- [DoS Attack Overview on page 4](#)
- [Understanding Screen Options on the SRX5000 Module Port Concentrator on page 4](#)

Attack Detection and Prevention Overview

Supported Platforms [LN Series, SRX Series](#)

The Juniper Networks Intrusion Detection and Prevention (IDP) feature, also known as a *stateful firewall*, detects and prevents attacks in network traffic.

An exploit can be either an information-gathering probe or an attack to compromise, disable, or harm a network or network resource. In some cases, the distinction between the two objectives of an exploit can be unclear. For example, a barrage of TCP SYN segments might be an IP address sweep with the intent of triggering responses from active hosts, or it might be a SYN flood attack with the intent of overwhelming a network so that it can no longer function properly. Furthermore, because an attacker usually precedes an attack by performing reconnaissance on the target, we can consider information-gathering efforts as a precursor to an impending attack—that is, they constitute the first stage of an attack. Thus, the term *exploit* encompasses both reconnaissance and attack activities, and the distinction between the two is not always clear.

Juniper Networks provides various detection and defense mechanisms at the zone and policy levels to combat exploits at all stages of their execution:

- Screen options at the zone level.
- Firewall policies at the inter-, intra-, and super-zone policy levels (*super-zone* here means in global policies, where no security zones are referenced).

To secure all connection attempts, Junos OS uses a dynamic packet-filtering method known as stateful inspection. Using this method, Junos OS identifies various components in the IP packet and TCP segment headers—source and destination IP addresses, source and destination port numbers, and packet sequence numbers—and maintains the state of each TCP session and pseudo UDP session traversing the firewall. (Junos OS also modifies session states based on changing elements such as dynamic port changes or session termination.) When a responding TCP packet arrives, Junos OS compares the information reported in its header with the state of its associated session stored in the inspection table. If they match, the responding packet is allowed to pass the firewall. If the two do not match, the packet is dropped.

Junos OS screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone. Junos OS then applies firewall policies, which can contain content filtering and IDP components, to the traffic that passes the screen filters.

**Related
Documentation**

- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

DoS Attack Overview

Supported Platforms [LN Series, SRX Series](#)

The intent of a denial-of-service (DoS) attack is to overwhelm the targeted victim with a tremendous amount of bogus traffic so that the victim becomes so preoccupied processing the bogus traffic that legitimate traffic cannot be processed. The target can be the firewall, the network resources to which the firewall controls access, or the specific hardware platform or operating system of an individual host.

If a DoS attack originates from multiple source addresses, it is known as a distributed denial-of-service (DDoS) attack. Typically, the source address of a DoS attack is spoofed. The source addresses in a DDoS attack might be spoofed, or the actual addresses of compromised hosts might be used as “zombie agents” to launch the attack.

The device can defend itself and the resources it protects from DoS and DDoS attacks.

**Related
Documentation**

- [Firewall DoS Attacks Overview on page 7](#)
- [Network DoS Attacks Overview on page 11](#)
- [OS-Specific DoS Attacks Overview on page 22](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Understanding Screen Options on the SRX5000 Module Port Concentrator

Supported Platforms [SRX5600, SRX5800](#)

The SRX5000 Module Port Concentrator (SRX5K-MPC) for the SRX5600 and SRX5800 supports screen options. Junos OS screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone.

Using screen options, your security device can protect against different internal and external attacks, including SYN flood attacks, UDP flood attacks, and port scan attacks. The Junos OS applies screen checks to traffic prior to the security policy processing, thereby resulting in less resource utilization.

The screen options are divided into the following two categories:

- Statistics-based screens
- Signature-based screens

Statistics-Based Screens

All screen features implemented on an SRX5K-MPC are independent of Layer 2 or Layer 3 mode. The flood protections are used to defend against SYN flood attacks, session table flood attacks, firewall denial-of-service (DoS) attacks, and network DoS attacks.

The following four types of threshold-based flood protection are performed on each processor for both IPv4 and IPv6:

- UDP-based flood protection
- ICMP-based flood protection
- TCP source-based SYN flood protection
- TCP destination-based SYN flood protection



NOTE: If one of the two TCP SYN flood protections is configured on a zone, the second TCP SYN flood protection is automatically enabled on the same zone. These two protections always work together.

Each flood protection is threshold-based, and the threshold is calculated per zone on each microprocessor. If the flood is detected on a microprocessor chip, that particular microprocessor takes action against the offending packets based on the configuration:

- Default action (report and drop)—Screen logging and reporting are done on an SPU, so offending packets need to be forwarded to the central point or SPU for this purpose. To protect SPUs from flooding, only the first offending packet for each screen in a zone is sent to the SPU for logging and reporting in each second. The rest of the offending packets are counted and dropped in a microprocessor.

For example, assume UDP flooding is configured at a logical interface with a threshold set to 5000 packets per second. If UDP packets come in at the rate of 20,000 per second, then about 5000 UDP packets are forwarded to the central point or SPU each second and the remaining packets are detected as flooding. However, only one UDP flooding packet is sent to the SPU for logging and reporting in each second. The remaining packets are dropped in the microprocessor.

- Alarm only (alarm-without-drop)—An offending packet detected by screen protection is not dropped. It skips the rest of the screen checks and is forwarded to the central

point or SPU with the screen result copied to its meta-header. It is not counted as a dropped packet.

Signature-Based Screens

The SRX5K-MPC provides signature-based screen options along with sanity checks on the received packet.

Sometimes packets received by the device are malformed or invalid, and they might cause damage to the device and network. These packets must be dropped during initial stages of processing.

For both signature-based screen options and sanity checks, the packet contents including packet header, status and control bits, and extension headers (for IPv6) are examined. You can configure the screens as per your requirements, whereas packet sanity checks are performed by default.

The packet sanity checks and screen options are performed on packets received on ingress interfaces.

The processor does sanity checks and runs some screen features to detect the malformed and malicious ingress packets received from physical interfaces. A specific action is performed on both IPv4 and IPv6 packets if not specified. Packets that fail a sanity check are counted and dropped.

The following packet sanity checks are supported:

- IPv4 sanity check
- IPv6 sanity check

The following screen features are supported:

- IP-based screen
- UDP-based screen
- TCP-based screen
- ICMP-based screen

The screen features are applicable to both IPv4 and IPv6 packets, with the exception of IP options screens, which only apply to IPv4 packets. If a packet is detected by one screen option, it skips the rest of the screen checks and is forwarded to the central point or Services Processing Unit (SPU) for logging and statistics collection.

Related Documentation

- [Attack Detection and Prevention Overview on page 3](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

Firewall DoS Attacks

- [Firewall DoS Attacks Overview on page 7](#)
- [Understanding Session Table Flood Attacks on page 7](#)
- [Understanding Source-Based Session Limits on page 8](#)
- [Understanding Destination-Based Session Limits on page 9](#)
- [Understanding SYN-ACK-ACK Proxy Flood Attacks on page 10](#)
- [Understanding Firewall Filters on the SRX5000 Module Port Concentrator on page 10](#)

Firewall DoS Attacks Overview

Supported Platforms [LN Series](#), [SRX Series](#)

The intent of a denial-of-service (DoS) attack is to overwhelm the targeted victim with a tremendous amount of bogus traffic so that the victim becomes so preoccupied processing the bogus traffic that legitimate traffic cannot be processed.

If attackers discover the presence of the Juniper Networks firewall, they might launch a DoS attack against it instead of the network behind it. A successful DoS attack against a firewall amounts to a successful DoS attack against the protected network in that it thwarts attempts of legitimate traffic to traverse the firewall.

An attacker might use session table floods and SYN-ACK-ACK proxy floods to fill up the session table of Junos OS and thereby produce a DoS.

Related Documentation

- [DoS Attack Overview on page 4](#)
- [Network DoS Attacks Overview on page 11](#)
- [OS-Specific DoS Attacks Overview on page 22](#)
- [Understanding Session Table Flood Attacks on page 7](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Understanding Session Table Flood Attacks

Supported Platforms [LN Series](#), [SRX Series](#)

A successful DoS attack overwhelms its victim with such a massive barrage of false simulated traffic that it becomes unable to process legitimate connection requests. DoS attacks can take many forms—SYN flood, SYN-ACK-ACK flood, UDP flood, ICMP flood, and so on—but they all seek the same objective, which is to fill up their victim's session table.

When the session table is full, that host cannot create any new sessions and begins rejecting new connection requests. The source-based session limits screen option and the destination-based session limit screen option help mitigate such attacks.

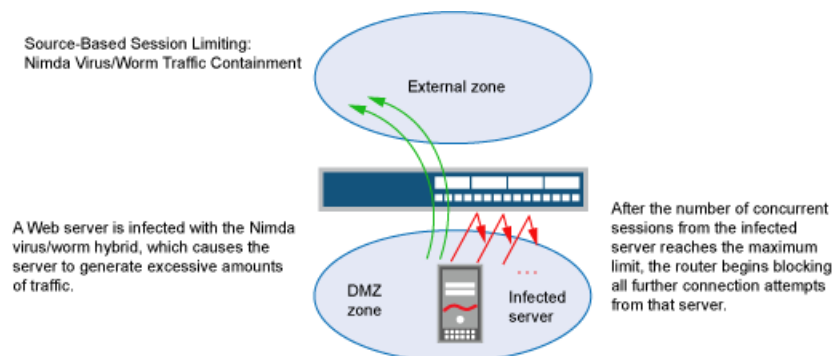
- Related Documentation**
- [DoS Attack Overview on page 4](#)
 - [Understanding Source-Based Session Limits on page 8](#)
 - [Understanding SYN Flood Attacks on page 12](#)
 - [Understanding SYN-ACK-ACK Proxy Flood Attacks on page 10](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Understanding Source-Based Session Limits

Supported Platforms [LN Series](#), [SRX Series](#)

In addition to limiting the number of concurrent sessions from the same source IP address, you can also limit the number of concurrent sessions to the same destination IP address. One benefit of setting a source-based session limit is that it can stem an attack such as the Nimda virus (which is actually both a virus and a worm) that infects a server and then begins generating massive amounts of traffic from that server. Because all the virus-generated traffic originates from the same IP address, a source-based session limit ensures that the firewall can curb such excessive amounts of traffic. See [Figure 1 on page 8](#).

Figure 1: Limiting Sessions Based on Source IP Address



Another benefit of source-based session limiting is that it can mitigate attempts to fill up the firewall's session table if all the connection attempts originate from the same source IP address.

Determining what constitutes an acceptable number of connection requests requires a period of observation and analysis to establish a baseline for typical traffic flows. You also need to consider the maximum number of concurrent sessions required to fill up the session table of the particular Juniper Networks platform you are using. To see the maximum number of sessions that your session table supports, use the CLI command **show security flow session summary**, and then look at the last line in the output, which lists the number of current (allocated) sessions, the maximum number of sessions, and the number of failed session allocations:

```
Maximum-sessions: 32768
```

The default maximum for source-based session limits is 128 concurrent sessions, a value that might need adjustment to suit the needs of your network environment and the platform.



NOTE: Junos OS supports source-based session limits for both IPv4 and IPv6 traffic.

Related Documentation

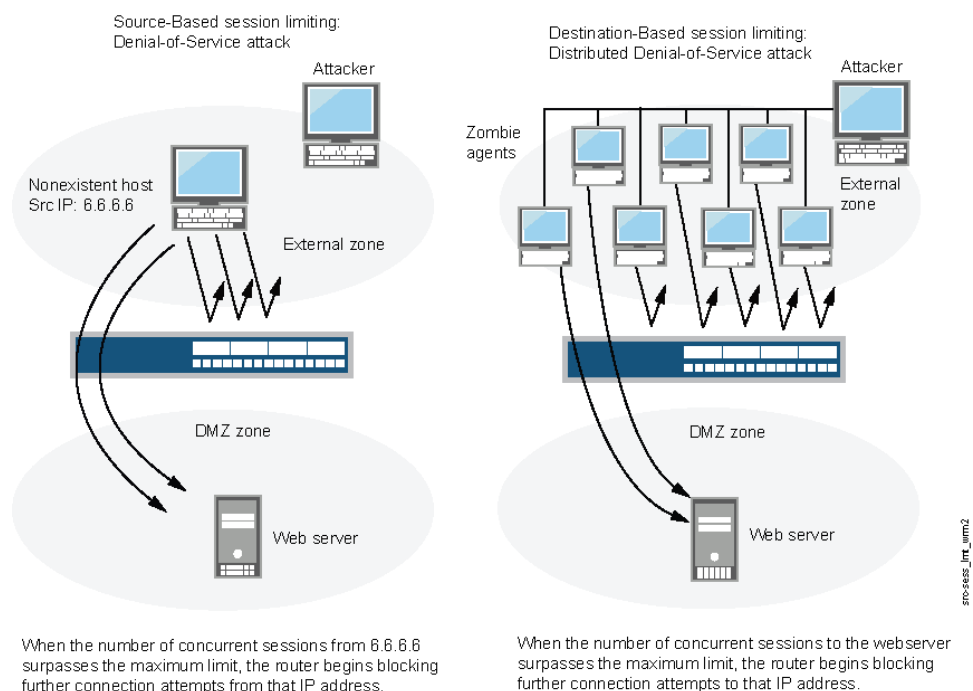
- [DoS Attack Overview on page 4](#)
- [Example: Setting Source-Based Session Limits on page 27](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Understanding Destination-Based Session Limits

Supported Platforms [LN Series](#), [SRX Series](#)

In addition to limiting the number of concurrent sessions from the same source IP address, you can also limit the number of concurrent sessions to the same destination IP address. A wily attacker can launch a distributed denial-of-service (DDoS) attack. In a DDoS attack, the malicious traffic can come from hundreds of hosts, known as “zombie agents,” that are surreptitiously under the control of an attacker. In addition to the SYN, UDP, and ICMP flood detection and prevention screen options, setting a destination-based session limit can ensure that Junos OS allows only an acceptable number of concurrent connection requests—no matter what the source—to reach any one host. See [Figure 2 on page 9](#).

Figure 2: Distributed DOS Attack



The default maximum for destination-based session limits is 128 concurrent sessions, a value that might need adjustment to suit the needs of your network environment and the platform.

**Related
Documentation**

- [DoS Attack Overview on page 4](#)
- [Example: Setting Destination-Based Session Limits on page 29](#)
- [Understanding Source-Based Session Limits on page 8](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Understanding SYN-ACK-ACK Proxy Flood Attacks

Supported Platforms [LN Series, SRX Series](#)

When an authentication user initiates a Telnet or an FTP connection, the user sends a SYN segment to the Telnet or FTP server. Junos OS intercepts the SYN segment, creates an entry in its session table, and proxies a SYN-ACK segment to the user. The user then replies with an ACK segment. At this point, the initial three-way handshake is complete. Junos OS sends a login prompt to the user. If the user, with malicious intent, does not log in but instead continues initiating SYN-ACK-ACK sessions, the firewall session table can fill up to the point where the device begins rejecting legitimate connection requests.

To prevent such an attack, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, Junos OS rejects further connection requests from that IP address. By default, the threshold is 512 connections from any single IP address. You can change this threshold (to any number between 1 and 250,000) to better suit the requirements of your network environment.



NOTE: Junos OS supports SYN-ACK-ACK proxy protection for both IPv4 and IPv6 addresses.

**Related
Documentation**

- [DoS Attack Overview on page 4](#)
- [Example: Protecting Against a SYN-ACK-ACK Proxy Flood Attack on page 31](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Understanding Firewall Filters on the SRX5000 Module Port Concentrator

Supported Platforms [SRX5600, SRX5800](#)

The SRX5000 Module Port Concentrator (SRX5K-MPC) for the SRX5600 and SRX5800 supports firewall filter to provide filter based forwarding and packet filtering at logical interfaces including the chassis loopback interface. A firewall filter is used to secure networks, to protect Routing Engines and Packet Forwarding Engines, and to ensure class of service (CoS).

The firewall filter provides:

- Filter-based forwarding at logical interfaces
- Protection of a Routing Engine from DoS attacks
- Blocking of certain types of packets to reach a Routing Engine and packet counter

The firewall filter examines packets and performs actions according to the configured filter policy. The policy is composed of match conditions and actions. The match conditions cover various fields of Layer 3 packet and Layer 4 header information. In association with the match conditions, various actions are defined in the firewall filter policy, and these actions include **accept**, **discard**, **log** counter, and so on.

After configuring the firewall filter, you can apply a logical interface to the firewall filter in the ingress or egress, or in both directions. All packets passing through the logical interface are checked by the firewall filter. As part of the firewall filter configuration, a policer is defined and applied to the logical interface. A policer restricts the traffic bandwidth at the logical interface.



NOTE: Firewall filtering on an SRX5K-MPC does not support aggregated Ethernet interfaces.



NOTE: On SRX5600 and SRX5800 devices with an SRX5K-MPC, applying a policer at the loopback (lo0) interface helps ensure that the Packet Forwarding Engine discards fewer packets being sent to the Routing Engine.

Related Documentation

- [Firewall DoS Attacks Overview on page 7](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

Network DoS Attacks

- [Network DoS Attacks Overview on page 11](#)
- [Understanding SYN Flood Attacks on page 12](#)
- [Understanding Whitelists for SYN Flood Screens on page 17](#)
- [Understanding SYN Cookie Protection on page 17](#)
- [Understanding ICMP Flood Attacks on page 19](#)
- [Understanding UDP Flood Attacks on page 20](#)
- [Understanding Land Attacks on page 21](#)

Network DoS Attacks Overview

Supported Platforms [LN Series, SRX Series](#)

A denial-of-service (DoS) attack directed against one or more network resources floods the target with an overwhelming number of SYN, ICMP, or UDP packets or with an overwhelming number of SYN fragments.

Depending on the attackers' purpose and the extent and success of previous intelligence gathering efforts, the attackers might single out a specific host, such as a device or server or they might aim at random hosts across the targeted network. Either approach has the potential of upsetting service to a single host or to the entire network, depending on how critical the role of the victim is to the rest of the network.

**Related
Documentation**

- [DoS Attack Overview on page 4](#)
- [Firewall DoS Attacks Overview on page 7](#)
- [OS-Specific DoS Attacks Overview on page 22](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

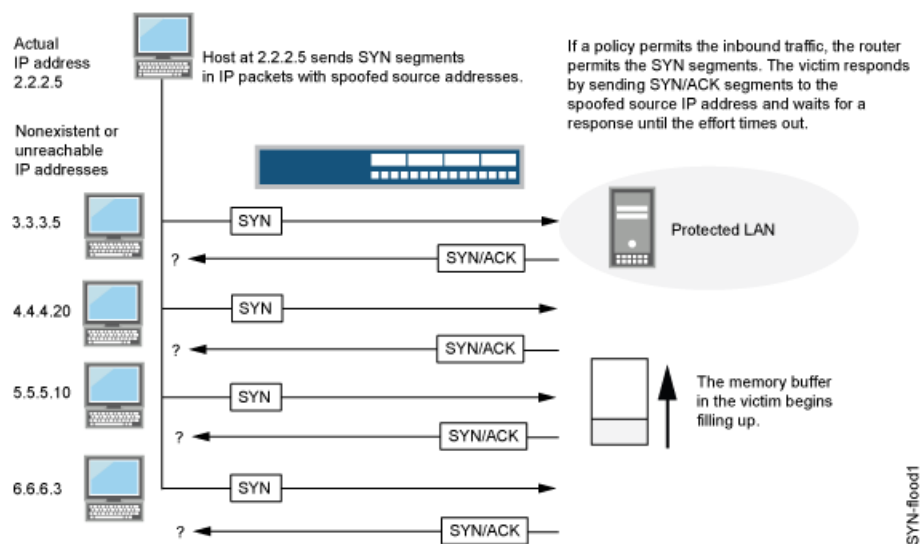
Understanding SYN Flood Attacks

Supported Platforms [LN Series](#), [SRX Series](#)

A SYN flood occurs when a host becomes so overwhelmed by SYN segments initiating incomplete connection requests that it can no longer process legitimate connection requests.

Two hosts establish a TCP connection with a triple exchange of packets known as a *three-way handshake*: A sends a SYN segment to B; B responds with a SYN/ACK segment; and A responds with an ACK segment. A SYN flood attack inundates a site with SYN segments containing forged (spoofed) IP source addresses with nonexistent or unreachable addresses. B responds with SYN/ACK segments to these addresses and then waits for responding ACK segments. Because the SYN/ACK segments are sent to nonexistent or unreachable IP addresses, they never elicit responses and eventually time out. See [Figure 3 on page 13](#).

Figure 3: SYN Flood Attack



By flooding a host with incomplete TCP connections, the attacker eventually fills the memory buffer of the victim. Once this buffer is full, the host can no longer process new TCP connection requests. The flood might even damage the victim's operating system. Either way, the attack disables the victim and its normal operations.

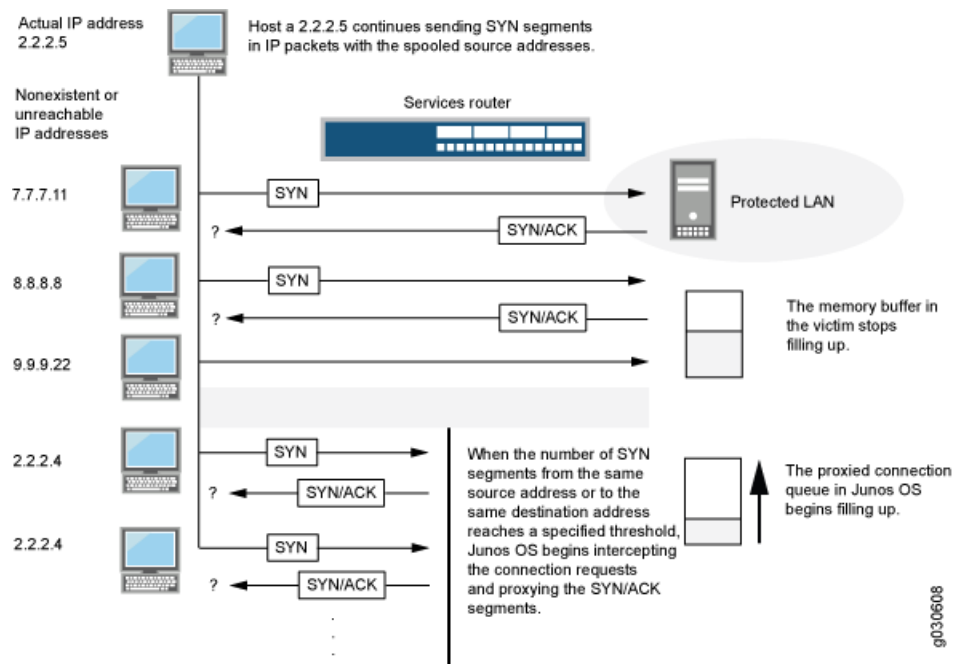
This topic includes the following sections:

- [SYN Flood Protection on page 13](#)
- [SYN Flood Options on page 15](#)

SYN Flood Protection

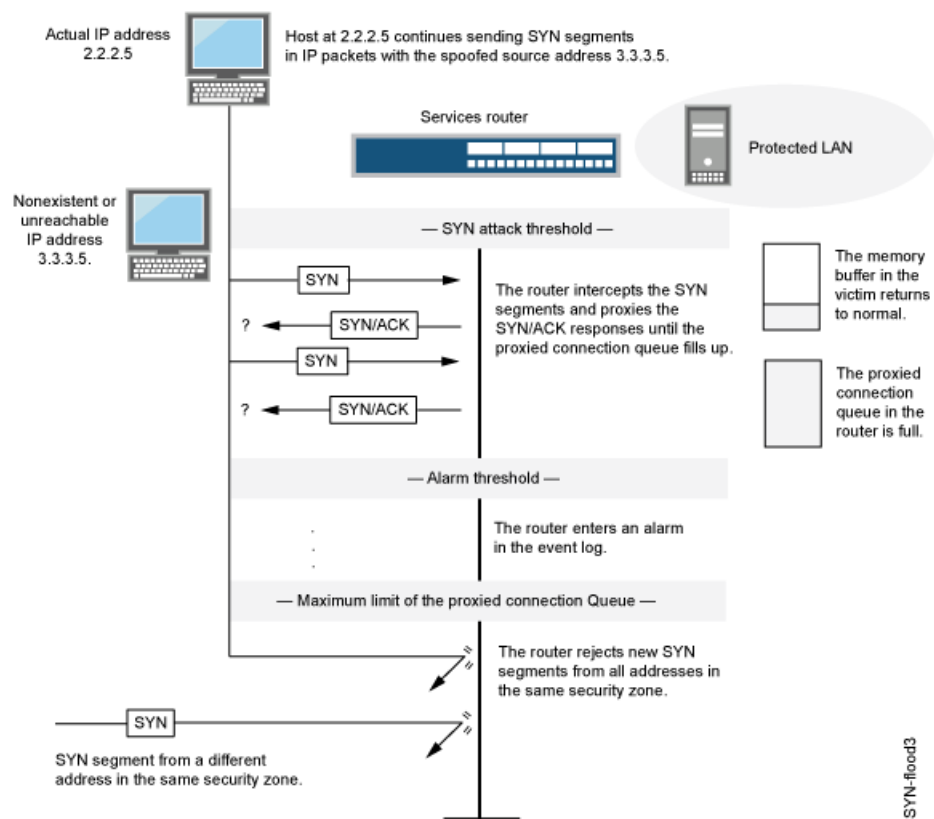
Junos OS can impose a limit on the number of SYN segments permitted to pass through the firewall per second. You can base the attack threshold on the destination address and ingress interface port, the destination address only, or the source address only. When the number of SYN segments per second exceeds one of these thresholds, Junos OS starts proxying incoming SYN segments, replying with SYN/ACK segments and storing the incomplete connection requests in a connection queue. The incomplete connection requests remain in the queue until the connection is completed or the request times out. In [Figure 4 on page 14](#), the SYN attack threshold has passed, and Junos OS has started proxying SYN segments.

Figure 4: Proxying SYN Segments



In [Figure 5 on page 15](#), the proxied connection queue has completely filled up, and Junos OS is rejecting new incoming SYN segments. This action shields hosts on the protected network from the bombardment of incomplete three-way handshakes.

Figure 5: Rejecting New SYN Segments



The device starts receiving new SYN packets when the proxy queue drops below the maximum limit.



NOTE: The procedure of proxying incomplete SYN connections above a set threshold pertains only to traffic permitted by existing policies. Any traffic for which a policy does not exist is automatically dropped.

SYN Flood Options

You can set the following parameters for proxying uncompleted TCP connection requests:

- **Attack Threshold**—This option allows you to set the number of SYN segments (that is, TCP segments with the SYN flag set) to the same destination address per second required to activate the SYN proxying mechanism. Although you can set the threshold to any number, you need to know the normal traffic patterns at your site to set an appropriate threshold for it. For example, if it is an e-business site that normally gets 20,000 SYN segments per second, you might want to set the threshold to 30,000 per second. If a smaller site normally gets 20 SYN segments per second, you might consider setting the threshold to 40.
- **Alarm Threshold**—This option allows you to set the number of proxied, half-complete TCP connection requests per second after which Junos OS enters an alarm in the event

log. The value you set for an alarm threshold triggers an alarm when the number of proxied, half-completed connection requests to the same destination address per second exceeds that value. For example, if you set the SYN attack threshold at 2000 SYN segments per second and the alarm at 1000, then a total of 3000 SYN segments to the same destination address per second is required to trigger an alarm entry in the log.

For each SYN segment to the same destination address in excess of the alarm threshold, the attack detection module generates a message. At the end of the second, the logging module compresses all similar messages into a single log entry that indicates how many SYN segments to the same destination address and port number arrived after exceeding the alarm threshold. If the attack persists beyond the first second, the event log enters an alarm every second until the attack stops.

- **Source Threshold**—This option allows you to specify the number of SYN segments received per second from a single source IP address—regardless of the destination IP address—before Junos OS begins dropping connection requests from that source.

Tracking a SYN flood by source address uses different detection parameters from tracking a SYN flood by destination address. When you set a SYN attack threshold and a source threshold, you put both the basic SYN flood protection mechanism and the source-based SYN flood tracking mechanism in effect.

- **Destination Threshold**—This option allows you to specify the number of SYN segments received per second for a single destination IP address before Junos OS begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based on destination IP address only—regardless of the destination port number.

When you set a SYN attack threshold and a destination threshold, you put both the basic SYN flood protection mechanism and the destination-based SYN flood tracking mechanism in effect.

Consider a case where Junos OS has policies permitting FTP requests and HTTP requests to the same IP address. If the SYN flood attack threshold is 1000 packets per second (pps) and an attacker sends 999 FTP packets and 999 HTTP pps, Junos OS treats both FTP and HTTP packets with the same destination address as members of a single set and rejects the 1001st packet—FTP or HTTP—to that destination.

- **Timeout**—This option allows you to set the maximum length of time before a half-completed connection is dropped from the queue. The default is 20 seconds, and you can set the timeout from 0–50 seconds. You might try decreasing the timeout value to a shorter length until you begin to see any dropped connections during normal traffic conditions. Twenty seconds is a very conservative timeout for a three-way handshake ACK response.



NOTE: Junos OS supports SYN flood protection for both IPv4 and IPv6 traffic.

**Related
Documentation**

- [Example: Enabling SYN Flood Protection on page 38](#)
- [Configuring SYN Flood Protection Options \(CLI Procedure\)](#)

- [Example: Enabling SYN Flood Protection for Webservers in the DMZ on page 40](#)
- [Understanding Whitelists for SYN Flood Screens on page 17](#)
- [Example: Configuring Whitelists for SYN Flood Screens on page 46](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

Understanding Whitelists for SYN Flood Screens

Supported Platforms [LN Series](#), [SRX Series](#)

Junos OS provides the administrative option to configure a whitelist of trusted IP addresses to which the SYN flood screen will not reply with a SYN/ACK. Instead, the SYN packets from the source addresses or to the destination addresses in the list are allowed to bypass the SYN cookie and SYN proxy mechanisms. This feature is needed when you have a service in your network that cannot tolerate proxied SYN/ACK replies under any condition, including a SYN flood event.

Both IP version 4 (IPv4) and IP version 6 (IPv6) whitelists are supported. Addresses in a whitelist should be all IPv4 or all IPv6. In each whitelist, there can be up to 32 IP address prefixes. You can specify multiple addresses or address prefixes as a sequence of addresses separated by spaces and enclosed in square brackets.

- Related Documentation**
- [Understanding SYN Flood Attacks on page 12](#)
 - [Example: Enabling SYN Flood Protection on page 38](#)
 - [Example: Configuring Whitelists for SYN Flood Screens on page 46](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Understanding SYN Cookie Protection

Supported Platforms [LN Series](#), [SRX Series](#)

SYN cookie is a stateless SYN proxy mechanism you can use in conjunction with other defenses against a SYN flood attack.

As with traditional SYN proxying, SYN cookie is activated when the SYN flood attack threshold is exceeded. However, because SYN cookie is stateless, it does not set up a session or policy and route lookups upon receipt of a SYN segment, and it maintains no connection request queues. This dramatically reduces CPU and memory usage and is the primary advantage of using SYN cookie over the traditional SYN proxying mechanism.

When SYN cookie is enabled on Junos OS and becomes the TCP-negotiating proxy for the destination server, it replies to each incoming SYN segment with a SYN/ACK containing an encrypted cookie as its initial sequence number (ISN). The cookie is an MD5 hash of the original source address and port number, destination address and port number, and ISN from the original SYN packet. After sending the cookie, Junos OS drops the original SYN packet and deletes the calculated cookie from memory. If there is no

response to the packet containing the cookie, the attack is noted as an active SYN attack and is effectively stopped.

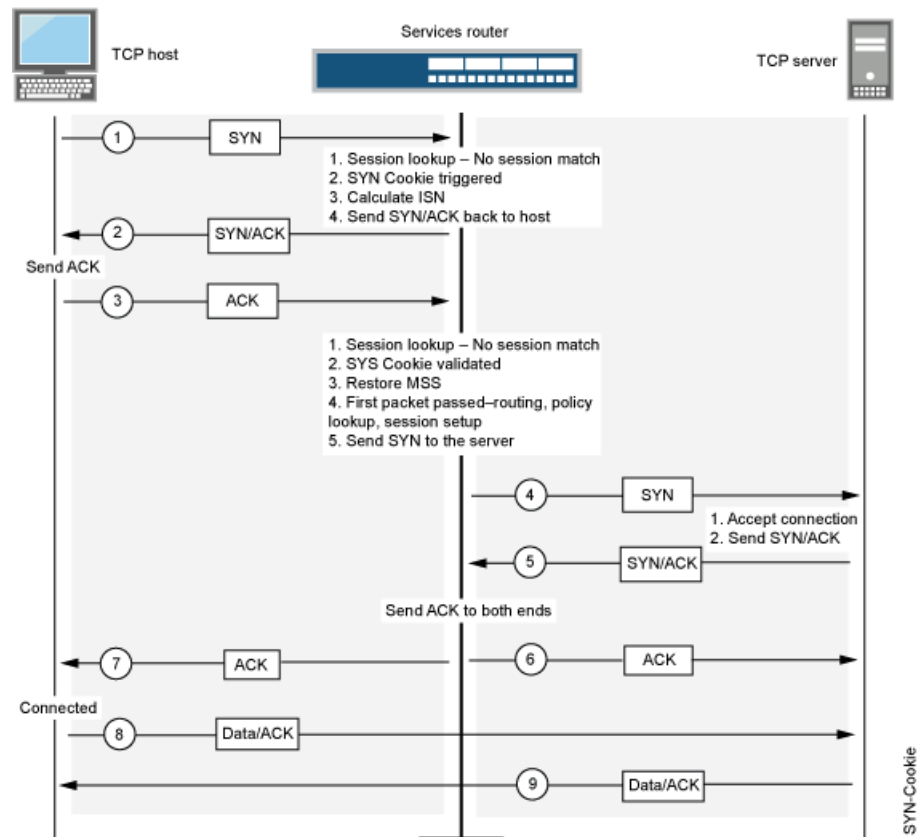
If the initiating host responds with a TCP packet containing the cookie + 1 in the TCP ACK field, Junos OS extracts the cookie, subtracts 1 from the value, and recomputes the cookie to validate that it is a legitimate ACK. If it is legitimate, Junos OS starts the TCP proxy process by setting up a session and sending a SYN to the server containing the source information from the original SYN. When Junos OS receives a SYN/ACK from the server, it sends ACKs to the server and to the initiation host. At this point the connection is established and the host and server are able to communicate directly.



NOTE: The use of SYN cookie or SYN proxy enables the SRX Series device to protect the TCP servers behind it from SYN flood attacks in IPv6 flows.

Figure 6 on page 18 shows how a connection is established between an initiating host and a server when SYN cookie is active on Junos OS.

Figure 6: Establishing a Connection with SYN Cookie Active



Related Documentation

- [Example: Enabling SYN Cookie Protection on page 48](#)
- [DoS Attack Overview on page 4](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Understanding ICMP Flood Attacks

Supported Platforms LN Series, SRX Series

An ICMP flood typically occurs when ICMP echo requests overload the victim with so many requests that the victim expends all its resources responding until it can no longer process valid network traffic.



NOTE: ICMP messages generated in flow mode are now rate-limited to 20 messages every 10 seconds. This rate limit is calculated on a per-CPU basis.

When enabling the ICMP flood protection feature, you can set a threshold that, once exceeded, invokes the ICMP flood attack protection feature. (The default threshold value is 1000 packets per second.) If the threshold is exceeded, Junos OS ignores further ICMP echo requests for the remainder of that second plus the next second as well. See [Figure 7 on page 19](#).



NOTE: An ICMP flood can consist of any type of ICMP message. Therefore, Junos OS monitors all ICMP message types, not just echo requests.

Figure 7: ICMP Flooding

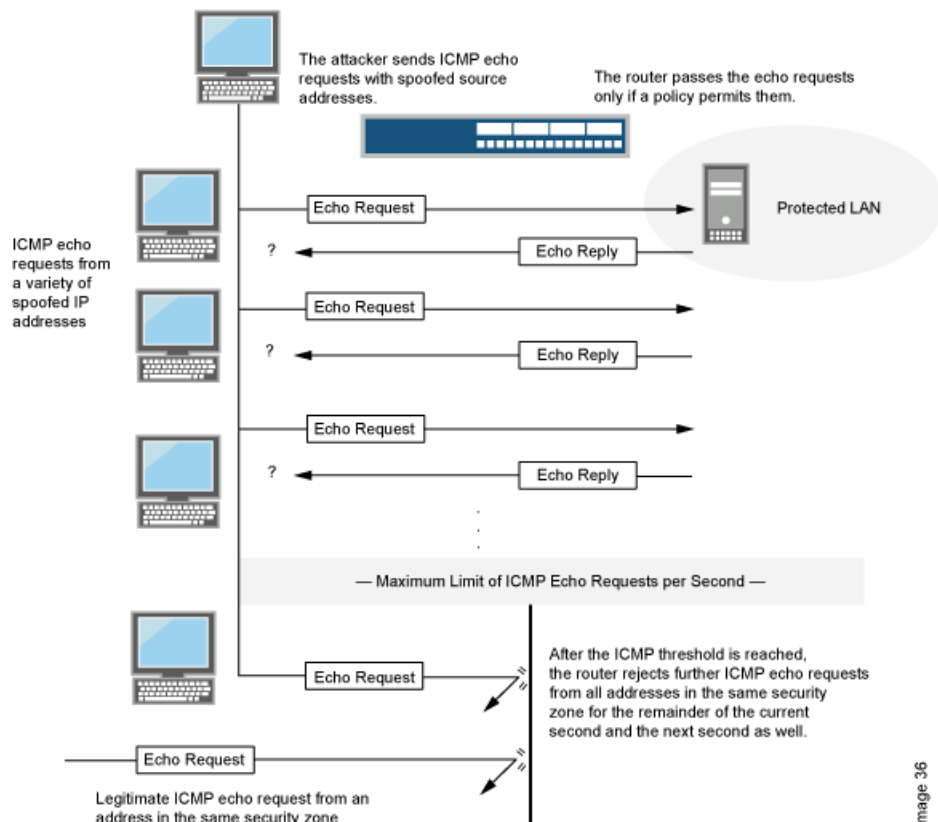


Image 36



NOTE: ICMP flood protection is supported for both ICMP and ICMPv6 packets.

**Related
Documentation**

- [Example: Enabling ICMP Flood Protection on page 50](#)
- [DoS Attack Overview on page 4](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

Understanding UDP Flood Attacks

Supported Platforms [LN Series](#), [SRX Series](#)

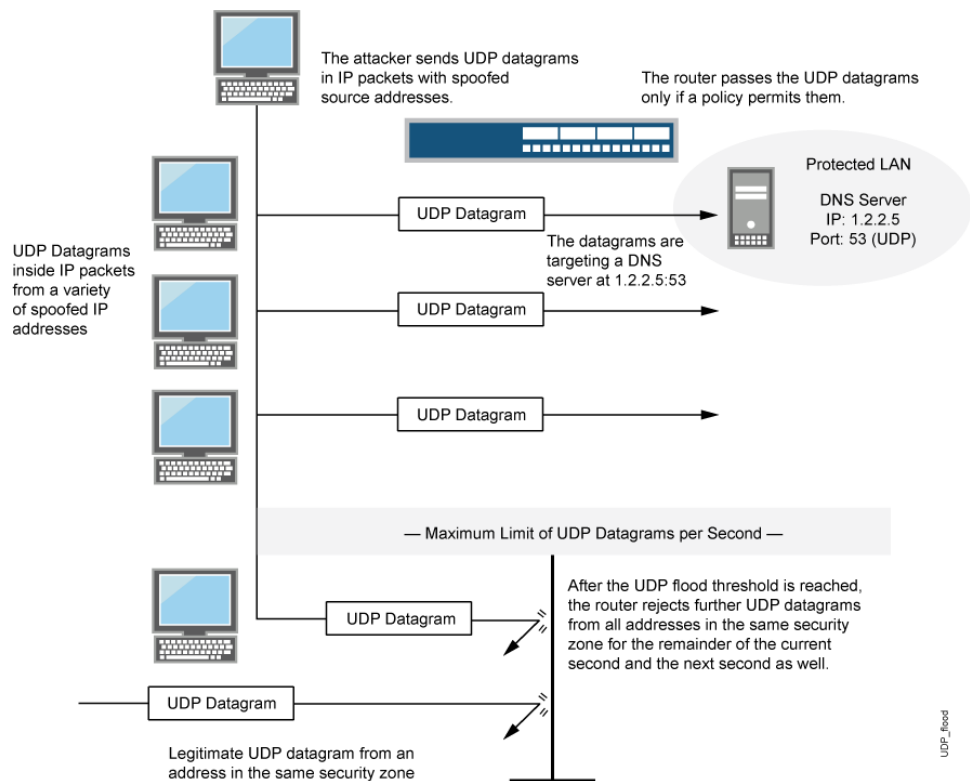
Similar to an ICMP flood, a UDP flood occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the victim to the point that the victim can no longer handle valid connections.

After enabling the UDP flood protection feature, you can set a threshold that, once exceeded, invokes the UDP flood attack protection feature. (The default threshold value is 1000 packets per second, or pps.) If the number of UDP datagrams from one or more sources to a single destination exceeds this threshold, Junos OS ignores further UDP datagrams to that destination for the remainder of that second plus the next second as well. See [Figure 8 on page 21](#).



NOTE: The high-end SRX Series devices do not drop the packet in the next second.

Figure 8: UDP Flooding



NOTE: Junos OS supports UDP flood protection for IPV4 and IPV6 packets.

Related Documentation

- [Example: Enabling UDP Flood Protection on page 52](#)
- [DoS Attack Overview on page 4](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

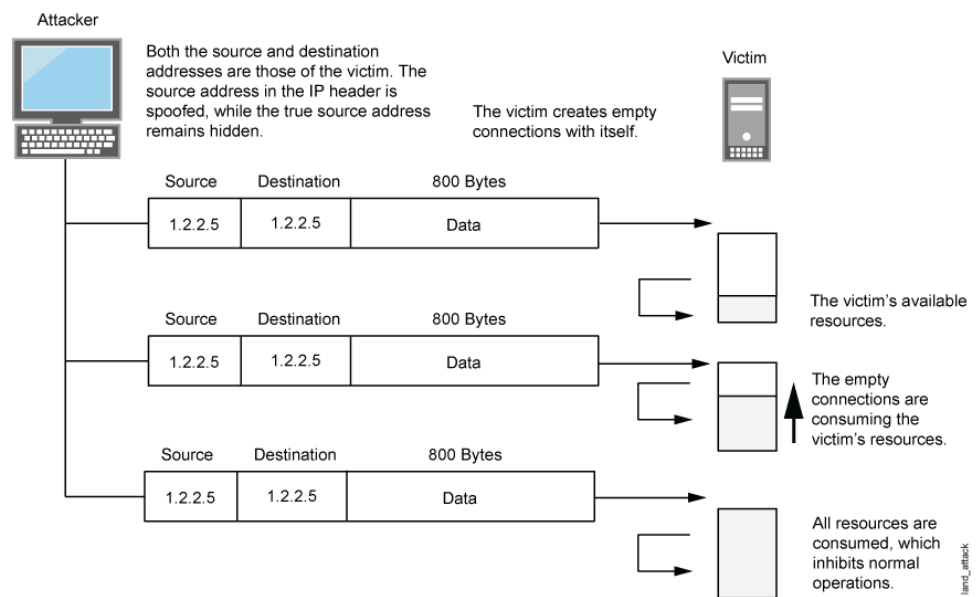
Understanding Land Attacks

Supported Platforms [LN Series, SRX Series](#)

Combining a SYN attack with IP spoofing, a land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and the source IP address.

The receiving system responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached. Flooding a system with such empty connections can overwhelm the system, causing a denial of service (DoS). See [Figure 9 on page 22](#).

Figure 9: Land Attack



When you enable the screen option to block land attacks, Junos OS combines elements of the SYN flood defense and IP spoofing protection to detect and block any attempts of this nature.



NOTE: Junos OS supports land attack protection for both IPv4 and IPv6 packets.

Related Documentation

- [Example: Protecting Against a Land Attack on page 54](#)
- [DoS Attack Overview on page 4](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

OS-Specific DoS Attacks

- [OS-Specific DoS Attacks Overview on page 22](#)
- [Understanding Ping of Death Attacks on page 23](#)
- [Understanding Teardrop Attacks on page 24](#)
- [Understanding WinNuke Attacks on page 25](#)

OS-Specific DoS Attacks Overview

Supported Platforms [LN Series](#), [SRX Series](#)

If an attacker not only identifies the IP address and responsive port numbers of an active host but also its operating system (OS), instead of resorting to brute-force attacks, the

attacker can launch more elegant attacks that can produce one-packet or two-packet “kills.”

OS-specific denial-of-service (DoS) attacks, including ping of death attacks, teardrop attacks, and WinNuke attacks, can cripple a system with minimal effort. If Junos OS is protecting hosts susceptible to these attacks, you can configure Junos OS to detect these attacks and block them before they reach their target.

Related Documentation

- [Understanding Ping of Death Attacks on page 23](#)
- [DoS Attack Overview on page 4](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

Understanding Ping of Death Attacks

Supported Platforms [LN Series, SRX Series](#)

OS-specific DoS attacks, such as ping of death attacks, can cripple a system with minimal effort.

The maximum allowable IP packet size is 65,535 bytes, including the packet header, which is typically 20 bytes. An ICMP echo request is an IP packet with a pseudo header, which is 8 bytes. Therefore, the maximum allowable size of the data area of an ICMP echo request is 65,507 bytes ($65,535 - 20 - 8 = 65,507$).

However, many ping implementations allow the user to specify a packet size larger than 65,507 bytes. A grossly oversized ICMP packet can trigger a range of adverse system reactions such as denial of service (DoS), crashing, freezing, and rebooting.

When you enable the ping of death screen option, Junos OS detects and rejects such oversized and irregular packet sizes even when the attacker hides the total packet size by fragmenting it. See [Figure 10 on page 23](#).



NOTE: For information about IP specifications, see RFC 791, *Internet Protocol*. For information about ICMP specifications, see RFC 792, *Internet Control Message Protocol*. For information about ping of death attacks, see <http://www.insecure.org/sploits/ping-o-death.html>.

Figure 10: Ping of Death



The size of this packet is 65,538 bytes. It exceeds the size limit prescribed by RFC 791, *Internet Protocol*, which is 65,535 bytes. As the packet is transmitted, it becomes broken into numerous fragments. The reassembly process might cause the receiving system to crash.



NOTE: Junos OS supports ping of death protection for both IPv4 and IPv6 packets.

Related Documentation

- [Example: Protecting Against a Ping of Death Attack on page 56](#)
- [DoS Attack Overview on page 4](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

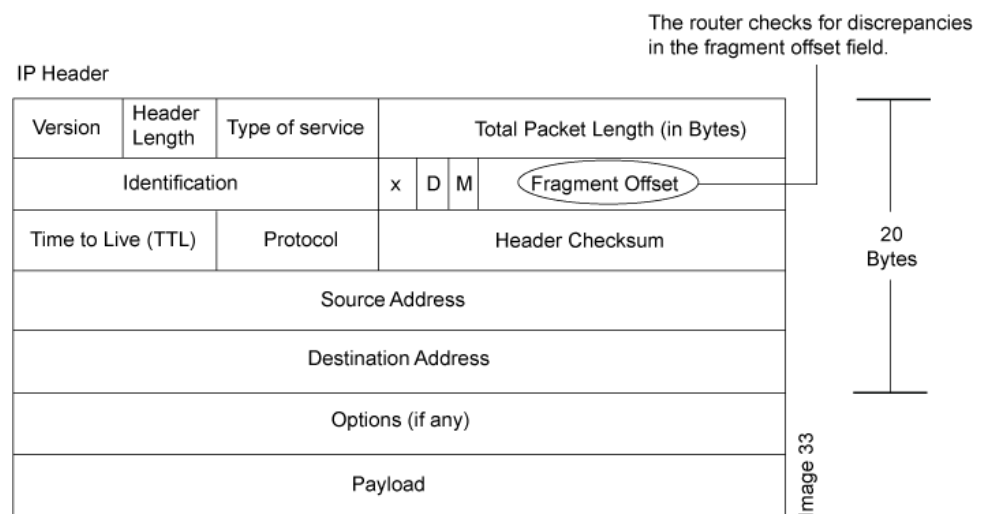
Understanding Teardrop Attacks

Supported Platforms [LN Series, SRX Series](#)

OS-specific denial-of-service (DoS) attacks, such as teardrop attacks, can cripple a system with minimal effort.

Teardrop attacks exploit the reassembly of fragmented IP packets. In the IP header, one of the fields is the fragment offset field, which indicates the starting position, or offset, of the data contained in a fragmented packet relative to the data of the original unfragmented packet. See [Figure 11 on page 24](#).

Figure 11: Teardrop Attacks



When the sum of the offset and size of one fragmented packet differ from that of the next fragmented packet, the packets overlap, and the server attempting to reassemble the packet can crash, especially if it is running an older OS that has this vulnerability. See [Figure 12 on page 25](#).

Figure 12: Fragment Discrepancy

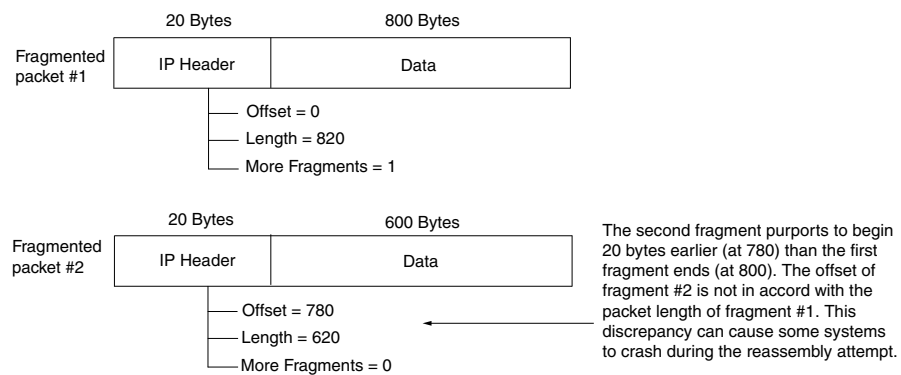


Image 33

After you enable the teardrop attack screen option, whenever Junos OS detects this discrepancy in a fragmented packet, it drops it.



NOTE: Junos OS supports teardrop attack prevention for both IPv4 and IPv6 packets.

Related Documentation

- [Example: Protecting Against a Teardrop Attack on page 57](#)
- [DoS Attack Overview on page 4](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Understanding WinNuke Attacks

Supported Platforms [LN Series, SRX Series](#)

OS-specific denial-of-service (DoS) attacks, such as WinNuke attacks, can cripple a system with minimal effort.

WinNuke is a DoS attack targeting any computer on the Internet running Windows. The attacker sends a TCP segment—usually to NetBIOS port 139 with the urgent (URG) flag set—to a host with an established connection (see [Figure 13 on page 26](#)). This introduces a NetBIOS fragment overlap, which causes many machines running Windows to crash. After the attacked machine is rebooted, the following message appears, indicating that an attack has occurred:

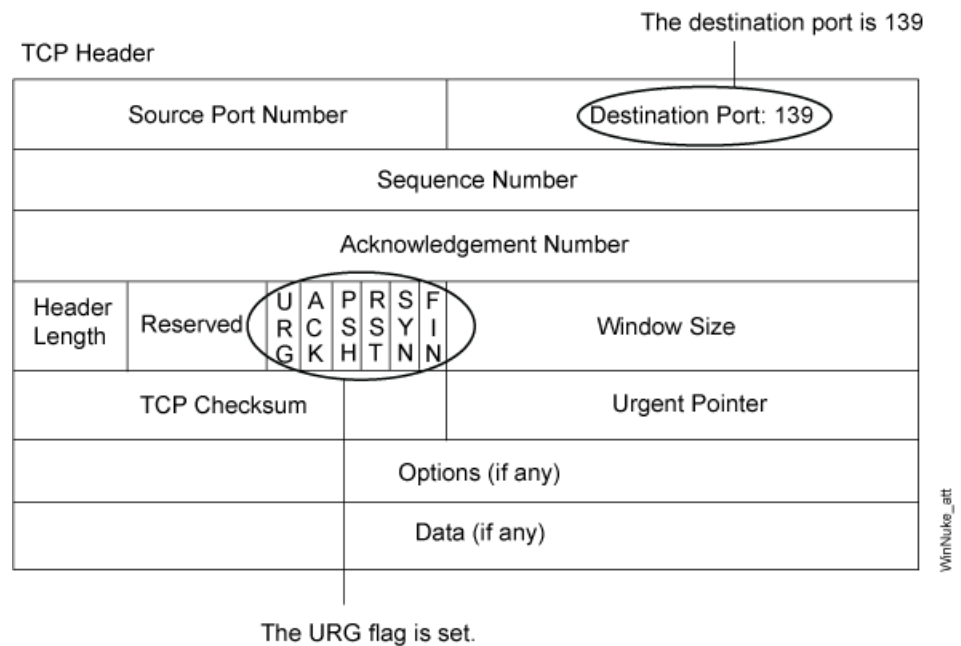
An exception OE has occurred at 0028:[address] in VxD MSTCP(01) + 000041AE. This was called from 0028:[address] in VxD NDIS(01) + 00008660. It may be possible to continue normally.

Press any key to attempt to continue.

Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue.

Figure 13: WinNuke Attack Indicators



If you enable the WinNuke attack defense screen option, Junos OS scans any incoming Microsoft NetBIOS session service (port 139) packets. If Junos OS observes that the URG flag is set in one of those packets, it unsets the URG flag, clears the URG pointer, forwards the modified packet, and makes an entry in the event log noting that it has blocked an attempted WinNuke attack.



NOTE: Junos OS supports WinNuke attack protection for both IPv4 and IPv6 traffic.

Related Documentation

- [Example: Protecting Against a WinNuke Attack on page 58](#)
- [DoS Attack Overview on page 4](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

CHAPTER 2

Configuration

- [Firewall DoS Attacks on page 27](#)
- [Network DoS Attacks on page 33](#)
- [OS-Specific DoS Attacks on page 56](#)
- [Configuration Statements on page 59](#)

Firewall DoS Attacks

- [Example: Setting Source-Based Session Limits on page 27](#)
- [Example: Setting Destination-Based Session Limits on page 29](#)
- [Example: Protecting Against a SYN-ACK-ACK Proxy Flood Attack on page 31](#)

Example: Setting Source-Based Session Limits

Supported Platforms [LN Series, SRX Series](#)

This example shows how to limit the amount of sessions based on source IP.

- [Requirements on page 27](#)
- [Overview on page 27](#)
- [Configuration on page 28](#)
- [Verification on page 29](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

The following example shows how to limit the number of sessions that any one server in the DMZ and in zone_a can initiate. Because the DMZ contains only web servers, none of which should initiate traffic, you set the source-session limit at the lowest possible value, which is one session. On the other hand, zone_a contains personal computers, servers, printers, and so on, many of which do initiate traffic. For zone_a, you set the source-session limit to a maximum of 80 concurrent sessions.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option 1-limit-session limit-session source-ip-based 1
set security zones security-zone dmz screen 1-limit-session
set security screen ids-option 80-limit-session limit-session source-ip-based 80
set security zones security-zone zone_a screen 80-limit-session
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To configure the source-based session limits:

1. Specify the number of concurrent sessions based on source IP for the DMZ zone.

```
[edit security]
user@host# set screen ids-option 1-limit-session limit-session source-ip-based 1
```
2. Set the security zone for the DMZ to the configuration limit.

```
[edit security]
user@host# set zones security-zone dmz screen 1-limit-session
```
3. Specify the number of concurrent sessions based on source IP for the zone_a zone.

```
[edit security]
user@host# set screen ids-option 80-limit-session limit-session source-ip-based 80
```
4. Set the security zone for zone_a to the configuration limit.

```
[edit security]
user@host# set zones security-zone zone_a screen 80-limit-session
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
ids-option 1-limit-session {
  limit-session {
    source-ip-based 1;
  }
}
ids-option 80-limit-session {
  limit-session {
    source-ip-based 1;
  }
}

[edit]
user@host# show security zones
security-zone dmz {
```

```

    screen 1-limit-session;
  }
  security-zone zone_a {
    screen 80-limit-session;
  }

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Source-Based Session Limits

Purpose Verify source-based session limits.

Action Enter the **show security screen ids-option 1-limit-session**, **show security screen ids-option 80-limit-session**, and **show security zones** commands from operational mode.

```

user@host> show security screen ids-option 1-limit-session
Screen object status:

```

Name	Value
Session source limit threshold	1

```

user@host> show security screen ids-option 80-limit-session
Screen object status:

```

Name	Value
Session source limit threshold	80

```

user@host> show security zones

```

```

Security zone: dmz
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: 1-limit-session
  Interfaces bound: 0
  Interfaces:

```

- Related Documentation**
- [Understanding Session Table Flood Attacks on page 7](#)
 - [Understanding Source-Based Session Limits on page 8](#)
 - [Example: Setting Destination-Based Session Limits on page 29](#)
 - [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Example: Setting Destination-Based Session Limits

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to set the destination-based session limits.

- [Requirements on page 30](#)
- [Overview on page 30](#)
- [Configuration on page 30](#)
- [Verification on page 31](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you limit the amount of traffic to a webserver at 1.2.2.5. The server is in the DMZ. The example assumes that after observing the traffic flow from the external zone to this server for a month, you have determined that the average number of concurrent sessions it receives is 2000. Also, you set the new session limit at 2000 concurrent sessions. Although traffic spikes might sometimes exceed that limit, the example assumes that you are opting for firewall security over occasional server inaccessibility.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option 2000-limit-session limit-session destination-ip-based 2000
set security zones security-zone external_zone screen 2000-limit-session
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To set the destination-based session limits:

1. Specify the number of concurrent sessions.

```
[edit]
user@host# set security screen ids-option 2000-limit-session limit-session
destination-ip-based 2000
```

2. Set the security zone for the external zone.

```
[edit]
user@host# set security zones security-zone external_zone screen
2000-limit-session
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
ids-option 2000-limit-session {
  limit-session {
    destination-ip-based 2000;
  }
}
[edit]
```



```

user@host# show security zones
security-zone external_zone {
    screen 2000-limit-session;
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Destination-Based Session Limits

Purpose Verify destination-based session limits.

Action Enter the **show security screen ids-option 2000-limit-session** and **show security zones** commands from operational mode.

```
user@host> show security screen ids-option 2000-limit-session
```

```
node0:
```

```
-----
Screen object status:
```

Name	Value
Session destination limit threshold	2000
Value	

```
user@host> show security zones
```

```

Security zone: external_zone
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Screen: 2000-limit-session
Interfaces bound: 0
Interfaces:

```

- Related Documentation**
- [Understanding Destination-Based Session Limits on page 9](#)
 - [DoS Attack Overview on page 4](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Example: Protecting Against a SYN-ACK-ACK Proxy Flood Attack

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to protect against a SYN-ACK-ACK proxy flood attack.

- [Requirements on page 32](#)
- [Overview on page 32](#)
- [Configuration on page 32](#)
- [Verification on page 33](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable protection against a SYN-ACK-ACK proxy flood. The value unit is connections per source address. The default value is 512 connections from any single address.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option 1000-syn-ack-ack-proxy tcp syn-ack-ack-proxy threshold 1000
set security zones security-zone zone screen 1000-syn-ack-ack-proxy
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To protect against a SYN-ACK-ACK proxy flood attack:

1. Specify the source session limits.

```
[edit]
user@host# set security screen ids-option 1000-syn-ack-ack-proxy tcp
syn-ack-ack-proxy threshold 1000
```

2. Set the security zone for zone screen.

```
[edit]
user@host# set security zones security-zone zone screen 1000-syn-ack-ack-proxy
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
ids-option 1000-syn-ack-ack-proxy {
  tcp {
    syn-ack-ack-proxy threshold 1000;
  }
}

[edit]
user@host# show security zones
security-zone zone {
  screen 1000-syn-ack-ack-proxy;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying SYN-ACK-ACK Proxy Flood Attack

Purpose Verify SYN-ACK-ACK proxy flood attack.

Action Enter the `show security screen ids-option 1000-syn-ack-ack-proxy` and `show security zones` commands from operational mode.

```
user@host> show security screen ids-option 1000-syn-ack-ack-proxy
node0:
```

```
-----
Screen object status:
```

Name	Value
TCP SYN-ACK-ACK proxy threshold	1000

```
user@host> show security zones
```

```
Security zone: zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: 1000-syn-ack-ack-proxy
  Interfaces bound: 0
  Interfaces:
```

- Related Documentation**
- [Understanding SYN-ACK-ACK Proxy Flood Attacks on page 10](#)
 - [DoS Attack Overview on page 4](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Network DoS Attacks

- [Example: Configuring Multiple Screening Options on page 33](#)
- [Example: Enabling SYN Flood Protection on page 38](#)
- [Example: Enabling SYN Flood Protection for Webservers in the DMZ on page 40](#)
- [Example: Configuring Whitelists for SYN Flood Screens on page 46](#)
- [Example: Enabling SYN Cookie Protection on page 48](#)
- [Example: Enabling ICMP Flood Protection on page 50](#)
- [Example: Enabling UDP Flood Protection on page 52](#)
- [Example: Protecting Against a Land Attack on page 54](#)

Example: Configuring Multiple Screening Options

Supported Platforms [SRX Series](#)

This example shows how to create one intrusion detection service (IDS) profile for multiple screening options.

- [Requirements on page 34](#)
- [Overview on page 34](#)
- [Configuration on page 34](#)
- [Verification on page 37](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In a security zone, you can apply one IDS profile to multiple screening options. In this example we are configuring the following screening options:

- ICMP screening
- IP screening
- TCP screening
- UDP screening

These screening options are assigned to an untrust zone.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option Screen-Config icmp ip-sweep threshold 1000
set security screen ids-option Screen-Config icmp fragment
set security screen ids-option Screen-Config icmp large
set security screen ids-option Screen-Config icmp flood threshold 200
set security screen ids-option Screen-Config icmp ping-death
set security screen ids-option Screen-Config ip bad-option
set security screen ids-option Screen-Config ip stream-option
set security screen ids-option Screen-Config ip spoofing
set security screen ids-option Screen-Config ip strict-source-route-option
set security screen ids-option Screen-Config ip unknown-protocol
set security screen ids-option Screen-Config ip tear-drop
set security screen ids-option Screen-Config tcp syn-fin
set security screen ids-option Screen-Config tcp tcp-no-flag
set security screen ids-option Screen-Config tcp syn-frag
set security screen ids-option Screen-Config tcp port-scan threshold 1000
set security screen ids-option Screen-Config tcp syn-ack-ack-proxy threshold 500
set security screen ids-option Screen-Config tcp syn-flood alarm-threshold 500
set security screen ids-option Screen-Config tcp syn-flood attack-threshold 500
set security screen ids-option Screen-Config tcp syn-flood source-threshold 50
set security screen ids-option Screen-Config tcp syn-flood destination-threshold 1000
```

```

set security screen ids-option Screen-Config tcp syn-flood timeout 10
set security screen ids-option Screen-Config tcp land
set security screen ids-option Screen-Config tcp winnuke
set security screen ids-option Screen-Config tcp tcp-sweep threshold 1000
set security screen ids-option Screen-Config udp flood threshold 500
set security screen ids-option Screen-Config udp udp-sweep threshold 1000
set security zones security-zone untrust screen Screen-Config

```

Enter **commit** from configuration mode.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure an IDS profile for multiple screening options:

1. Configure the ICMP screening options.

```

[edit security screen ids-option Screen-Config]
user@host# set icmp ip-sweep threshold 1000
user@host# set icmp fragment
user@host# set icmp large
user@host# set icmp flood threshold 200
user@host# set icmp ping-death

```

2. Configure the IP screening options.

```

[edit security screen ids-option Screen-Config]
user@host# set ip bad-option
user@host# set ip stream-option
user@host# set ip spoofing
user@host# set ip strict-source-route-option
user@host# set ip unknown-protocol
user@host# set ip tear-drop

```

3. Configure the TCP screening options.

```

[edit security screen ids-option Screen-Config]
user@host# set tcp syn-fin
user@host# set tcp tcp-no-flag
user@host# set tcp syn-frag
user@host# set tcp port-scan threshold 1000
user@host# set tcp syn-ack-ack-proxy threshold 500
user@host# set tcp syn-flood alarm-threshold 500
user@host# set tcp syn-flood attack-threshold 500
user@host# set tcp syn-flood source-threshold 50
user@host# set tcp syn-flood destination-threshold 1000
user@host# set tcp syn-flood timeout 10
user@host# set tcp land
user@host# set tcp winnuke
user@host# set tcp tcp-sweep threshold 1000

```

4. Configure the UDP screening options.

```

[edit security screen ids-option Screen-Config]
user@host# set udp flood threshold 500
user@host# set udp udp-sweep threshold 1000

```

5. Attach the IDS profile to the zone.

```
[edit]
user@host# set security zones security-zone untrust screen Screen-Config
```

Results From configuration mode, confirm your configuration by entering the **show security screen ids-option Screen-Config** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen ids-option Screen-Config
icmp {
  ip-sweep threshold 1000;
  fragment;
  large;
  flood threshold 200;
  ping-death;
}
ip {
  bad-option;
  stream-option;
  spoofing;
  strict-source-route-option;
  unknown-protocol;
  tear-drop;
}
tcp {
  syn-fin;
  tcp-no-flag;
  syn-frag;
  port-scan threshold 1000;
  syn-ack-ack-proxy threshold 500;
  syn-flood {
    alarm-threshold 500;
    attack-threshold 500;
    source-threshold 50;
    destination-threshold 1000;
    timeout 10;
  }
  land;
  winnuke;
  tcp-sweep threshold 1000;
}
udp {
  flood threshold 500;
  udp-sweep threshold 1000;
}

[edit]
user@host# show security zones
security-zone untrust {
  screen Screen-Config;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying the IDS Profile for Multiple Screening Options

Purpose Verify that the IDS profile for multiple screening options is configured properly.

Action Enter the `show security screen ids-option Screen-Config Screen object status` and `show security zones` command from operational mode.

```
user@host> show security screen ids-option Screen-Config
Screen object status:
```

Name	Value
ICMP flood threshold	200
UDP flood threshold	500
TCP winnuke	enabled
TCP port scan threshold	1000
ICMP address sweep threshold	1000
TCP sweep threshold	1000
UDP sweep threshold	1000
IP tear drop	enabled
TCP SYN flood attack threshold	500
TCP SYN flood alarm threshold	500
TCP SYN flood source threshold	50
TCP SYN flood destination threshold	1000
TCP SYN flood timeout	10
IP spoofing	enabled
ICMP ping of death	enabled
TCP land attack	enabled
TCP SYN fragment	enabled
TCP no flag	enabled
IP unknown protocol	enabled
IP bad options	enabled
IP strict source route option	enabled
IP stream option	enabled
ICMP fragmentation	enabled
ICMP large packet	enabled
TCP SYN FIN	enabled
TCP SYN-ACK-ACK proxy threshold	500

```
user@host> show security zones
```

```
Security zone: untrust
Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: Screen-Config
  Interfaces bound: 0
  Interfaces:
```



NOTE: On all SRX Series devices, the TCP synchronization flood alarm threshold value does not indicate the number of packets dropped, however the value does show the packet information after the alarm threshold has been reached.

The synchronization cookie or proxy never drops packets; therefore the alarm-without-drop (not drop) action is shown in the system log.

Example: Enabling SYN Flood Protection

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to enable SYN flood protection.

- [Requirements on page 38](#)
- [Overview on page 38](#)
- [Configuration on page 38](#)
- [Verification on page 39](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable the zone-syn-flood protection screen option and set the timeout value to 20. You also specify the zone where the flood might originate.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option zone-syn-flood tcp syn-flood source-threshold 10000
set security screen ids-option zone-syn-flood tcp syn-flood destination-threshold 10000
set security zones security-zone untrust screen zone-syn-flood
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To enable SYN flood protection:

1. Specify the screen object name.

```
[edit]
user@host# set security screen ids-option zone-syn-flood tcp syn-flood
source-threshold 10000
user@host# set security screen ids-option zone-syn-flood tcp syn-flood
destination-threshold 10000
```

2. Set the security zone for the zone screen.

```
[edit]
user@host# set security zones security-zone untrust screen zone-syn-flood
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.


```
[edit]
user@host# show security screen
ids-option zone-syn-flood {
  tcp {
    syn-flood {
      source-threshold 10000;
      destination-threshold 10000;
      timeout 20;
    }
  }
}

[edit]
user@host# show security zones
security-zone untrust {
  screen zone-syn-flood;
  interfaces {
    ge-0/0/1.0;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying SYN Flood Protection

Purpose Verify SYN flood protection.

Action Enter the **show security screen ids-option zone-syn-flood** and **show security zones** commands from operational mode.

```
user@host> show security screen ids-option zone-syn-flood
node0:
```

Screen object status:

Name	Value
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	10000
TCP SYN flood destination threshold	10000
TCP SYN flood timeout	20

```
user@host> show security zones
```

```
Security zone: untrust
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: zone-syn-flood
  Interfaces bound: 1
  Interfaces:
    ge-0/0/1.0
```

Related Documentation

- [Understanding SYN Flood Attacks on page 12](#)
- [Configuring SYN Flood Protection Options \(CLI Procedure\)](#)

- [Example: Enabling SYN Flood Protection for Webserver in the DMZ on page 40](#)
- [Understanding Whitelists for SYN Flood Screens on page 17](#)
- [Example: Configuring Whitelists for SYN Flood Screens on page 46](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

Example: Enabling SYN Flood Protection for Webserver in the DMZ

Supported Platforms [LN Series, SRX Series](#)

This example shows how to enable SYN flood protection for webserver in the DMZ.

- [Requirements on page 40](#)
- [Overview on page 40](#)
- [Configuration on page 43](#)
- [Verification on page 46](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

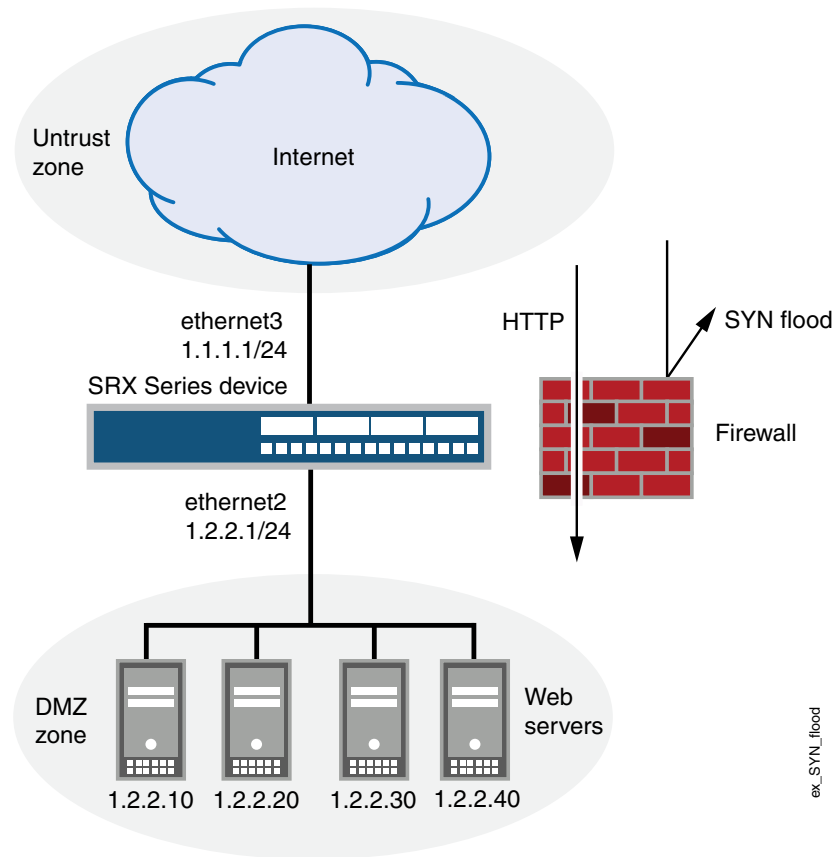
Overview

This example shows how to protect four webserver in the DMZ from SYN flood attacks originating in the external zone, by enabling the SYN flood protection screen option for the external zone. See [Figure 14 on page 41](#)



NOTE: We recommend that you augment the SYN flood protection that Junos OS provides with device-level SYN flood protection on each webserver. In this example, the webserver are running UNIX, which also provides some SYN flood defenses, such as adjusting the length of the connection request queue and changing the timeout period for incomplete connection requests.

Figure 14: Device-Level SYN Flood Protection



To configure the SYN flood protection parameters with appropriate values for your network, you must first establish a baseline of typical traffic flows. For example, for one week, you run a sniffer on ethernet3—the interface bound to zone_external—to monitor the number of new TCP connection requests arriving every second for the four web servers in the DMZ. Your analysis of the data accumulated from one week of monitoring produces the following statistics:

- Average number of new connection requests per server: 250 per second
- Average peak number of new connection requests per server: 500 per second



NOTE: A sniffer is a network-analyzing device that captures packets on the network segment to which you attach it. Most sniffers allow you to define filters to collect only the type of traffic that interests you. Later, you can view and evaluate the accumulated information. In this example, you want the sniffer to collect all TCP packets with the SYN flag set arriving at ethernet3 and destined for one of the four web servers in the DMZ. You might want to continue running the sniffer at regular intervals to see whether there are traffic patterns based on the time of day, day of the week, time of the month, or season of the year. For example, in some organizations, traffic might increase dramatically during a critical event. Significant changes probably warrant adjusting the various thresholds.

Based on this information, you set the following SYN flood protection parameters for zone_external as shown in [Table 3 on page 42](#).

Table 3: SYN Flood Protection Parameters

Parameter	Value	Reason for Each Value
Attack threshold	625 pps	This is 25% higher than the average peak number of new connection requests per second per server, which is unusual for this network environment. When the number of SYN packets per second for any one of the four web servers exceeds this number, the device begins proxying new connection requests to that server. (In other words, beginning with the 626th SYN packet to the same destination address in one second, the device begins proxying connection requests to that address.)
Alarm threshold	250 pps	When the device proxies 251 new connection requests in one second, it makes an alarm entry in the event log. By setting the alarm threshold somewhat higher than the attack threshold, you can avoid alarm entries for traffic spikes that only slightly exceed the attack threshold.
Source threshold	25 pps	<p>When you set a source threshold, the device tracks the source IP address of SYN packets, regardless of the destination address. (Note that this source-based tracking is separate from the tracking of SYN packets based on destination address, which constitutes the basic SYN flood protection mechanism.)</p> <p>In the one week of monitoring activity, you observed that no more than 1/25 of new connection requests for all servers came from any one source within a one-second interval. Therefore, connection requests exceeding this threshold are unusual and provide sufficient cause for the device to execute its proxying mechanism. (Note that 25 pps is 1/25 of the attack threshold, which is 625 pps.)</p> <p>If the device tracks 25 SYN packets from the same source IP address, then, beginning with the 26th packet, it rejects all further SYN packets from that source for the remainder of that second and for the next second as well.</p>
Destination threshold	0 pps	When you set a destination threshold, the device runs a separate tracking of only the destination IP address, regardless of the destination port number. Because the four web servers receive only HTTP traffic (destination port 80)—no traffic to any other destination port number reaches them—setting another destination threshold offers no additional advantage.

Table 3: SYN Flood Protection Parameters (*continued*)

Parameter	Value	Reason for Each Value
Timeout	20 seconds	The default value of 20 seconds is a reasonable length of time to hold incomplete connection requests.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces ge-0/0/0 unit 0 family inet address 1.2.2.1/24
set interfaces fe-1/0/0 unit 0 family inet address 1.1.1.1/24
set security zones security-zone zone_dmz interfaces ge-0/0/0.0
set security zones security-zone zone_external interfaces fe-1/0/0.0
set security zones security-zone zone_dmz address-book address ws1 1.2.2.10/32
set security zones security-zone zone_dmz address-book address ws2 1.2.2.20/32
set security zones security-zone zone_dmz address-book address ws3 1.2.2.30/32
set security zones security-zone zone_dmz address-book address ws4 1.2.2.40/32
set security zones security-zone zone_dmz address-book address-set web_servers address
ws1
set security zones security-zone zone_dmz address-book address-set web_servers address
ws2
set security zones security-zone zone_dmz address-book address-set web_servers address
ws3
set security zones security-zone zone_dmz address-book address-set web_servers address
ws4
set security policies from-zone zone_external to-zone zone_dmz policy id_1 match
source-address any destination-address web_servers application junos-http
set security policies from-zone zone_external to-zone zone_dmz policy id_1 then permit
set security screen ids-option zone_external-syn-flood tcp syn-flood alarm-threshold
250 attack-threshold 625 source-threshold 25 timeout 20
set security zones security-zone zone_external screen zone_external-syn-flood
```

Step-by-Step Procedure

To configure SYN flood protection parameters:

1. Set interfaces.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 1.2.2.1/24
user@host# set interfaces fe-1/0/0 unit 0 family inet address 1.1.1.1/24
user@host# set security zones security-zone zone_dmz interfaces ge-0/0/0.0
user@host# set security zones security-zone zone_external interfaces fe-1/0/0.0
```

2. Define addresses.

```
[edit]
user@host# set security zones security-zone zone_dmz address-book address ws1
1.2.2.10/32
user@host# set security zones security-zone zone_dmz address-book address ws2
1.2.2.20/32
user@host# set security zones security-zone zone_dmz address-book address ws3
1.2.2.30/32
```

```
user@host# set security zones security-zone zone_dmz address-book address ws4
1.2.2.40/32
user@host# set security zones security-zone zone_dmz address-book address-set
web_servers address ws1
user@host# set security zones security-zone zone_dmz address-book address-set
web_servers address ws2
user@host# set security zones security-zone zone_dmz address-book address-set
web_servers address ws3
user@host# set security zones security-zone zone_dmz address-book address-set
web_servers address ws4
```

3. Configure the policy.

```
[edit]
user@host# set security policies from-zone zone_external to-zone zone_dmz policy
id_1 match source-address any
user@host# set security policies from-zone zone_external to-zone zone_dmz policy
id_1 match destination-address web_servers
user@host# set security policies from-zone zone_external to-zone zone_dmz policy
id_1 match application junos-http
user@host# set security policies from-zone zone_external to-zone zone_dmz policy
id_1 then permit
```

4. Configure the screen options.

```
[edit]
user@host# set security screen ids-option zone_external-syn-flood tcp syn-flood
alarm-threshold 250
user@host# set security screen ids-option zone_external-syn-flood tcp syn-flood
attack-threshold 625
user@host# set security screen ids-option zone_external-syn-flood tcp syn-flood
source-threshold 25
user@host# set security screen ids-option zone_external-syn-flood tcp syn-flood
timeout 20
user@host# set security zones security-zone zone_external screen
zone_external-syn-flood
```

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security policies**, and **show security screen** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 1.2.2.1/24;
    }
  }
}
fe-1/0/0 {
```

```

unit 0 {
    family inet {
        address 1.1.1.1/24;
    }
}
...
[edit]
user@host# show security zones
...
    security-zone zone_dmz {
address-book {
address ws1 1.2.2.10/32;
    address ws2 1.2.2.20/32;
    address ws3 1.2.2.30/32;
    address ws4 1.2.2.40/32;
address-set web_servers {
    address ws1;
    address ws2;
    address ws3;
    address ws4;
}
}
interfaces {
    ge-0/0/0.0;
}
}
security-zone zone_external {
    screen zone_external-syn-flood;
    interfaces {
        fe-1/0/0.0;
    }
}
[edit]
user@host# show security policies
from-zone zone_external to-zone zone_dmz {
    policy id_1 {
match {
source-address any;
    destination-address web_servers;
    application junos-http;
}
then {
permit;
}
}
}
[edit]
user@host# show security screen
...
ids-option zone_external-syn-flood {
    tcp {
syn-flood {
alarm-threshold 250;
    attack-threshold 625;
    source-threshold 25;

```

```
    timeout 20;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying SYN Flood Protection for Webservers in the DMZ

Purpose Verify SYN flood protection for web servers in the DMZ.

Action From operational mode, enter the **show interfaces**, **show security zones**, **show security policies**, and **show security screen ids-option zone_external-syn-flood** commands.

Related Documentation

- [Understanding SYN Flood Attacks on page 12](#)
- [Example: Enabling SYN Flood Protection on page 38](#)
- [Configuring SYN Flood Protection Options \(CLI Procedure\)](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Example: Configuring Whitelists for SYN Flood Screens

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to configure whitelists of IP addresses to be exempted from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process.

- [Requirements on page 46](#)
- [Overview on page 46](#)
- [Configuration on page 47](#)
- [Verification on page 48](#)

Requirements

Before you begin, configure a security screen and enable the screen in the security zone. See [Example: Enabling SYN Flood Protection](#).

Overview

In this example, you configure whitelists named **wlipv4** and **wlipv6**. All addresses are IP version 4 (IPv4) for **wlipv4**, and all addresses are IP version 6 (IPv6) for **wlipv6**. Both whitelists include destination and source IP addresses.

Multiple addresses or address prefixes can be configured as a sequence of addresses separated by spaces and enclosed in square brackets, as shown in the configuration of the destination addresses for **wlipv4**.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option js1 tcp syn-flood white-list wlipv4 source-address 1.1.1.0/24
set security screen ids-option js1 tcp syn-flood white-list wlipv4 destination-address
  2.2.2.2/32
set security screen ids-option js1 tcp syn-flood white-list wlipv4 destination-address
  3.3.3.3/32
set security screen ids-option js1 tcp syn-flood white-list wlipv4 destination-address
  4.4.4.4/32
set security screen ids-option js1 tcp syn-flood white-list wlipv6 source-address 2001::1/64
set security screen ids-option js1 tcp syn-flood white-list wlipv6 destination-address
  2002::1/64
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the whitelists:

1. Specify the name of the whitelist and the IP addresses to be exempted from the SYN/ACK.

```
[edit security screen ids-option js1 tcp syn-flood]
user@host# set white-list wlipv4 source-address 1.1.1.0/24
user@host# set white-list wlipv4 destination-address [2.2.2.2 3.3.3.3 4.4.4.4]
user@host# set white-list wlipv6 source-address 2001::1/64
user@host# set white-list wlipv6 destination-address 2002::1/64
```

Results From configuration mode, confirm your configuration by entering the **show security screen** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
ids-option js1 {
  tcp {
    syn-flood {
      white-list wlipv4 {
        source-address 1.1.1.0/24;
        destination-address [ 2.2.2.2/32 3.3.3.3/32 4.4.4.4/32 ];
      }
      white-list wlipv6 {
        source-address 2001::1/64;
        destination-address 2002::1/64;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Whitelist Configuration

Purpose Verify that the whitelist is configured properly.

Action From operational mode, enter the **show security screen ids-option** command.

Related Documentation

- [Understanding SYN Flood Attacks on page 12](#)
- [Example: Enabling SYN Flood Protection on page 38](#)
- [Understanding Whitelists for SYN Flood Screens on page 17](#)
- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Example: Enabling SYN Cookie Protection

Supported Platforms LN Series, SRX Series

This example shows how to enable the SYN cookie protection.

- [Requirements on page 48](#)
- [Overview on page 48](#)
- [Configuration on page 48](#)
- [Verification on page 50](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you set the external-syn-flood timeout value to 20 and set the security zone for external screen to external-syn-flood. Also, you set the protection mode to syn-cookie.



NOTE: The SYN cookie feature can detect and protect only against spoofed SYN flood attacks, thus minimizing the negative impact on hosts that are secured by Junos OS. If an attacker uses a legitimate IP source address, rather than a spoofed IP source, then the SYN cookie mechanism does not stop the attack.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network

configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option external-syn-flood tcp syn-flood timeout 20
set security zones security-zone external screen external-syn-flood
set security flow syn-flood-protection-mode syn-cookie
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To enable the SYN cookie protection:

1. Specify the external-syn-flood timeout value.

```
[edit]
user@host# set security screen ids-option external-syn-flood tcp syn-flood timeout
20
```

2. Set the security-zone for external screen.

```
[edit]
user@host# set security zones security-zone external screen external-syn-flood
```

3. Set the protection mode.

```
[edit]
user@host# set security flow syn-flood-protection-mode syn-cookie
```

Results From configuration mode, confirm your configuration by entering the **show security screen**, **show security zones**, and **show security flow** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
set security flow syn-flood-protection-mode syn-cookie {
  tcp {
    syn-flood {
      source-ip-based 1;
    }
  }
}

[edit]
user@host# show security zones
security-zone external {
  screen external-syn-flood;
}

[edit]
user@host# show security flow
syn-flood-protection-mode syn-cookie;
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying SYN Cookie Protection

Purpose Verifying SYN cookie protection.

Action Enter the **show security screen ids-option external-syn-flood** and **show security zones** commands from operational mode.

```
user@host> show security screen ids-option external-syn-flood
node0:
```

Screen object status:

Name	Value
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	4000
TCP SYN flood destination threshold	4000
TCP SYN flood timeout	20

```
user@host> show security zones
```

```
Security zone: external
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: external-syn-flood
  Interfaces bound: 0
  Interfaces:
```

```
user@host> show security zones
```

```
Security zone: external
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: external-syn-flood
  Interfaces bound: 0
  Interfaces:
```

- Related Documentation**
- [Understanding SYN Cookie Protection on page 17](#)
 - [DoS Attack Overview on page 4](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Example: Enabling ICMP Flood Protection

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to enable ICMP flood protection.

- [Requirements on page 51](#)
- [Overview on page 51](#)
- [Configuration on page 51](#)
- [Verification on page 52](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable ICMP flood protection. The value unit is ICMP packets per second, or pps. The default value is 1000 pps. You specify the zone where a flood might originate.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option 1000-icmp-flood icmp flood threshold 1000
set security zones security-zone zone screen 1000-icmp-flood
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To enable ICMP flood protection:

1. Specify the ICMP flood threshold value.

```
[edit]
user@host# set security screen ids-option 1000-icmp-flood icmp flood threshold
1000
```

2. Set the security zone for zone screen.

```
[edit]
user@host# set security zones security-zone zone screen 1000-icmp-flood
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
ids-option 1000-icmp-flood {
  icmp {
    flood threshold 1000;
  }
}
```

```
[edit]
user@host# show security zones
security-zone zone {
  screen 1000-icmp-flood;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying ICMP Flood Protection

Purpose Verify ICMP flood protection

Action Enter the **show security screen ids-option 1000-icmp-flood** and **show security zones** commands from operational mode.

```
user@host> show security screen ids-option 1000-icmp-flood
node0:
```

Screen object status:

Name	Value
ICMP flood threshold	1000

```
user@host> show security zones
```

```
Security zone: zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: 1000-icmp-flood
  Interfaces bound: 0
  Interfaces:
```

- Related Documentation**
- [Understanding ICMP Flood Attacks on page 19](#)
 - [DoS Attack Overview on page 4](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Example: Enabling UDP Flood Protection

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to enable UDP flood protection.

- [Requirements on page 52](#)
- [Overview on page 52](#)
- [Configuration on page 53](#)
- [Verification on page 53](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable UDP flood protection. The value unit is UDP packets per second, or pps. The default value is 1000 pps. You specify the zone where a flood might originate.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option 1000-udp-flood udp flood threshold 1000
set security zones security-zone external screen 1000-udp-flood
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To enable UDP flood protection:

1. Specify the UDP flood threshold value.

```
[edit]
user@host# set security screen ids-option 1000-udp-flood udp flood threshold
1000
```

2. Set the security zone for external screen.

```
[edit]
user@host# set security zones security-zone external screen 1000-udp-flood
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
ids-option 1000-udp-flood {
  udp {
    flood threshold 1000;
  }
}

[edit]
user@host# show security zones
security-zone external {
  screen 1000-udp-flood;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying UDP Flood Protection

Purpose Verify UDP flood protection.

Action Enter the **show security screen ids-option 1000-udp-flood** and **show security zones** commands from operational mode.

```
user@host> show security screen ids-option 1000-udp-flood
node0:
```

Screen object status:

Name	Value
UDP flood threshold	1000

```
user@host> show security zones
```

```
Security zone: external
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: 1000-udp-flood
  Interfaces bound: 0
  Interfaces:
```

- Related Documentation**
- [Understanding UDP Flood Attacks on page 20](#)
 - [DoS Attack Overview on page 4](#)
 - [Denial-of-Service Attacks Feature Guide for Security Devices](#)

Example: Protecting Against a Land Attack

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to protect against a land attack.

- [Requirements on page 54](#)
- [Overview on page 54](#)
- [Configuration on page 54](#)
- [Verification on page 55](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

This example shows how to enable protection against a land attack. In this example, you set the security screen object name as land and set the security zone as zone.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security screen ids-option land tcp land
```



```
set security zones security-zone zone screen land
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*. To enable protection against a land attack:

1. Specify the screen object name.

```
[edit]
user@host# set security screen ids-option land tcp land
```

2. Set the security zone.

```
[edit]
user@host# set security zones security-zone zone screen land
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen
  ids-option land {
    tcp {
      land;
    }
  }

[edit]
user@host# show security zones
  security-zone zone {
    screen land;
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Protection Against a Land Attack

Purpose Verify protection against a land attack.

Action Enter the **show security screen ids-option land** and **show security zones** commands from operational mode.

```
user@host> show security screen ids-option land
node0:
-----
Screen object status:

Name                                     Value
TCP land attack                         enabled

user@host> show security zones

Security zone: zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
```

Screen: 1and
Interfaces bound: 0
Interfaces:

**Related
Documentation**

- [Understanding Land Attacks on page 21](#)
- [DoS Attack Overview on page 4](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

OS-Specific DoS Attacks

- [Example: Protecting Against a Ping of Death Attack on page 56](#)
- [Example: Protecting Against a Teardrop Attack on page 57](#)
- [Example: Protecting Against a WinNuke Attack on page 58](#)

Example: Protecting Against a Ping of Death Attack

Supported Platforms [LN Series, SRX Series](#)

This example shows how to protect against a ping-of-death attack.

- [Requirements on page 56](#)
- [Overview on page 56](#)
- [Configuration on page 56](#)
- [Verification on page 57](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable protection against a ping-of-death attack and specify the zone where the attack originates.

Configuration

**Step-by-Step
Procedure**

To enable protection against a ping of death:

1. Specify the screen object name.

[edit]
user@host# set security screen ids-option ping-death icmp ping-death
2. Set the security zone for zone screen.

[edit]
user@host# set security zones security-zone zone screen ping-death
3. If you are done configuring the device, commit the configuration.

[edit]
user@host# commit

Verification

To verify the configuration is working properly, enter the **show security screen ids-option ping-death** and **show security zones** commands in operational mode.

Related Documentation

- [Understanding Ping of Death Attacks on page 23](#)
- [DoS Attack Overview on page 4](#)
- *Denial-of-Service Attacks Feature Guide for Security Devices*

Example: Protecting Against a Teardrop Attack

Supported Platforms [LN Series, SRX Series](#)

This example shows how to protect against a teardrop attack.

- [Requirements on page 57](#)
- [Overview on page 57](#)
- [Configuration on page 57](#)
- [Verification on page 57](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable protection against a teardrop attack and also specify the zone where the attack originates.

Configuration

Step-by-Step Procedure

To enable protection against teardrop attack:

1. Specify the screen name.

```
[edit]
user@host# set security screen ids-option tear-drop ip tear-drop
```
2. Associate the screen with a security zone.

```
[edit]
user@host# set security zones security-zone zone screen tear-drop
```
3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen ids-option tear-drop** and **show security zones** commands in operational mode.

- Related Documentation**
- [Understanding Teardrop Attacks on page 24](#)
 - [DoS Attack Overview on page 4](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Example: Protecting Against a WinNuke Attack

Supported Platforms [LN Series, SRX Series](#)

This example shows how to protect against a WinNuke attack.

- [Requirements on page 58](#)
- [Overview on page 58](#)
- [Configuration on page 58](#)
- [Verification on page 58](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you enable protection against a WinNuke attack and specify the zone where the attack originates.

Configuration

Step-by-Step Procedure

To enable protection against WinNuke attack:

1. Specify the screen name.

```
[edit]  
user@host# set security screen ids-option winnuke tcp winnuke
```
2. Associate the screen with a security zone.

```
[edit]  
user@host# set security zones security-zone zone screen winnuke
```
3. If you are done configuring the device, commit the configuration.

```
[edit]  
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen ids-option winnuke** and **show security zones** commands in operational mode.

- Related Documentation**
- [Understanding WinNuke Attacks on page 25](#)
 - [DoS Attack Overview on page 4](#)
 - *Denial-of-Service Attacks Feature Guide for Security Devices*

Configuration Statements

- [\[edit security screen\] Hierarchy Level on page 60](#)
- [attack-threshold on page 62](#)
- [description \(Security Screen\) on page 63](#)
- [destination-ip-based on page 64](#)
- [destination-threshold on page 65](#)
- [fin-no-ack on page 66](#)
- [flood \(Security ICMP\) on page 67](#)
- [flood \(Security UDP\) on page 68](#)
- [icmp \(Security Screen\) on page 69](#)
- [ids-option on page 70](#)
- [ip \(Security Screen\) on page 73](#)
- [ip-sweep on page 75](#)
- [land on page 76](#)
- [limit-session on page 76](#)
- [ping-death on page 77](#)
- [port-scan on page 78](#)
- [screen \(Security Zones\) on page 79](#)
- [source-ip-based on page 79](#)
- [source-threshold on page 80](#)
- [syn-ack-ack-proxy on page 81](#)
- [syn-check-required on page 81](#)
- [syn-fin on page 82](#)
- [syn-flood on page 83](#)
- [syn-flood-protection-mode on page 84](#)
- [syn-frag on page 84](#)
- [tcp \(Security Screen\) on page 85](#)
- [tcp-no-flag on page 86](#)
- [tcp-sweep on page 87](#)
- [timeout \(Security Screen\) on page 88](#)
- [traceoptions \(Security Screen\) on page 89](#)
- [udp \(Security Screen\) on page 91](#)
- [udp-sweep on page 92](#)
- [white-list on page 93](#)
- [winnuke on page 94](#)

[edit security screen] Hierarchy Level

Supported Platforms [LN Series](#), [SRX Series](#)

```
security {
  screen {
    ids-option screen-name {
      alarm-without-drop;
      description text;
      icmp {
        flood {
          threshold number;
        }
        fragment;
        icmpv6-malformed;
        ip-sweep {
          threshold number;
        }
        large;
        ping-death;
      }
    }
    ip {
      bad-option;
      block-frag;
      ipv6-extension-header {
        AH-header;
        ESP-header;
        HIP-header;
        destination-header {
          ILNP-nonce-option;
          home-address-option;
          line-identification-option;
          tunnel-encapsulation-limit-option;
          user-defined-option-type low | <to high>;
        }
        fragment-header;
        hop-by-hop-header {
          CALIPSO-option;
          RPL-option;
          SFM-DPD-option;
          jumbo-payload-option;
          quick-start-option;
          router-alert-option;
          user-defined-option-type low | <to high>;
        }
        mobility-header;
        no-next-header;
        routing-header;
        shim6-header;
        user-defined-option-type low | <to high>;
      }
      ipv6-extension-header-limit limit;
      ipv6-malformed-header;
      loose-source-route-option;
      record-route-option;
```

```

security-option;
source-route-option;
spoofing;
stream-option;
strict-source-route-option;
tear-drop;
timestamp-option;
unknown-protocol;
}
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
tcp {
    fin-no-ack;
    land;
    port-scan {
        threshold number;
    }
    syn-ack-ack-proxy {
        threshold number;
    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
        threshold threshold number;
    }
    winnuke;
}
udp {
    flood {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
}
}
traceoptions {
    file filename {
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
    }
}

```

```
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
```

Related Documentation

- [Security Configuration Statement Hierarchy](#)
- [Junos OS Logical Systems Library for Security Devices](#)

attack-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `attack-threshold number;`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Define the number of SYN packets per second required to trigger the SYN proxy response.

Options *number* —Number of SYN packets per second required to trigger the SYN proxy response.
Range: 1 through 500,000 per second
Default: 200 per second



NOTE: For SRX Series devices, the applicable range is 1 through 1,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)
- [destination-threshold on page 65](#)

description (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `description text;`

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 12.1 of Junos OS.

Description Specify descriptive text for a screen.



NOTE: The descriptive text should not include characters, such as "<", ">", "&", or "\n".

Options *text*—Descriptive text about a screen.

Range: 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

Required Privilege security—To view this statement in the configuration.

Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

destination-ip-based

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax destination-ip-based *number*;

Hierarchy Level [edit security screen ids-option *screen-name* limit-session]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Limit the number of concurrent sessions the device can direct to a single destination IP address.

Options *number*—Maximum number of concurrent sessions that can be directed to a destination IP address.

Range: 1 through 1,000,000

Default: 128



NOTE: For SRX Series devices, the applicable range is 1 through 8,000,000.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

destination-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax destination-threshold *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based only on the destination IP address, regardless of the destination port number.

Options *number* —Number of SYN segments received per second before the device begins dropping connection requests.

Range: 4 through 500,000 per second

Default: 2048 per second



NOTE: For SRX Series devices, the applicable range is 4 through 1,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)
- [attack-threshold on page 62](#)

fin-no-ack

Supported Platforms	LN Series , SRX Series
Syntax	fin-no-ack;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of an illegal combination of flags, and reject packets that have this combination.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

flood (Security ICMP)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax flood {
 threshold *number*;
}

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the device to detect and prevent Internet Control Message Protocol (ICMP) floods. An ICMP flood occurs when ICMP echo requests are broadcast with the purpose of flooding a system with so much data that it first slows down, and then times out and is disconnected. The threshold defines the number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Options threshold *number* —Number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Range: 1 through 1,000,000 per second

Default: 1,000 per second



NOTE: For SRX Series devices the applicable range is 1 through 4,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [flood \(Security UDP\) on page 68](#)
- [Security Configuration Statement Hierarchy](#)

flood (Security UDP)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax flood {
 threshold *number*;
}

Hierarchy Level [edit security screen ids-option *screen-name* udp]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the device to detect and prevent UDP floods. UDP flooding occurs when an attacker sends UDP packets to slow down the system to the point that it can no longer process valid connection requests.

The threshold defines the number of UDP packets per second allowed to ping the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options threshold *number* —Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.

Range: 1 through 1,000,000 per second

Default: 1,000 per second



NOTE: For SRX series devices the applicable range is 1 through 4,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)
- [flood \(Security ICMP\) on page 67](#)

icmp (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
icmp {
    flood {
        threshold number;
    }
    fragment;
    icmpv6-malformed;
    ip-sweep {
        threshold number;
    }
    large;
    ping-death;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure ICMP intrusion detection service (IDS) options.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

ids-option

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `ids-option screen-name {
 alarm-without-drop;
 description text;
 icmp {
 flood {
 threshold number;
 }
 fragment;
 icmpv6-malformed;
 ip-sweep {
 threshold number;
 }
 large;
 ping-death;
 }
 ip {
 bad-option;
 block-frag;
 ipv6-extension-header {
 AH-header;
 ESP-header;
 HIP-header;
 destination-header {
 ILNP-nonce-option;
 home-address-option;
 line-identification-option;
 tunnel-encapsulation-limit-option;
 user-defined-option-type low | <to high>;
 }
 fragment-header;
 hop-by-hop-header {
 CALIPSO-option;
 RPL-option;
 SFM-DPD-option;
 jumbo-payload-option;
 quick-start-option;
 router-alert-option;
 user-defined-option-type low | <to high>;
 }
 mobility-header;
 no-next-header;
 routing-header;
 shim6-header;
 user-defined-option-type low | <to high>;
 }
 ipv6-extension-header-limit limit;
 ipv6-malformed-header;
 loose-source-route-option;
 record-route-option;
 security-option;
 source-route-option;`


```

spoofing;
stream-option;
strict-source-route-option;
tear-drop;
timestamp-option;
unknown-protocol;
}
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
tcp {
    fin-no-ack;
    land;
    port-scan {
        threshold number;
    }
    syn-ack-ack-proxy {
        threshold number;
    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
        threshold threshold number;
    }
    winnuke;
}
udp {
    flood {
        threshold number;
    }
    port-scan {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
}
}

```

Hierarchy Level [edit security screen]

Release Information	Statement introduced in Junos OS Release 8.5. Support for the description option added in Junos OS Release 12.1. Support for the port scan for UDP option added in Junos OS Release 12.1X47-D10.
Description	Define screens for intrusion detection service (IDS).
Options	<p>description text—Descriptive text about screen.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Security Configuration Statement Hierarchy</i>

ip (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
ip {
  bad-option;
  block-frag;
  ipv6-extension-header {
    AH-header;
    ESP-header;
    HIP-header;
    destination-header {
      ILNP-nonce-option;
      home-address-option;
      line-identification-option;
      tunnel-encapsulation-limit-option;
      user-defined-option-type low | <to high>;
    }
    fragment-header;
    hop-by-hop-header {
      CALIPSO-option;
      RPL-option;
      SFM-DPD-option;
      jumbo-payload-option;
      quick-start-option;
      router-alert-option;
      user-defined-option-type low | <to high>;
    }
    mobility-header;
    no-next-header;
    routing-header;
    shim6-header
    user-defined-option-type low | <to high>;
  }
  ipv6-extension-header-limit limit;
  ipv6-malformed-header;
  loose-source-route-option;
  record-route-option;
  security-option;
  source-route-option;
  spoofing;
  stream-option;
  strict-source-route-option;
  tear-drop;
  timestamp-option;
  unknown-protocol;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for IPv6 bad-option extension header screens added in Junos OS Release 12.1X46-D10.

Description Configure IP layer IDS options.

- Options**
- **bad-option**—Detect and drop any packet with an incorrectly formatted IP option in the IP packet header. The device records the event in the screen counters list for the ingress interface. This screen option is applicable to IPv4 and IPv6.
 - **block-frag**—Enable IP packet fragmentation blocking.
 - **loose-source-route-option**—Detect packets where the IP option is 3 (loose source routing), and record the event in the screen counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other devices in between those specified. The type 0 routing header of the loose source route option is the only related header defined in IPv6 .
 - **record-route-option**—Detect packets where the IP option is 7 (record route), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **security-option**—Detect packets where the IP option is 2 (security), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **source-route-option**—Detect packets, and record the event in the screen counters list for the ingress interface.
 - **spoofing**—Prevent spoofing attacks. Spoofing attacks occur when unauthorized agents attempt to bypass firewall security by imitating valid client IP addresses. Using the spoofing option invalidates such false source IP address connections.

The default behavior is to base spoofing decisions on individual interfaces.
 - **stream-option**—Detect packets where the IP option is 8 (stream ID), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **strict-source-route-option**—Detect packets where the IP option is 9 (strict source routing), and record the event in the screen counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field. Currently, this screen option is applicable only to IPv4.
 - **tear-drop**—Block the teardrop attack. Teardrop attacks occur when fragmented IP packets overlap and cause the host attempting to reassemble the packets to crash. The teardrop option directs the device to drop any packets that have such a discrepancy.
 - **timestamp-option**—Detect packets where the IP option list includes option 4 (Internet timestamp), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **unknown-protocol**—Discard all received IP frames with protocol numbers greater than 137 for IPv4 and 139 for IPv6. Such protocol numbers are undefined or reserved.

Required Privilege	security—To view this statement in the configuration.
Level	security-control—To add this statement to the configuration.

Related Documentation • [Security Configuration Statement Hierarchy](#)

ip-sweep

Supported Platforms [LN Series, SRX Series](#)

Syntax

```
ip-sweep {
    threshold number;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and prevent an IP Sweep attack. An IP Sweep attack occurs when an attacker sends ICMP echo requests (pings) to multiple destination addresses. If a target host replies, the reply reveals the target's IP address to the attacker. If the device receives 10 ICMP echo requests within the number of microseconds specified in this statement, it flags this as an IP Sweep attack, and rejects the 11th and all further ICMP packets from that host for the remainder of the second.

Options **threshold *number***—Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device. More than 10 requests from a host during this period triggers an IP Sweep attack response on the device during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation • [Security Configuration Statement Hierarchy](#)

land

Supported Platforms	LN Series , SRX Series
Syntax	land;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable prevention of Land attacks by combining the SYN flood defense with IP spoofing protection. Land attacks occur when an attacker sends spoofed IP packets with headers containing the target's IP address for the source and destination IP addresses. The attacker sends these packets with the SYN flag set to any available port. The packets induce the target to create empty sessions with itself, filling its session table and overwhelming its resources.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

limit-session

Supported Platforms	LN Series , SRX Series
Syntax	limit-session { destination-ip-based <i>number</i> ; source-ip-based <i>number</i> ; }
Hierarchy Level	[edit security screen ids-option <i>screen-name</i>]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Limit the number of concurrent sessions the device can initiate from a single source IP address or the number of sessions it can direct to a single destination IP address.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

ping-death

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax ping-death;

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and reject oversized and irregular ICMP packets. Although the TCP/IP specification requires a specific packet size, many ping implementations allow larger packet sizes. Larger packets can trigger a range of adverse system reactions, including crashing, freezing, and restarting.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

port-scan

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
port-scan {  
    threshold number;  
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Prevent port scan attacks. A port scan attack occurs when an attacker sends packets with different port numbers to scan available services. The attack succeeds if a port responds. To prevent this attack, the device internally logs the number of different ports scanned from a single remote source. For example, if a remote host scans 10 ports in 0.005 seconds (equivalent to 5000 microseconds, the default threshold setting), the device flags this behavior as a port scan attack, and rejects further packets from the remote source.

Options **threshold *number*** —Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers. If the number of ports during the threshold period reaches 10 or more, the device rejects additional packets from the source.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)

screen (Security Zones)

Supported Platforms	LN Series, SRX Series
Syntax	screen <i>screen-name</i> ;
Hierarchy Level	[edit security zones functional-zone management], [edit security zones security-zone <i>zone-name</i>]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify a security screen for a security zone.
Options	<i>screen-name</i> —Name of the screen.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> <i>Security Zones and Interfaces Feature Guide for Security Devices</i>

source-ip-based

Supported Platforms	LN Series, SRX Series
Syntax	source-ip-based <i>number</i> ;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> limit-session]
Release Information	Statement modified in Release 9.2 of Junos OS.
Description	Limit the number of concurrent sessions the device can initiate from a single source IP address.
Options	<i>number</i> —Maximum number of concurrent sessions that can be initiated from a source IP address. Range: 1 through 1,000,000 Default: 128



NOTE: For SRX Series devices the applicable range is 1 through 8,000,000.

Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> <i>Security Configuration Statement Hierarchy</i>

source-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `source-threshold number;`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the number of SYN segments that the device can receive per second from a single source IP address (regardless of the destination IP address and port number) before the device begins dropping connection requests from that source.

Options *number* —Number of SYN segments to be received per second before the device starts dropping connection requests.

Range: 4 through 500,000 per second

Default: 4000 per second



NOTE: For SRX Series devices the applicable range is 4 through 1,000,000 per second.

Required Privilege security—To view this statement in the configuration.

Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

syn-ack-ack-proxy

Supported Platforms	LN Series, SRX Series
Syntax	syn-ack-ack-proxy; { threshold <i>number</i> , }
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.
Description	Prevent the SYN-ACK-ACK attack, which occurs when the attacker establishes multiple telnet sessions without allowing each session to terminate. This behavior consumes all open slots, generating a denial-of-service (DoS) condition.
Options	threshold <i>number</i> — Number of connections from any single IP address. Range: 1 through 250,000 Default: 512
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Security Configuration Statement Hierarchy</i>

syn-check-required

Supported Platforms	LN Series, SRX Series
Syntax	syn-check-required;
Hierarchy Level	[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> then permit tcp-options]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Enable sync check per policy. The syn-check-required value overrides the global value no-syn-check.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Security Policies Feature Guide for Security Devices</i>

syn-fin

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax syn-fin;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of an illegal combination of flags that attackers can use to consume sessions on the target device, thus resulting in a denial-of-service (DoS) condition.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

syn-flood

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
syn-flood {
    alarm-threshold number;
    attack-threshold number;
    destination-threshold number;
    source-threshold number;
    timeout seconds;
    white-list name {
        destination-address destination-address;
        source-address source-address;
    }
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure detection and prevention of SYN flood attacks. Such attacks occur when the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses.



NOTE: On all SRX Series devices, the TCP synchronization flood alarm threshold value does not indicate the number of packets dropped, however the value does show the packet information after the alarm threshold has been reached.

The synchronization cookie or proxy never drops packets; therefore the **alarm-without-drop (not drop)** action is shown in the system log.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)

syn-flood-protection-mode

Supported Platforms	LN Series , SRX Series
Syntax	syn-flood-protection-mode (syn-cookie syn-proxy);
Hierarchy Level	[edit security flow]
Release Information	Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.
Description	Enable SYN cookie or SYN proxy defenses against SYN attacks. SYN flood protection mode is enabled globally on the device and is activated when the configured syn-flood attack-threshold value is exceeded.
Options	<ul style="list-style-type: none">• syn-cookie—Uses a cryptographic hash to generate a unique Initial Sequence Number (ISN). This is enabled by default.• syn-proxy—Uses a proxy to handle the SYN attack.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Flow-Based Processing Feature Guide for Security Devices</i>

syn-frag

Supported Platforms	LN Series , SRX Series
Syntax	syn-frag;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of a SYN fragment attack and drops any packet fragments used for the attack. A SYN fragment attack floods the target host with SYN packet fragments. The host caches these fragments, waiting for the remaining fragments to arrive so it can reassemble them. The flood of connections that cannot be completed eventually fills the host's memory buffer. No further connections are possible, and damage to the host's operating system can occur.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

tcp (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
tcp {
  fin-no-ack;
  land;
  port-scan {
    threshold number;
  }
  syn-ack-ack-proxy {
    threshold number;
  }
  syn-fin;
  syn-flood {
    alarm-threshold number;
    attack-threshold number;
    destination-threshold number;
    source-threshold number;
    timeout seconds;
    white-list name {
      destination-address destination-address;
      source-address source-address;
    }
  }
  syn-frag;
  tcp-no-flag;
  tcp-sweep {
    threshold threshold number;
  }
  winnuke;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure TCP-layer intrusion detection service (IDS) options.



NOTE: On all SRX Series devices, the TCP synchronization flood alarm threshold value does not indicate the number of packets dropped, however the value does show the packet information after the alarm threshold has been reached.

The synchronization cookie or proxy never drops packets; therefore the alarm-without-drop (not drop) action is shown in the system log.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

tcp-no-flag

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax tcp-no-flag;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to drop illegal TCP packets with a missing or malformed flag field.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

tcp-sweep

Supported Platforms [LN Series, SRX Series](#)

Syntax

```
tcp-sweep {
    threshold number;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the device to detect and prevent TCP sweep attack. In a TCP sweep attack, an attacker sends TCP SYN packets to the target device as part of the TCP handshake. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends TCP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as a TCP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further TCP packets from that host for the remainder of the specified threshold period.

Options **threshold *number***—Maximum number of microseconds during which up to 10 TCP SYN packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers TCP Sweep attack response on the router during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)

timeout (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `timeout seconds;`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum length of time before a half-completed connection is dropped from the queue. You can decrease the timeout value until you see any connections dropped during normal traffic conditions.

Options ***seconds*** —Time interval before a half-completed connection is dropped from the queue.
Range: 1 through 50 seconds
Default: 20 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

traceoptions (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure screen tracing options.

To specify more than one tracing option, include multiple **flag** statements.

Options

- **file**—Configure the trace file options.

- **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
- **files number**—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10 files

- **match regular-expression**—Refine the output to include lines that contain the regular expression.
- **size maximum-file-size**—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: **x K** to specify KB, **x m** to specify MB, or **x g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
 - **all**—Trace all screen events
 - **configuration**—Trace screen configuration events
 - **flow**—Trace flow events
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>
------------------------------	---

udp (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
udp {
  flood {
    threshold number;
  }
  udp-sweep {
    threshold threshold number;
  }
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the number of packets allowed per second to the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

security—	To view this statement in the configuration.
security-control—	To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

udp-sweep

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
udp-sweep {  
    threshold number;  
}
```

Hierarchy Level [edit security screen ids-option *screen-name* udp]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the device to detect and prevent UDP sweep attack. In a UDP sweep attack, an attacker sends UDP packets to the target device. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends UDP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as an UDP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further UDP packets from that host for the remainder of the specified threshold period.

Options **threshold *number***—Maximum number of microseconds during which up to 10 UDP packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers an UDP Sweep attack response on the device during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)

white-list

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `white-list name {
 destination-address [address];
 source-address [address];
}`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement introduced in Release 12.1 of Junos OS.

Description Configure a whitelist of IP addresses that are to be exempt from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process.

Both IP version 4 (IPv4) and IP version 6 (IPv6) whitelists are supported. Addresses in a whitelist must be all IPv4 or all IPv6. Each whitelist can have up to 32 IP address prefixes.

- Options**
- **destination-address *address***—Destination IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.
 - **source-address *address***—Source IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

winnuke

Supported Platforms [LN Series, SRX Series](#)

Syntax winnuke;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of attacks on Windows NetBios communications. Packets are modified as necessary and passed on. Each WinNuke attack triggers an attack log entry in the event alarm log.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

CHAPTER 3

Administration

- [Operational Commands on page 95](#)

Operational Commands

- [clear security screen statistics](#)
- [clear security screen statistics interface](#)
- [clear security screen statistics zone](#)
- [show security screen ids-option](#)
- [show security screen statistics](#)

clear security screen statistics

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax clear security screen statistics
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 9.0 of Junos OS.

Description Clear intrusion detection service (IDS) security screen statistics on the device.

Options **node**—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.

- **node-id** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level clear

Related Documentation

- [show security screen statistics on page 106](#)

List of Sample Output [clear security screen statistics node 0 on page 96](#)

Output Fields This command produces no output.

Sample Output

[clear security screen statistics node 0](#)

```
user@host> clear security screen statistics node 0
```

clear security screen statistics interface

Supported Platforms	LN Series , SRX Series
Syntax	clear security screen statistics interface <i>interface-name</i>
Release Information	Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS.
Description	Clear intrusion detection service (IDS) security screen statistics for an interface.
Options	<ul style="list-style-type: none"> interface <i>interface-name</i> —Name of the interface on which to clear security screen statistics. node—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node. <ul style="list-style-type: none"> node-id —Identification number of the node. It can be 0 or 1. all —Clear all nodes. local —Clear the local node. primary—Clear the primary node.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> show security screen statistics on page 106
List of Sample Output	clear security screen statistics interface fab0 on page 97 clear security screen statistics interface fab0 node 0 on page 97
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security screen statistics interface fab0

```

user@host> clear security screen statistics interface fab0
node0:
-----
IDS statistics has been cleared.
node1:
-----
IDS statistics has been cleared.
```

Sample Output

clear security screen statistics interface fab0 node 0

```

user@host> clear security screen statistics interface fab0 node 0
node0:
-----
IDS statistics has been cleared.
```


clear security screen statistics zone

Supported Platforms	LN Series , SRX Series
Syntax	clear security screen statistics zone <i>zone-name</i> <node (<i>node-id</i> all local primary)>
Release Information	Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS.
Description	Clear IDS security screen statistics for a security zone.
Options	<ul style="list-style-type: none"> • zone zone-name—Name of the security zone for which to clear security screen statistics. • node—(Optional) For chassis cluster configurations, clear security screen statistics for a security zone on a specific node. <ul style="list-style-type: none"> • <i>node-id</i>—Identification number of the node. It can be 0 or 1. • all—Clear all nodes. • local—Clear the local node. • primary—Clear the primary node.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show security screen statistics on page 106
List of Sample Output	clear security screen statistics zone abc node all on page 99 clear security screen statistics node 0 zone my-zone on page 99
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security screen statistics zone abc node all

```

user@host> clear security screen statistics zone abc node all
node0:
-----
IDS statistics has been cleared.
node1:
-----
IDS statistics has been cleared.
```

Sample Output

clear security screen statistics node 0 zone my-zone

```

user@host> clear security screen statistics node 0 zone my-zone
node0:
-----
IDS statistics has been cleared.
```


show security screen ids-option

Supported Platforms	LN Series , SRX Series
Syntax	show security screen ids-option screen-name <node (<i>node-id</i> all local primary)>
Release Information	Command introduced in Junos OS Release 8.5. Support for node options added in Junos OS Release 9.0. Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10. Support for UDP port scan added in Junos OS Release 12.1X47-D10.
Description	Display configuration information about the specified security screen.
Options	<ul style="list-style-type: none"> • screen-name —Name of the screen. • node—(Optional) For chassis cluster configurations, display the configuration status of the security screen on a specific node. <ul style="list-style-type: none"> • node-id —Identification number of the node. It can be 0 or 1. • all—Display information about all nodes. • local—Display information about the local node. • primary—Display information about the primary node.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • ids-option on page 70
List of Sample Output	show security screen ids-option jscreen on page 103 show security screen ids-option jscreen (IPv6) on page 104 show security screen ids-option jscreen1 node all on page 104
Output Fields	Table 4 on page 101 lists the output fields for the show security screen ids-option command. Output fields are listed in the approximate order in which they appear.

Table 4: show security screen ids-option Output Fields

Field Name	Field Description
TCP address sweep threshold	Number of microseconds for which the device accepts 10 TCP packets from the same remote source to different destination addresses.
TCP port scan threshold	Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers.
ICMP address sweep threshold	Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device.

Table 4: show security screen ids-option Output Fields (*continued*)

Field Name	Field Description
UDP flood threshold	Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.
UDP port scan threshold	Number of microseconds during which the device accepts packets from the same remote source IP with up to 10 different destination port numbers.
TCP winnuke	Enable or disable the detection of TCP WinNuke attacks.
TCP SYN flood attack threshold	Number of SYN packets per second required to trigger the SYN proxy response.
TCP SYN flood alarm threshold	Number of half-complete proxy connections per second at which the device makes entries in the event alarm log.
TCP SYN flood source threshold	Number of SYN segments to be received per second before the device begins dropping connection requests.
TCP SYN flood destination threshold	Number of SYN segments received per second before the device begins dropping connection requests.
TCP SYN flood timeout	Maximum length of time before a half-completed connection is dropped from the queue.
TCP SYN flood queue size	Number of proxy connection requests that can be held in the proxy connection queue before the device begins rejecting new connection requests.
ICMP large packet	Enable or disable the detection of any ICMP frame with an IP length greater than 1024 bytes.
UDP address sweep threshold	Number of microseconds for which the device accepts 10 UDP packets from the same remote source to different destination addresses.
IPv6 extension routing	Enable or disable the IPv6 extension routing screen option.
IPv6 extension shim6	Enable or disable the IPv6 extension shim6 screen option.
IPv6 extension fragment	Enable or disable the IPv6 extension fragment screen option.
IPv6 extension AH	Enable or disable the IPv6 extension Authentication Header Protocol screen option.
IPv6 extension ESP	Enable or disable the IPv6 extension Encapsulating Security Payload screen option.
IPv6 extension mobility	Enable or disable the IPv6 extension mobility screen option.
IPv6 extension HIP	Enable or disable the IPv6 extension Host Identify Protocol screen option.
IPv6 extension no next	Enable or disable the IPv6 extension no-next screen option.
IPv6 extension user-defined	Enable or disable the IPv6 extension user-defined screen option.

Table 4: show security screen ids-option Output Fields (*continued*)

Field Name	Field Description
IPv6 extension HbyH jumbo	Enable or disable the IPv6 extension HbyH jumbo screen option.
IPv6 extension HbyH RPL	Enable or disable the IPv6 extension HbyH RPL screen option.
IPv6 extension HbyH router alert	Enable or disable the IPv6 extension HbyH router screen option.
IPv6 extension HbyH quick start	Enable or disable the IPv6 extension HbyH quick-start screen option.
IPv6 extension HbyH CALIPSO	Enable or disable the IPv6 extension HbyH Common Architecture Label IPv6 Security Screen option.
IPv6 extension HbyH SMF DPD	Enable or disable the IPv6 extension HbyH Simplified Multicast Forwarding IPv6 Duplicate Packet Detection screen option.
IPv6 extension HbyH user-defined	Enable or disable the IPv6 extension HbyH user-defined screen option.
IPv6 extension Dst tunnel encap limit	Enable or disable the IPv6 extension distributed (network) storage tunnel encapsulation limit screen option.
IPv6 extension Dst home address	Enable or disable the IPv6 extension DST home address screen option.
IPv6 extension Dst ILNP nonce	Enable or disable the IPv6 extension DST Identifier-Locator Network Protocol nonce screen option.
IPv6 extension Dst line-id	Enable or disable the IPv6 extension DST line-ID screen option.
IPv6 extension Dst user-defined	Enable or disable the IPv6 extension DST user-defined screen option.
IPv6 extension header limit	Threshold for the number of IPv6 extension headers that can pass through the screen.
IPv6 malformed header	Enable or disable the IPv6 malformed header screen option.
ICMPv6 malformed header	Enable or disable the ICMPv6 malformed packet screen option.

Sample Output

show security screen ids-option jscreen

```

user@host> show security screen ids-option jscreen
Screen object status:
Name                                     Value
TCP port scan threshold                 5000
UDP port scan threshold                 10000
ICMP address sweep threshold            5000

```

Sample Output

show security screen ids-option jscreen (IPv6)

```
user@host> show security screen ids-option jscreen
```

```
Screen object status:
```

Name	Value
ICMP ping of death	enabled
.....	
IPv6 extension routing	enabled
IPv6 extension shim6	enabled
IPv6 extension fragment	enabled
IPv6 extension AH	enabled
IPv6 extension ESP	enabled
IPv6 extension mobility	enabled
IPv6 extension HIP	enabled
IPv6 extension no next	enabled
IPv6 extension user-defined	enabled
IPv6 extension HbyH jumbo	enabled
IPv6 extension HbyH RPL	enabled
IPv6 extension HbyH router alert	enabled
IPv6 extension HbyH quick start	enabled
IPv6 extension HbyH CALIPSO	enabled
IPv6 extension HbyH SMF DPD	enabled
IPv6 extension HbyH user-defined	enabled
IPv6 extension Dst tunnel encap limit	enabled
IPv6 extension Dst home address	enabled
IPv6 extension Dst ILNP nonce	enabled
IPv6 extension Dst line-id	enabled
IPv6 extension Dst user-defined	enabled
IPv6 extension header limit	20
IPv6 Malformed header	enabled
ICMPv6 malformed packet	enabled

Sample Output

show security screen ids-option jscreen1 node all

```
user@host> show security screen ids-option jscreen1 node all
```

```
node0:
```

```
-----  
Screen object status:
```

Name	Value
UDP flood threshold	1000
TCP winnuke	enabled
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	4000
TCP SYN flood destination threshold	4000
TCP SYN flood timeout	20
TCP SYN flood queue size	1024
ICMP large packet	enabled

```
node1:
```

```
-----  
Screen object status:
```

Name	Value
UDP flood threshold	1000

TCP winnuke	enabled
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	4000
TCP SYN flood destination threshold	4000
TCP SYN flood timeout	20
TCP SYN flood queue size	1024
ICMP large packet	enabled

show security screen statistics

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `show security screen statistics (zone zone-name | interface interface-name)
<logical-system (logical-system-name | all)>
<node (node-id | all | local | primary)>
<root-logical-system>`

Release Information Command introduced in Release 8.5 of Junos OS. **node** options added in Release 9.0 of Junos OS. **logical-system all** option added in Junos OS Release 11.2R6. Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10.

Description Display intrusion detection service (IDS) security screen statistics.

- Options**
- **zone *zone-name***—Display screen statistics for this security zone.
 - **interface *interface-name***—Display screen statistics for this interface.
 - **logical-system**—(Optional) Display screen statistics for configured logical systems.
 - ***logical-system-name***—Display screen statistics for the named logical system.
 - **all**—Display screen statistics for all logical systems, including the master (root) logical system.
 - **node**—(Optional) For chassis cluster configurations, display screen statistics on a specific node.
 - ***node-id***—Identification number of a node. It can be 0 or 1.
 - **all**—Display information about all nodes.
 - **local**—Display information about the local node.
 - **primary**—Display information about the primary node.
 - **root-logical-system**—(Optional) Display screen statistics for the master logical system only.

Required Privilege Level view

- Related Documentation**
- [clear security screen statistics on page 96](#)
 - [clear security screen statistics interface on page 97](#)
 - [clear security screen statistics zone on page 99](#)
 - [Junos OS Logical Systems Library for Security Devices](#)

List of Sample Output [show security screen statistics zone scrzone on page 109](#)
[show security screen statistics zone untrust \(IPv6\) on page 109](#)
[show security screen statistics interface ge-0/0/3 on page 110](#)
[show security screen statistics interface ge-0/0/1 \(IPv6\) on page 110](#)

[show security screen statistics interface ge-0/0/1 node primary on page 111](#)
[show security screen statistics zone trust logical-system all on page 111](#)

Output Fields [Table 5 on page 107](#) lists the output fields for the **show security screen statistics** command. Output fields are listed in the approximate order in which they appear.

Table 5: show security screen statistics Output Fields

Field Name	Field Description
ICMP flood	Internet Control Message Protocol (ICMP) flood counter. An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
UDP flood	User Datagram Protocol (UDP) flood counter. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks. WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP port scan	Number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP address sweep	Number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.
IP tear drop	Number of teardrop attacks. Teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN flood	Number of TCP SYN attacks.
IP spoofing	Number of IP spoofs. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP ping of death	ICMP ping of death counter. Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP source route option	Number of IP source route attacks.
TCP address sweep	Number of TCP address sweeps.
TCP land attack	Number of land attacks. Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN fragment	Number of TCP SYN fragments.
TCP no flag	Number of TCP headers without flags set. A normal TCP segment header has at least one control flag set.
IP unknown protocol	Number of IPs.
IP bad options	Number of invalid options.

Table 5: show security screen statistics Output Fields (*continued*)

Field Name	Field Description
IP record route option	Number of packets with the IP record route option enabled. This option records the IP addresses of the network devices along the path that the IP packet travels.
IP timestamp option	Number of IP timestamp option attacks. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
IP security option	Number of IP security option attacks.
IP loose source route option	Number of IP loose source route option attacks. This option specifies a partial route list for a packet to take on its journey from source to destination.
IP strict source route option	Number of IP strict source route option attacks. This option specifies the complete route list for a packet to take on its journey from source to destination.
IP stream option	Number of stream option attacks. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.
ICMP fragment	Number of ICMP fragments. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP large packet	Number of large ICMP packets.
TCP SYN FIN	Number of TCP SYN FIN packets.
TCP FIN no ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.
Source session limit	Number of concurrent sessions that can be initiated from a source IP address.
TCP SYN-ACK-ACK proxy	Number of TCP flags enabled with SYN-ACK-ACK. To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold and SRX Series devices running Junos OS reject further connection requests from that IP address.
IP block fragment	Number of IP block fragments.
Destination session limit	Number of concurrent sessions that can be directed to a single destination IP address.
UDP address sweep	Number of UDP address sweeps.
IPv6 extension header	Number of packets filtered for the defined IPv6 extension headers.
IPv6 extension hop by hop option	Number of packets filtered for the defined IPv6 hop-by-hop option types.
IPv6 extension destination option	Number of packets filtered for the defined IPv6 destination option types.
IPv6 extension header limit	Number of packets filtered for crossing the defined IPv6 extension header limit.

Table 5: show security screen statistics Output Fields (*continued*)

IPv6 malformed header	Number of IPv6 malformed headers defined for the intrusion detection service (IDS).
ICMPv6 malformed packet	Number of ICMPv6 malformed packets defined for the IDS options.

Sample Output

show security screen statistics zone scrzone

```

user@host> show security screen statistics zone scrzone
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                   0
UDP flood                                    0
TCP winnuke                                  0
TCP port scan                               91
ICMP address sweep                           0
TCP sweep                                    0
UDP sweep                                    0
IP tear drop                                 0
TCP SYN flood                                0
IP spoofing                                  0
ICMP ping of death                           0
IP source route option                       0
TCP land attack                              0
TCP SYN fragment                             0
TCP no flag                                  0
IP unknown protocol                          0
IP bad options                               0
IP record route option                       0
IP timestamp option                          0
IP security option                           0
IP loose source route option                 0
IP strict source route option                0
IP stream option                             0
ICMP fragment                               0
ICMP large packet                            0
TCP SYN FIN                                  0
TCP FIN no ACK                               0
Source session limit                         0
TCP SYN-ACK-ACK proxy                        0
IP block fragment                            0
Destination session limit                    0

```

Sample Output

show security screen statistics zone untrust (IPv6)

```

user@host> show security screen statistics zone untrust
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                   0
UDP flood                                    0
TCP winnuke                                  0
.....
IPv6 extension header                        0
IPv6 extension hop by hop option             0

```

IPv6	extension destination option	0
IPv6	extension header limit	0
IPv6	malformed header	0
ICMPv6	malformed packet	0

Sample Output

show security screen statistics interface ge-0/0/3

```
user@host> show security screen statistics interface ge-0/0/3
Screen statistics:
IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
TCP winnuke               0
TCP port scan             91
ICMP address sweep        0
TCP sweep                 0
UDP sweep                 0
IP tear drop              0
TCP SYN flood             0
IP spoofing               0
ICMP ping of death        0
IP source route option    0
TCP land attack           0
TCP SYN fragment          0
TCP no flag               0
IP unknown protocol       0
IP bad options            0
IP record route option    0
IP timestamp option       0
IP security option        0
IP loose source route option 0
IP strict source route option 0
IP stream option          0
ICMP fragment             0
ICMP large packet         0
TCP SYN FIN               0
TCP FIN no ACK            0
Source session limit      0
TCP SYN-ACK-ACK proxy     0
IP block fragment         0
Destination session limit 0
```

Sample Output

show security screen statistics interface ge-0/0/1 (IPv6)

```
user@host> show security screen statistics interface ge-0/0/1
Screen statistics:
IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
.....
IPv6 extension header      0
IPv6 extension hop by hop option 0
IPv6 extension destination option 0
IPv6 extension header limit 0
```


IPv6 malformed header	0
ICMPv6 malformed packet	0

Sample Output

show security screen statistics interface ge-0/0/1 node primary

```
user@host> show security screen statistics interface ge-0/0/1 node primary
node0:
```

```
-----
Screen statistics:
IDS attack type      Statistics
ICMP flood           1
UDP flood            1
TCP winnuke          1
TCP port scan        1
ICMP address sweep   1
TCP sweep            1
UDP sweep            1
IP tear drop         1
TCP SYN flood        1
IP spoofing          1
ICMP ping of death   1
IP source route option 1
TCP land attack      1
TCP SYN fragment     1
TCP no flag          1
IP unknown protocol  1
IP bad options        1
IP record route option 1
IP timestamp option  1
IP security option    1
IP loose source route option 1
IP strict source route option 1
IP stream option     1
ICMP fragment        1
ICMP large packet     1
TCP SYN FIN          1
TCP FIN no ACK        1
Source session limit  1
TCP SYN-ACK-ACK proxy 1
IP block fragment     1
Destination session limit 1
```

Sample Output

show security screen statistics zone trust logical-system all

```
user@host> show security screen statistics zone trust logical-system all
Logical system: root-logical-system
Screen statistics:
```

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0

TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls1

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls2

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuker	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

PART 2

Reconnaissance Deterrence Feature Guide for Security Devices

- [Overview on page 117](#)
- [Configuration on page 137](#)
- [Administration on page 195](#)

CHAPTER 4

Overview

- [Attack Detection and Prevention on page 117](#)
- [IP Address and Port Options on page 118](#)
- [System Probes and Flag Set on page 125](#)
- [Attacker Evasion Techniques on page 128](#)

Attack Detection and Prevention

- [Attack Detection and Prevention Overview on page 117](#)

Attack Detection and Prevention Overview

Supported Platforms [LN Series](#), [SRX Series](#)

The Juniper Networks Intrusion Detection and Prevention (IDP) feature, also known as a *stateful firewall*, detects and prevents attacks in network traffic.

An exploit can be either an information-gathering probe or an attack to compromise, disable, or harm a network or network resource. In some cases, the distinction between the two objectives of an exploit can be unclear. For example, a barrage of TCP SYN segments might be an IP address sweep with the intent of triggering responses from active hosts, or it might be a SYN flood attack with the intent of overwhelming a network so that it can no longer function properly. Furthermore, because an attacker usually precedes an attack by performing reconnaissance on the target, we can consider information-gathering efforts as a precursor to an impending attack—that is, they constitute the first stage of an attack. Thus, the term *exploit* encompasses both reconnaissance and attack activities, and the distinction between the two is not always clear.

Juniper Networks provides various detection and defense mechanisms at the zone and policy levels to combat exploits at all stages of their execution:

- Screen options at the zone level.
- Firewall policies at the inter-, intra-, and super-zone policy levels (*super-zone* here means in global policies, where no security zones are referenced).

To secure all connection attempts, Junos OS uses a dynamic packet-filtering method known as stateful inspection. Using this method, Junos OS identifies various components

in the IP packet and TCP segment headers—source and destination IP addresses, source and destination port numbers, and packet sequence numbers—and maintains the state of each TCP session and pseudo UDP session traversing the firewall. (Junos OS also modifies session states based on changing elements such as dynamic port changes or session termination.) When a responding TCP packet arrives, Junos OS compares the information reported in its header with the state of its associated session stored in the inspection table. If they match, the responding packet is allowed to pass the firewall. If the two do not match, the packet is dropped.

Junos OS screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone. Junos OS then applies firewall policies, which can contain content filtering and IDP components, to the traffic that passes the screen filters.

Related Documentation

- [Denial-of-Service Attacks Feature Guide for Security Devices](#)

IP Address and Port Options

- [Reconnaissance Deterrence Overview on page 118](#)
- [Understanding IP Address Sweeps on page 118](#)
- [Understanding TCP Port Scanning on page 119](#)
- [Understanding UDP Port Scanning on page 120](#)
- [Understanding Network Reconnaissance Using IP Options on page 121](#)
- [Understanding Domain Name System Resolve on page 124](#)

Reconnaissance Deterrence Overview

Supported Platforms [LN Series, SRX Series](#)

Attackers can better plan their attack when they first know the layout of the targeted network (which IP addresses have active hosts), the possible entry points (which port numbers are active on the active hosts), and the constitution of their victims (which operating system the active hosts are running). To gain this information, attackers must perform reconnaissance.

Juniper Networks provides several screen options for deterring attackers' reconnaissance efforts and thereby hindering them from obtaining valuable information about the protected network and network resources.

Related Documentation

- [Understanding Network Reconnaissance Using IP Options on page 121](#)

Understanding IP Address Sweeps

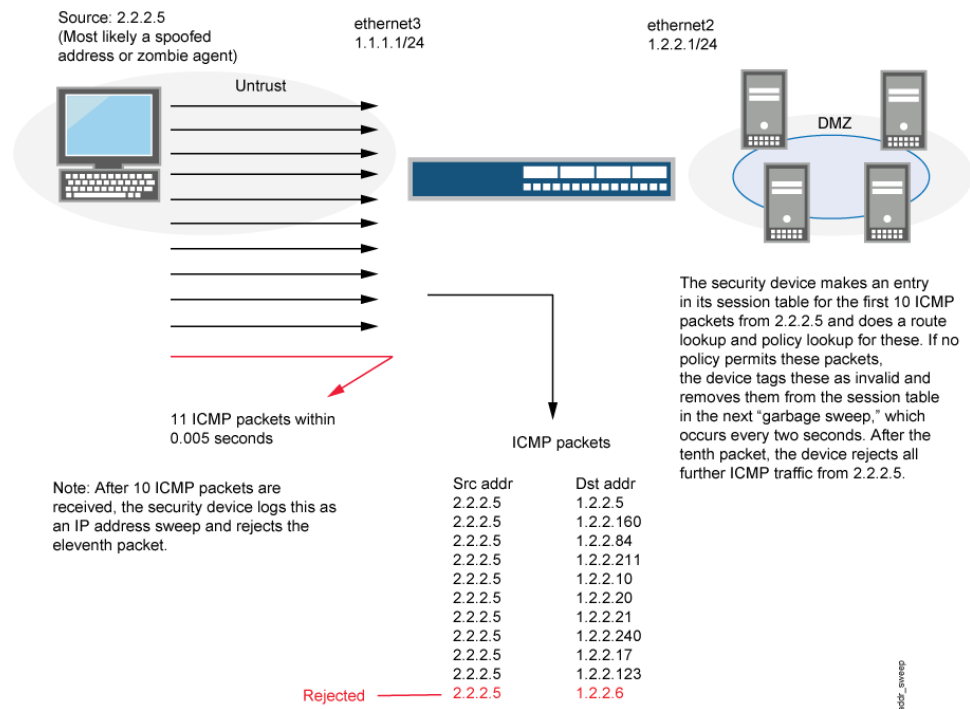
Supported Platforms [LN Series, SRX Series](#)

An address sweep occurs when one source IP address sends a defined number of ICMP packets sent to different hosts within a defined interval (5000 microseconds is the

default). The purpose of this attack is to send ICMP packets—typically echo requests—to various hosts in the hopes that at least one replies, thus uncovering an address to target.

Junos OS internally logs the number of ICMP packets to different addresses from one remote source. Using the default settings, if a remote host sends ICMP traffic to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as an address sweep attack and rejects all further ICMP packets from that host for the remainder of the specified threshold time period. See [Figure 15 on page 119](#).

Figure 15: Address Sweep



Consider enabling this screen option for a security zone only if there is a policy permitting ICMP traffic from that zone. Otherwise, you do not need to enable the screen option. The lack of such a policy denies all ICMP traffic from that zone, precluding an attacker from successfully performing an IP address sweep anyway.



NOTE: Junos OS supports this screen option for ICMPv6 traffic also.

Related Documentation

- [Reconnaissance Deterrence Overview on page 118](#)

Understanding TCP Port Scanning

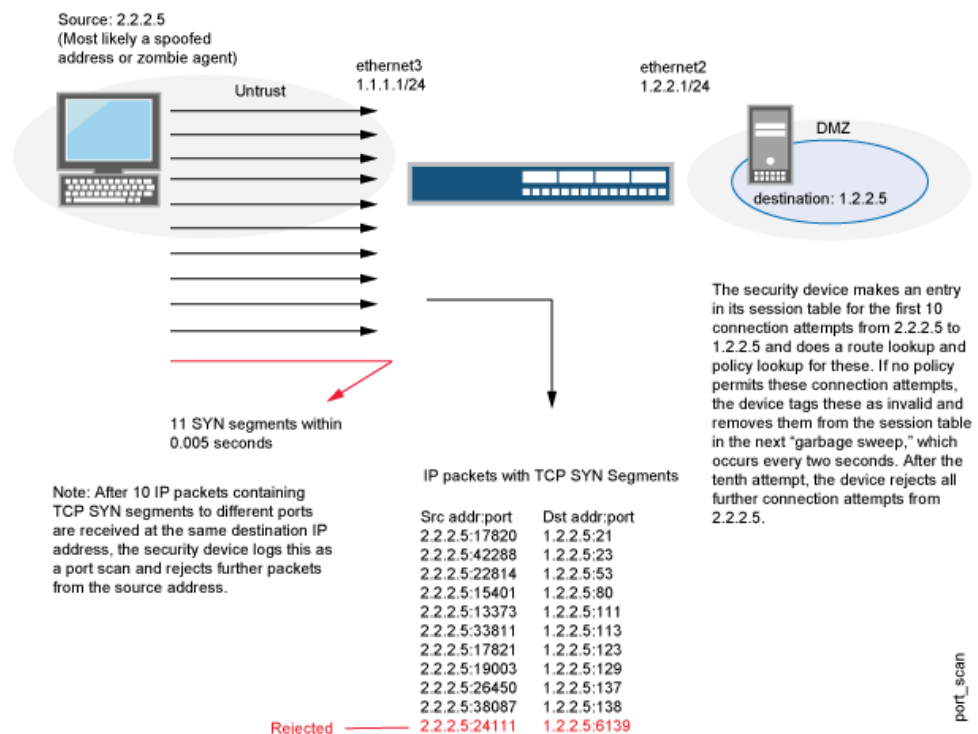
Supported Platforms [LN Series](#), [SRX Series](#)

A port scan occurs when one source IP address sends IP packets containing TCP SYN segments to 10 different destination ports within a defined interval (5000 microseconds).

is the default). The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.

Junos OS internally logs the number of different ports scanned from one remote source. Using the default settings, if a remote host scans 10 ports in 0.005 seconds (5000 microseconds), then the device flags this as a port scan attack and rejects all further packets from the remote source, regardless of the destination IP address, for the remainder of the specified timeout period. See [Figure 16 on page 120](#).

Figure 16: Port Scan



NOTE: Junos OS supports port scanning for both IPv4 and IPv6 traffic.

Related Documentation

- [Reconnaissance Deterrence Overview on page 118](#)

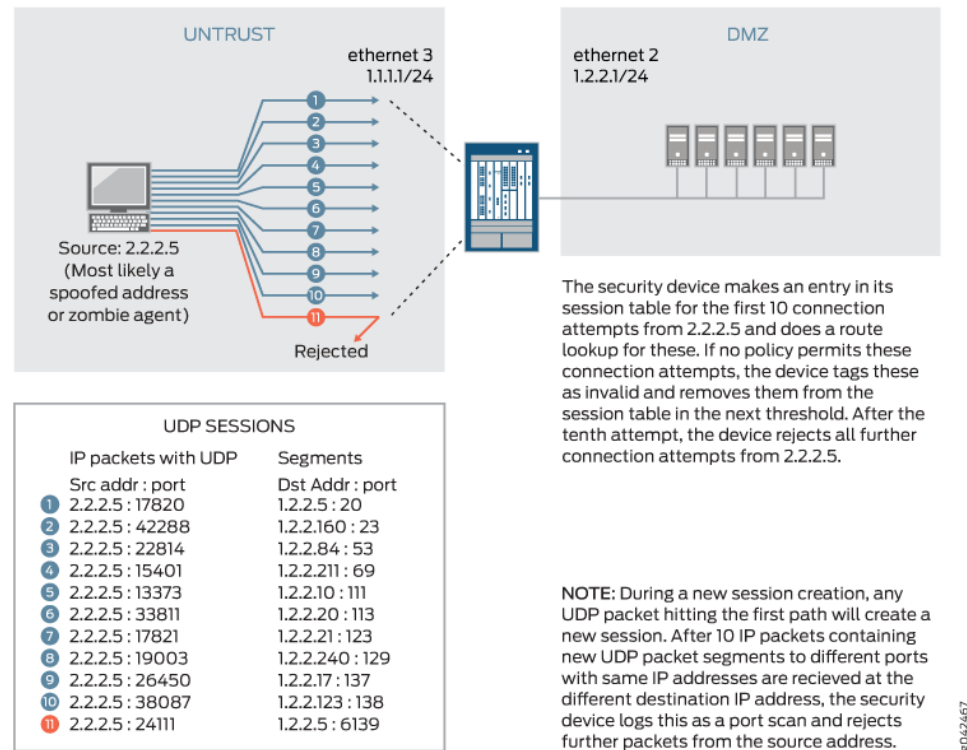
Understanding UDP Port Scanning

Supported Platforms [LN Series](#), [SRX Series](#)

UDP port scan gives statistical information on a session threshold. As the incoming packets traverse the screen, the sessions are established. The number of sessions threshold enforced is based on zone, source IP, and the threshold period and does not allow more than 10 new sessions in the configured threshold period, for each zone and source IP address. The UDP port scan is disabled by default. When the UDP port scan is enabled, the default threshold period is 5000 microseconds. This value can be manually

set to a range of 1000-1,000,000 microseconds. This feature protects some exposed public UDP services against DDoS attacks. See [Figure 17 on page 121](#)

Figure 17: UDP Port Scan



Related Documentation • [Reconnaissance Deterrence Overview on page 118](#)

Understanding Network Reconnaissance Using IP Options

Supported Platforms LN Series, SRX Series

The IP standard RFC 791, *Internet Protocol*, specifies a set of options for providing special routing controls, diagnostic tools, and security.

RFC 791 states that these options are “unnecessary for the most common communications” and, in reality, they rarely appear in IP packet headers. These options appear after the destination address in an IP packet header, as shown in [Figure 18 on page 122](#). When they do appear, they are frequently being put to some illegitimate use.

Figure 18: Routing Options

Version	Header	Type of Service	Total Packet Length (in Bytes)			
Identification			O	D	M	Fragment Offset
Time to Live (TTL)	Protocol		Header Checksum			
Source Address						
Destination Address						
Options						
Payload						

g030807

This topic contains the following sections:

- [Uses for IP Packet Header Options on page 122](#)
- [Screen Options for Detecting IP Options Used for Reconnaissance on page 124](#)

Uses for IP Packet Header Options

Table 6 on page 122 lists the IP options and their accompanying attributes.

Table 6: IP Options and Attributes

Type	Class	Number	Length	Intended Use	Nefarious Use
End of Options	0*	0	0	Indicates the end of one or more IP options.	None.
No Options	0	1	0	Indicates there are no IP options in the header.	None.
Security	0	2	11 bits	Provides a way for hosts to send security, TCC (closed user group) parameters, and Handling Restriction Codes compatible with Department of Defense (DoD) requirements. (This option, as specified in RFC 791, <i>Internet Protocol</i> , and RFC 1038, <i>Revised IP Security Option</i> , is obsolete.) Currently, this screen option is applicable only to IPv4.	Unknown. However, because it is obsolete, its presence in an IP header is suspect.
Loose Source Route	0	3	Varies	Specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other devices in between those specified.	Evasion. The attacker can use the specified routes to hide the true source of a packet or to gain access to a protected network.

Table 6: IP Options and Attributes (*continued*)

Type	Class	Number	Length	Intended Use	Nefarious Use
Record Route	0	7	Varies	<p>Records the IP addresses of the network devices along the path that the IP packet travels. The destination machine can then extract and process the route information. (Due to the size limitation of 40 bytes for both the option and storage space, this can only record up to 9 IP addresses.)</p> <p>Currently, this screen option is applicable only to IPv4.</p>	Reconnaissance. If the destination host is a compromised machine in the attacker's control, he or she can glean information about the topology and addressing scheme of the network through which the packet passed.
Stream ID	0	8	4 bits	<p>(Obsolete) Provided a way for the 16-bit SATNET stream identifier to be carried through networks that did not support the stream concept.</p> <p>Currently, this screen option is applicable only to IPv4.</p>	Unknown. However, because it is obsolete, its presence in an IP header is suspect.
Strict Source Route	0	9	Varies	<p>Specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field.</p> <p>Currently, this screen option is applicable only to IPv4.</p>	Evasion. An attacker can use the specified routes to hide the true source of a packet or to gain access to a protected network.
Timestamp	2**	4		<p>Records the time (in coordinated universal time [UTC]***) when each network device receives the packet during its trip from the point of origin to its destination. The network devices are identified by IP address.</p> <p>This option develops a list of IP addresses of the devices along the path of the packet and the duration of transmission between each one.</p> <p>Currently, this screen option is applicable only to IPv4.</p>	Reconnaissance. If the destination host is a compromised machine in the attacker's control, he or she can glean information about the topology and addressing scheme of the network through which the packet has passed.

* The class of options identified as 0 was designed to provide extra packet or network control.

** The class of options identified as 2 was designed for diagnostics, debugging, and measurement.

*** The timestamp uses the number of milliseconds since midnight UTC. UTC is also known as Greenwich Mean Time (GMT), which is the basis for the international time standard.

Screen Options for Detecting IP Options Used for Reconnaissance

The following screen options detect IP options that an attacker can use for reconnaissance or for some unknown but suspect purpose:

- **Record Route**—Junos OS detects packets where the IP option is 7 (record route) and records the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **Timestamp**—Junos OS detects packets where the IP option list includes option 4 (Internet timestamp) and records the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **Security**—Junos OS detects packets where the IP option is 2 (security) and records the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **Stream ID**—Junos OS detects packets where the IP option is 8 (stream ID) and records the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.

If a packet with any of the previous IP options is received, Junos OS flags this as a network reconnaissance attack and records the event for the ingress interface.

Related Documentation

- [Reconnaissance Deterrence Overview on page 118](#)

Understanding Domain Name System Resolve

Supported Platforms [LN Series](#), [SRX Series](#)

Prior to Junos OS Release 12.1X47, DNS resolution was performed with only UDP as a transport. Messages carried by UDP are restricted to 512 bytes; longer messages are truncated and the traffic class (TC) bit is set in the header. The maximum length of UDP DNS response messages is 512 bytes, but the maximum length of TCP DNS response messages is 65,535 bytes. A DNS resolver knows whether the response is complete if the TC bit is set in the header. Hence, a TCP DNS response can carry more information than a UDP DNS response.

There are three types of DNS resolve behaviors:

- UDP DNS resolve
- TCP DNS resolve
- UDP/TCP DNS resolve



NOTE: A policy uses UDP/TCP DNS resolve to resolve IP addresses. In UDP/TCP DNS resolve, UDP DNS resolve is first used, and when it gets truncated TCP DNS resolve is used.



NOTE: A Routing Engine policy supports a maximum of 1024 IPv4 address prefixes and 256 IPv6 address prefixes that can be sent to the PFE. If the maximum number of IPv4 or IPv6 address prefixes exceeds the limits, the addresses over the limitations will not be sent to the PFE and a syslog message is generated. The maximum number of addresses in a TCP DNS response is 4094 for IPv4 addresses and 2340 for IPv6 addresses, but only 1024 IPv4 addresses and 256 IPv6 addresses are loaded to the PFE.

Related Documentation

- [Reconnaissance Deterrence Overview on page 118](#)

System Probes and Flag Set

- [Reconnaissance Deterrence Overview on page 125](#)
- [Understanding Operating System Probes on page 125](#)
- [Understanding TCP Headers with SYN and FIN Flags Set on page 126](#)
- [Understanding TCP Headers With FIN Flag Set and Without ACK Flag Set on page 126](#)
- [Understanding TCP Header with No Flags Set on page 127](#)

Reconnaissance Deterrence Overview

Supported Platforms [LN Series, SRX Series](#)

Attackers can better plan their attack when they first know the layout of the targeted network (which IP addresses have active hosts), the possible entry points (which port numbers are active on the active hosts), and the constitution of their victims (which operating system the active hosts are running). To gain this information, attackers must perform reconnaissance.

Juniper Networks provides several screen options for deterring attackers' reconnaissance efforts and thereby hindering them from obtaining valuable information about the protected network and network resources.

Related Documentation

- [Understanding Network Reconnaissance Using IP Options on page 121](#)

Understanding Operating System Probes

Supported Platforms [LN Series, SRX Series](#)

Before launching an exploit, attackers might try to probe the targeted host to learn its operating system (OS). With that knowledge, they can better decide which attack to launch and which vulnerabilities to exploit. Junos OS can block reconnaissance probes commonly used to gather information about OS types.

Related Documentation

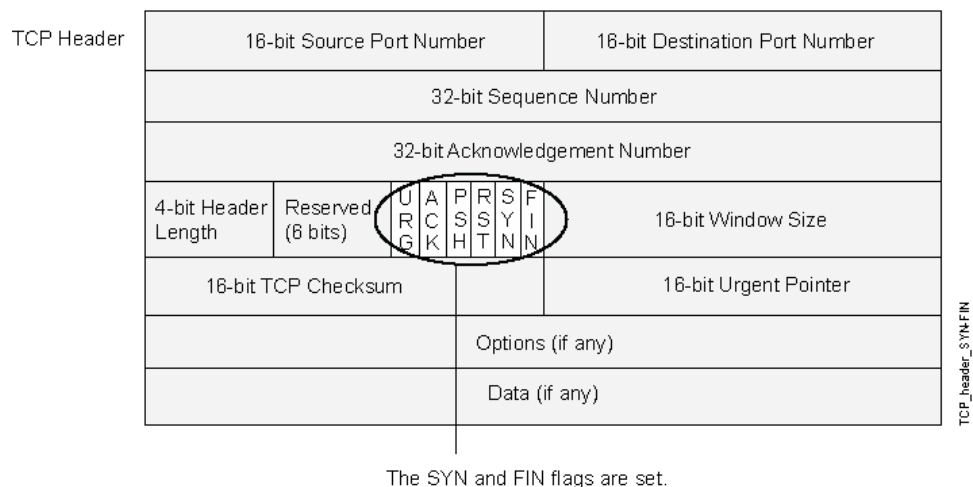
- [Reconnaissance Deterrence Overview on page 118](#)

Understanding TCP Headers with SYN and FIN Flags Set

Supported Platforms [LN Series](#), [SRX Series](#)

Both the SYN and FIN control flags are not normally set in the same TCP segment header. The SYN flag synchronizes sequence numbers to initiate a TCP connection. The FIN flag indicates the end of data transmission to finish a TCP connection. Their purposes are mutually exclusive. A TCP header with the SYN and FIN flags set is anomalous TCP behavior, causing various responses from the recipient, depending on the OS. See [Figure 19 on page 126](#).

Figure 19: TCP Header with SYN and FIN Flags Set



An attacker can send a segment with both flags set to see what kind of system reply is returned and thereby determine what kind of OS is on the receiving end. The attacker can then use any known system vulnerabilities for further attacks.

When you enable this screen option, Junos OS checks if the SYN and FIN flags are set in TCP headers. If it discovers such a header, it drops the packet.



NOTE: Junos OS supports TCP header with SYN and FIN flags set protection for both IPv4 and IPv6 traffic.

Related Documentation

- [Reconnaissance Deterrence Overview on page 118](#)

Understanding TCP Headers With FIN Flag Set and Without ACK Flag Set

Supported Platforms [LN Series](#), [SRX Series](#)

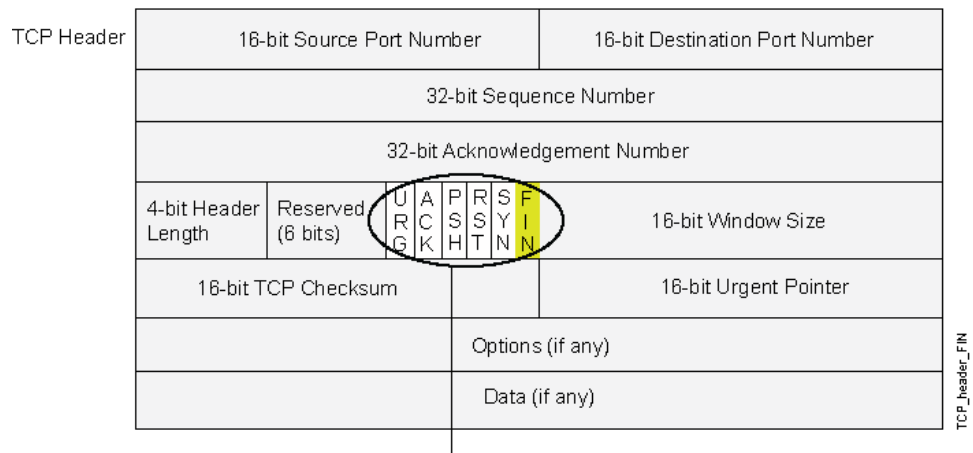
[Figure 20 on page 127](#) shows TCP segments with the FIN control flag set (to signal the conclusion of a session and terminate the connection). Normally, TCP segments with the FIN flag set also have the ACK flag set (to acknowledge the previous packet received).

Because a TCP header with the FIN flag set but not the ACK flag is anomalous TCP behavior, there is no uniform response to this. The OS might respond by sending a TCP segment with the RST flag set. Another might completely ignore it. The victim's response can provide the attacker with a clue as to its OS. (Other purposes for sending a TCP segment with the FIN flag set are to evade detection while performing address and port scans and to evade defenses on guard for a SYN flood by performing a FIN flood instead.)



NOTE: Vendors have interpreted RFC 793, *Transmission Control Protocol*, variously when designing their TCP/IP implementations. When a TCP segment arrives with the FIN flag set but not the ACK flag, some implementations send RST segments, while others drop the packet without sending an RST.

Figure 20: TCP Header with FIN Flag Set



Only the FIN flag is set.

When you enable this screen option, Junos OS checks if the FIN flag is set but not the ACK flag in TCP headers. If it discovers a packet with such a header, it drops the packet.



NOTE: Junos OS supports TCP header with SYN and FIN flags set protection for both IPv4 and Ipv6 traffic.

Related Documentation

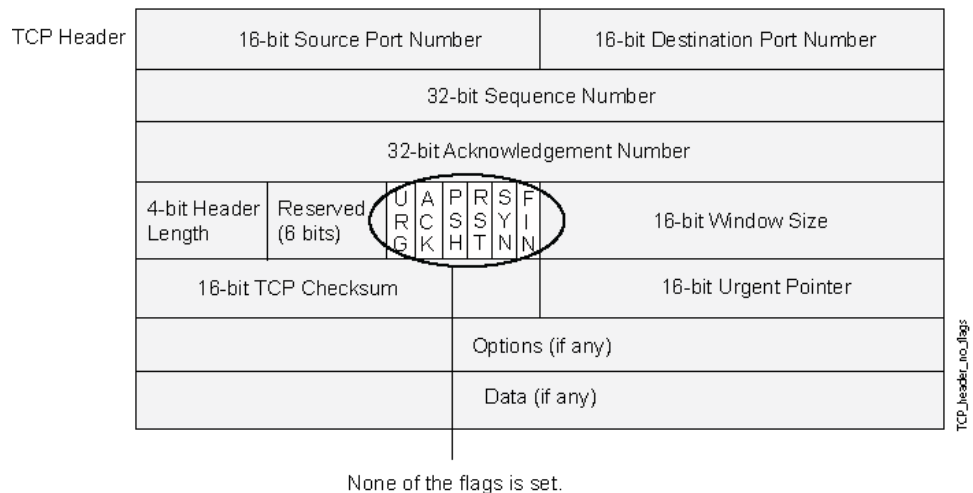
- [Reconnaissance Deterrence Overview on page 118](#)

Understanding TCP Header with No Flags Set

Supported Platforms [LN Series](#), [SRX Series](#)

A normal TCP segment header has at least one flag control set. A TCP segment with no control flags set is an anomalous event. Because different operating systems respond differently to such anomalies, the response (or lack of response) from the targeted device can provide a clue as to the type of OS it is running. See [Figure 21 on page 128](#).

Figure 21: TCP Header with No Flags Set



When you enable the device to detect TCP segment headers with no flags set, the device drops all TCP packets with a missing or malformed flags field.



NOTE: Junos OS supports TCP header with no flags set protection for both IPv4 and IPv6 traffic.

Related Documentation

- [Reconnaissance Deterrence Overview on page 118](#)

Attacker Evasion Techniques

- [Reconnaissance Deterrence Overview on page 128](#)
- [Understanding Attacker Evasion Techniques on page 129](#)
- [Understanding FIN Scans on page 129](#)
- [Understanding TCP SYN Checking on page 129](#)
- [Understanding IP Spoofing on page 131](#)
- [Understanding IP Spoofing in Layer 2 Transparent Mode on page 132](#)
- [Understanding IP Source Route Options on page 133](#)

Reconnaissance Deterrence Overview

Supported Platforms [LN Series](#), [SRX Series](#)

Attackers can better plan their attack when they first know the layout of the targeted network (which IP addresses have active hosts), the possible entry points (which port numbers are active on the active hosts), and the constitution of their victims (which operating system the active hosts are running). To gain this information, attackers must perform reconnaissance.

Juniper Networks provides several screen options for deterring attackers' reconnaissance efforts and thereby hindering them from obtaining valuable information about the protected network and network resources.

- Related Documentation**
- [Understanding Network Reconnaissance Using IP Options on page 121](#)

Understanding Attacker Evasion Techniques

Supported Platforms [LN Series, SRX Series](#)

Whether gathering information or launching an attack, it is generally expected that the attacker avoids detection. Although some IP address and port scans are blatant and easily detectable, more wily attackers use a variety of means to conceal their activity. Techniques such as using FIN scans instead of SYN scans—which attackers know most firewalls and intrusion detection programs detect—indicate an evolution of reconnaissance and exploit techniques for evading detection and successfully accomplishing their tasks.

- Related Documentation**
- [Reconnaissance Deterrence Overview on page 118](#)

Understanding FIN Scans

Supported Platforms [LN Series, SRX Series](#)

A FIN scan sends TCP segments with the FIN flag set in an attempt to provoke a response (a TCP segment with the RST flag set) and thereby discover an active host or an active port on a host. Attackers might use this approach rather than perform an address sweep with ICMP echo requests or an address scan with SYN segments, because they know that many firewalls typically guard against the latter two approaches but not necessarily against FIN segments. The use of TCP segments with the FIN flag set might evade detection and thereby help the attackers succeed in their reconnaissance efforts.

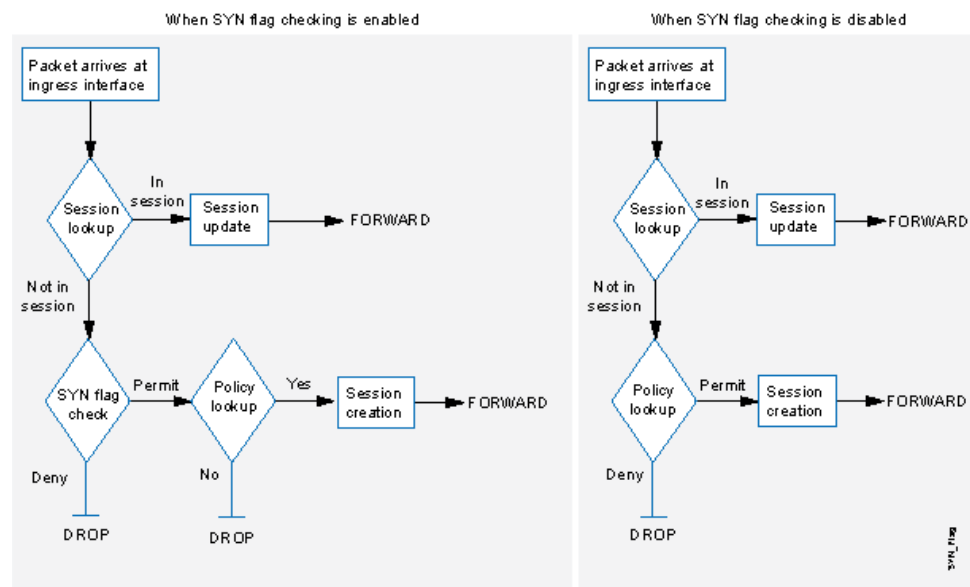
- Related Documentation**
- [Reconnaissance Deterrence Overview on page 118](#)

Understanding TCP SYN Checking

Supported Platforms [LN Series, SRX Series](#)

By default, Junos OS checks for SYN flags in the first packet of a session and rejects any TCP segments with non-SYN flags attempting to initiate a session. You can leave this packet flow as is or change it so that Junos OS does not enforce SYN flag checking before creating a session. [Figure 22 on page 130](#) illustrates packet flow sequences both when SYN flag checking is enabled and when it is disabled.

Figure 22: SYN Flag Checking



When Junos OS with SYN flag checking enabled receives a non-SYN TCP segment that does not belong to an existing session, it drops the packet. By default, Junos OS does not send a TCP RST to the source host on receiving the non-SYN segment. You can configure the device to send TCP RST to the source host by using the **set security zones security-zone trust tcp-rst** command. If the code bit of the initial non-SYN TCP packet is RST, the device does not send a TCP-RST.

Not checking for the SYN flag in the first packets offers the following advantages:

- **NSRP with Asymmetric Routing**—In an active/active NSRP configuration in a dynamic routing environment, a host might send the initial TCP segment with the SYN flag set to one device (Device-A), but the SYN/ACK might be routed to the other device in the cluster (Device-B). If this asymmetric routing occurs after Device-A has synchronized its session with Device-B, all is well. On the other hand, if the SYN/ACK response reaches Device-B before Device-A synchronizes the session and SYN checking is enabled, Device-B rejects the SYN/ACK, and the session cannot be established. With SYN checking disabled, Device-B accepts the SYN/ACK response—even though there is no existing session to which it belongs—and creates a new session table entry for it.
- **Uninterrupted Sessions**—If you reset the device or even change a component in the core section of a policy and SYN checking is enabled, all existing sessions or those sessions to which the policy change applies are disrupted and must be restarted. Disabling SYN checking avoids such disruptions to network traffic flows.



NOTE: A solution to this scenario is to install the device with SYN checking disabled initially. Then, after a few hours—when established sessions are running through the device—enable SYN checking. The core section in a policy contains the following main components: source and destination zones, source and destination addresses, one or more services, and an action.

However, the previous advantages exact the following security sacrifices:

- **Reconnaissance Holes**—When an initial TCP segment with a non-SYN flag—such as ACK, URG, RST, FIN—arrives at a closed port, many operating systems (Windows, for example) respond with a TCP segment that has the RST flag set. If the port is open, then the recipient does not generate any response.

By analyzing these responses or lack thereof, an intelligence gatherer can perform reconnaissance on the protected network and also on the Junos OS policy set. If a TCP segment is sent with a non-SYN flag set and the policy permits it through, the destination host receiving such a segment might drop it and respond with a TCP segment that has the RST flag set. Such a response informs the perpetrator of the presence of an active host at a specific address and that the targeted port number is closed. The intelligence gatherer also learns that the firewall policy permits access to that port number on that host.

By enabling SYN flag checking, Junos OS drops TCP segments without a SYN flag if they do not belong to an existing session. It does not return a TCP RST segment. Consequently, the scanner gets no replies regardless of the policy set or whether the port is open or closed on the targeted host.

- **Session Table Floods**—If SYN checking is disabled, an attacker can bypass the Junos OS SYN flood protection feature by flooding a protected network with a barrage of TCP segments that have non-SYN flags set. Although the targeted hosts drop the packets—and possibly send TCP RST segments in reply—such a flood can fill up the session table of the Juniper Networks device. When the session table is full, the device cannot process new sessions for legitimate traffic.

By enabling SYN checking and SYN flood protection, you can thwart this kind of attack. Checking that the SYN flag is set on the initial packet in a session forces all new sessions to begin with a TCP segment that has the SYN flag set. SYN flood protection then limits the number of TCP SYN segments per second so that the session table does not become overwhelmed.

If you do not need SYN checking disabled, Juniper Networks strongly recommends that it be enabled (its default state for an initial installation of Junos OS). You can enable it with the **set flow tcp-syn-check** command. With SYN checking enabled, the device rejects TCP segments with non-SYN flags set unless they belong to an established session.

Related Documentation

- [Reconnaissance Deterrence Overview on page 118](#)

Understanding IP Spoofing

Supported Platforms [LN Series](#), [SRX Series](#)

One method of attempting to gain access to a restricted area of the network is to insert a false source address in the packet header to make the packet appear to come from a trusted source. This technique is called IP spoofing. The mechanism to detect IP spoofing relies on route table entries. For example, if a packet with source IP address 10.1.1.6 arrives at ge-0/0/1, but Junos OS has a route to 10.1.1.0/24 through ge-0/0/0, a check for IP spoofing discovers that this address arrived at an invalid interface as defined in the route

table. A valid packet from 10.1.1.6 can only arrive via ge-0/0/0, not ge-0/0/1. Therefore, Junos OS concludes that the packet has a spoofed source IP address and discards it.



NOTE: Junos OS detects and drops both IPv4 and IPv6 spoofed packets.

**Related
Documentation**

- [Reconnaissance Deterrence Overview on page 118](#)

Understanding IP Spoofing in Layer 2 Transparent Mode

Supported Platforms [SRX Series](#)

In an IP spoofing attack, the attacker gains access to a restricted area of the network and inserts a false source address in the packet header to make the packet appear to come from a trusted source. IP spoofing is most frequently used in denial-of-service (DoS) attacks. When SRX Series devices are operating in transparent mode, the IP spoof-checking mechanism makes use of address book entries. Address books only exist on the Routing Engine. IP spoofing in Layer 2 transparent mode is performed on the Packet Forwarding Engine. Address book information cannot be obtained from the Routing Engine each time a packet is received by the Packet Forwarding Engine. Therefore, address books attached to the Layer 2 zones must be pushed to the Packet Forwarding Engine.



NOTE: IP spoofing in Layer 2 transparent mode does not support DNS and wildcard addresses.

When a packet is received by the Packet Forwarding Engine, the packet's source IP address is checked to determine if it is in the incoming zone's address-book. If the packet's source IP address is in the incoming zone's address book, then this IP address is allowed on the interface, and traffic is passed.

If the source IP address is not present in the incoming zone's address-book, but exists in other zones', then the IP address is considered a spoofed IP. Accordingly, actions such as drop and logging can be taken depending on the screen configuration (alarm-without-drop).



NOTE: If the alarm-without-drop option is configured, the Layer 2 spoofing packet only triggers an alarm message, but the packet is not dropped.

If a packet's source IP address is not present in the incoming zone's address book or other zones', then you cannot determine if the IP is spoofed or not. In such instances, the packet is passed.

Junos OS takes into account the following match conditions while it searches for source IP addresses in the address book:

- **Host-match**—The IP address match found in the address-book is an address without a prefix.
- **Prefix-match**—The IP address match found in the address-book is an address with a prefix.
- **Any-match**—The IP address match found in the address-book is “any”, “any-IPv4”, or “any-IPv6”.
- **No-match**—No IP address match is found.

**Related
Documentation**

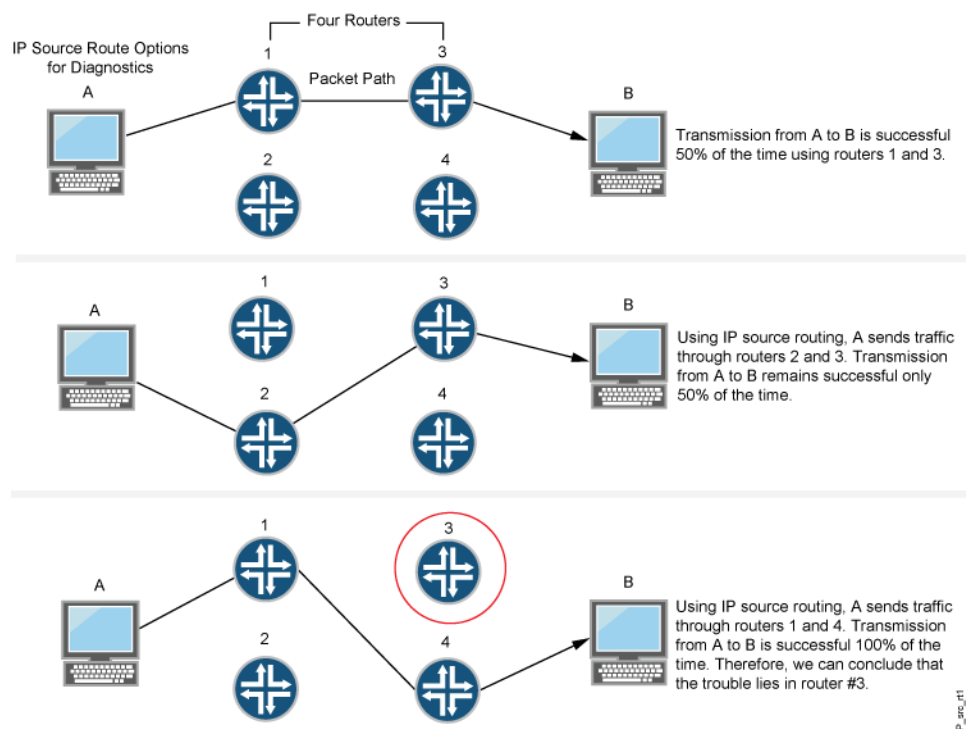
- [Configuring IP Spoofing in Layer 2 Transparent Mode on page 150](#)

Understanding IP Source Route Options

Supported Platforms [LN Series, SRX Series](#)

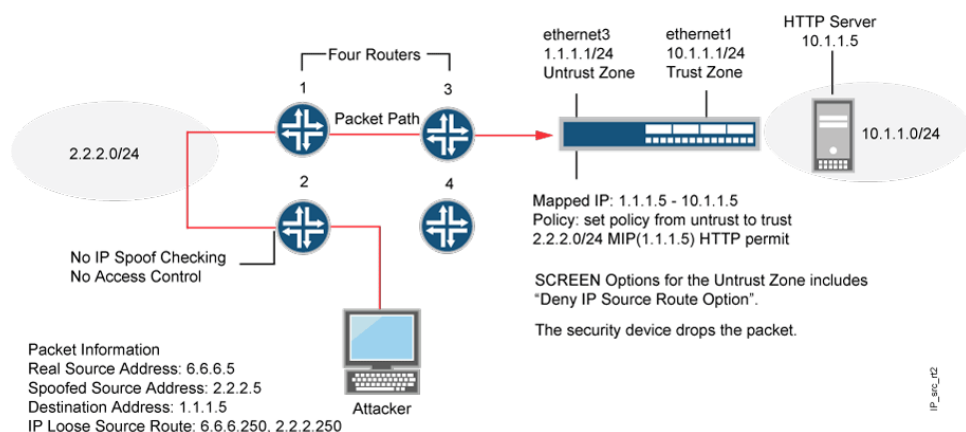
Source routing was designed to allow users at the source of an IP packet transmission to specify the IP addresses of the devices (also referred to as “hops”) along the path that they want an IP packet to take on its way to its destination. The original intent of the IP source route options was to provide routing control tools to aid diagnostic analysis. If, for example, the transmission of a packet to a particular destination meets with irregular success, you might first use either the record route or the timestamp IP option to discover the addresses of devices along the path or paths that the packet takes. You can then use either the loose or the strict source route option to direct traffic along a specific path, using the addresses you learned from the results that the record route or timestamp options produced. By changing device addresses to alter the path and sending several packets along different paths, you can note changes that either improve or lessen the success rate. Through analysis and the process of elimination, you might be able to deduce where the trouble lies. See [Figure 23 on page 134](#).

Figure 23: IP Source Routing



Although the uses of IP source route options were originally benign, attackers have learned to put them to more devious uses. They can use IP source route options to hide their true address and access restricted areas of a network by specifying a different path. For an example showing how an attacker can put both deceptions to use, consider the following scenario as illustrated in Figure 24 on page 134.

Figure 24: Loose IP Source Route Option for Deception



Junos OS only allows traffic 2.2.2.0/24 if it comes through ethernet1, an interface bound to zone_external. Devices 3 and 4 enforce access controls but devices 1 and 2 do not. Furthermore, device 2 does not check for IP spoofing. The attacker spoofs the source address and, by using the loose source route option, directs the packet through device 2 to the 2.2.2.0/24 network and from there out device 1. Device 1 forwards it to device 3,

which forwards it to the Juniper Networks device. Because the packet came from the 2.2.2.0/24 subnet and has a source address from that subnet, it seems to be valid. However, one remnant of the earlier chicanery remains: the loose source route option. In this example, you have enabled the deny IP source route screen option for zone_external. When the packet arrives at ethernet3, the device rejects it.

You can enable the device to either block any packets with loose or strict source route options set or detect such packets and then record the event in the counters list for the ingress interface. The screen options are as follows:

- Deny IP Source Route Option—Enable this option to block all IP traffic that employs the loose or strict source route option. Source route options can allow an attacker to enter a network with a false IP address.
- Detect IP Loose Source Route Option—The device detects packets where the IP option is 3 (Loose Source Routing) and records the event in the screen counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other devices in between those specified.
- Detect IP Strict Source Route Option—The device detects packets where the IP option is 9 (Strict Source Routing) and records the event in the screen counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field. Currently, this screen option is applicable to IPv4 only.

**Related
Documentation**

- [Reconnaissance Deterrence Overview on page 118](#)

CHAPTER 5

Configuration

- [IP Address and Port Options on page 137](#)
- [Operating System Probes on page 143](#)
- [Attacker Evasion Techniques on page 148](#)
- [Configuration Statements on page 156](#)

IP Address and Port Options

- [Example: Blocking IP Address Sweeps on page 137](#)
- [Example: Blocking Port Scans on page 139](#)
- [Example: Detecting Packets That Use IP Screen Options for Reconnaissance on page 141](#)

Example: Blocking IP Address Sweeps

Supported Platforms [LN Series, SRX Series](#)

This example describes how to configure a screen to block an IP address sweep originating from a security zone.

- [Requirements on page 137](#)
- [Overview on page 137](#)
- [Configuration on page 138](#)
- [Verification on page 138](#)

Requirements

Before you begin:

- Understand how IP address sweeps work. See [“Understanding IP Address Sweeps” on page 118](#).
- Configure security zones. *Security Zones and Interfaces Overview*.

Overview

You need to enable a screen for a security zone if you have configured a policy that permits ICMP traffic from that zone. If you have not configured such a policy, then your system

denies all ICMP traffic from that zone, and the attacker cannot perform an IP address sweep successfully anyway.

In this example you configure a **5000-ip-sweep** screen to block IP address sweeps originating in the zone-1 security zone.

Configuration

Step-by-Step Procedure

To configure a screen to block IP address sweeps:

1. Configure a screen.

```
[edit]
user@host# set security screen ids-option 5000-ip-sweep icmp ip-sweep threshold
5000
```

2. Enable the screen in the security zone.

```
[edit]
user@host# set security zones security-zone zone-1 screen 5000-ip-sweep
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 138](#)
- [Verifying the Security Screen Configuration on page 138](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones
Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: 5000-ip-sweep
  Interfaces bound: 1
  Interfaces:
    ge-1/0/0.0
```

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option screen-name** command.

```
[edit]
user@host> show security screen ids-option 5000-ip-sweep
```

Screen object status:

Name	Value
ICMP address sweep threshold	5000

Related Documentation

- [Reconnaissance Deterrence Feature Guide for Security Devices](#)

Example: Blocking Port Scans

Supported Platforms [LN Series, SRX Series](#)

This example shows how to configure a screen to block port scans originating from a particular security zone.

- [Requirements on page 139](#)
- [Overview on page 139](#)
- [Configuration on page 139](#)
- [Verification on page 140](#)

Requirements

Before you begin, understand how port scanning works. See [“Understanding Port Scanning” on page 119](#).

Overview

You can use a port scan to block IP packets containing TCP SYN segments or UDP segments sent to different ports from the same source address within a defined interval. The purpose of this attack is to scan the available services in the hopes that at least one port will respond. Once a port responds, it is identified as a service to target.

In this example, you configure a 5000 port-scan screen to block port scans originating from a particular security zone and then assign the screen to the zone called zone-1.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security screen ids-option 5000-port-scan tcp port-scan threshold 5000
set security screen ids-option 10000-port-scan udp port-scan threshold 10000
set security zones security-zone zone-1 screen 5000-port-scan
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a screen to block port scans:

1. Configure the screen.

```
[edit security]
user@host# set security screen ids-option 5000-port-scan tcp port-scan threshold
5000
user@host# set security screen ids-option 10000-port-scan udp port-scan threshold
10000
```

2. Enable the screen in the security zone.

```
[edit security]
user@host# set security zones security-zone zone-1 screen 5000-port-scan
```

Results From configuration mode, confirm your configuration by entering the **show security screen ids-option 5000-port-scan** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security screen ids-option 5000-port-scan
tcp {
  port-scan threshold 5000;
}
udp {
  port-scan threshold 10000;
}

[edit]
user@host# show security zones
security-zone zone-1 {
  screen 5000-port-scan;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 140](#)
- [Verifying the Security Screen Configuration on page 141](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones
```

```

Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: 5000-port-scan
  Interfaces bound: 0
  Interfaces:

```

Verifying the Security Screen Configuration

Purpose Verify the configuration information about the security screen.

Action From operational mode, enter the `show security screen ids-option screen-name` command.

[edit]

```
user@host> show security screen ids-option 5000-port-scan
```

Screen object status:

Name	Value
TCP port scan threshold	5000
UDP port scan threshold	10000

Related Documentation

- *Reconnaissance Deterrence Feature Guide for Security Devices*

Example: Detecting Packets That Use IP Screen Options for Reconnaissance

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to detect packets that use IP screen options for reconnaissance.

- [Requirements on page 141](#)
- [Overview on page 141](#)
- [Configuration on page 142](#)
- [Verification on page 143](#)

Requirements

Before you begin, understand how network reconnaissance works. See “[Understanding Network Reconnaissance Using IP Options](#)” on page 121.

Overview

RFC 791, *Internet Protocol*, specifies a set of options for providing special routing controls, diagnostic tools, and security. The screen options detect IP options that an attacker can use for reconnaissance, including record route, timestamp, security, and stream ID.

In this example, you configure an IP screen screen-1 and enable it in a security zone called zone-1.



NOTE: You can enable only one screen in one security zone.

Configuration

CLI Quick Configuration To quickly detect packets with the record route, timestamp, security, and stream ID IP screen options, copy the following commands and paste them into the CLI.

```
[edit]
set security screen ids-option screen-1 ip record-route-option
set security screen ids-option screen-1 ip timestamp-option
set security screen ids-option screen-1 ip security-option
set security screen ids-option screen-1 ip stream-option
set security zones security-zone zone-1 screen screen-1
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To detect packets that use IP screen options for reconnaissance:

1. Configure IP screen options.



NOTE: Currently, these screen options support IPv4 only.

```
[edit security screen]
user@host# set ids-option screen-1 ip record-route-option
user@host# set ids-option screen-1 ip timestamp-option
user@host# set ids-option screen-1 ip security-option
user@host# set ids-option screen-1 ip stream-option
```

2. Enable the screen in the security zone.

```
[edit security zones ]
user@host# set security-zone zone-1 screen screen-1
```

Results From configuration mode, confirm your configuration by entering the **show security screen** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
[user@host]show security screen
ids-option screen-1 {
  ip {
    record-route-option;
    timestamp-option;
    security-option;
    stream-option;
  }
}
[edit]
[user@host]show security zones
zones {
  security-zone zone-1 {
    screen screen-1;
```



```
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 143](#)
- [Verifying the Security Screen Configuration on page 143](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones

Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: screen-1
  Interfaces bound: 1
  Interfaces:
    ge-1/0/0.0
```

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option screen-name** command.

```
[edit]
user@host> show security screen ids-option screen-1
Screen object status:
```

Name	Value
IP record route option	enabled
IP timestamp option	enabled
IP security option	enabled
IP stream option	enabled

Related Documentation

- *Reconnaissance Deterrence Feature Guide for Security Devices*

Operating System Probes

- [Example: Blocking Packets with SYN and FIN Flags Set on page 144](#)
- [Example: Blocking Packets With FIN Flag Set and Without ACK Flag Set on page 145](#)
- [Example: Blocking Packets with No Flags Set on page 147](#)

Example: Blocking Packets with SYN and FIN Flags Set

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to create a screen to block packets with the SYN and FIN flags set.

- [Requirements on page 144](#)
- [Overview on page 144](#)
- [Configuration on page 144](#)
- [Verification on page 144](#)

Requirements

Before you begin, understand how TCP headers with SYN and FIN flags work. See [“Understanding TCP Headers with SYN and FIN Flags Set” on page 126](#).

Overview

The TCP header with the SYN and FIN flags set cause different responses from a targeted device depending on the OS it is running. The syn-fin screen is enabled for the security zone.

In this example, you create a screen called screen-1 in a security zone to block packets with the SYN and FIN flags set.

Configuration

Step-by-Step Procedure

To block packets with both the SYN and FIN flags set:

1. Configure the screen.

```
[edit]  
user@host# set security screen ids-option screen-1 tcp syn-fin
```
2. Enable the screen in the security zone.

```
[edit ]  
user@host# set security zones security-zone zone-1 screen screen-1
```
3. If you are done configuring the device, commit the configuration.

```
[edit]  
user@host# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 144](#)
- [Verifying the Security Screen Configuration on page 145](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones

Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: screen-1
  Interfaces bound: 1
  Interfaces:
    ge-1/0/0.0
```

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option screen-name** command.

```
[edit]
user@host> show security screen ids-option screen-1
Screen object status:
```

Name	Value
TCP SYN FIN	enabled

Related Documentation

- *Reconnaissance Deterrence Feature Guide for Security Devices*

Example: Blocking Packets With FIN Flag Set and Without ACK Flag Set

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to create a screen to block packets with the FIN flag set but the ACK flag not set.

- [Requirements on page 145](#)
- [Overview on page 145](#)
- [Configuration on page 146](#)
- [Verification on page 146](#)

Requirements

Before you begin, understand how TCP headers work. See “[Understanding TCP Headers With FIN Flag Set and Without ACK Flag Set](#)” on page 126.

Overview

The TCP segments with the FIN flag set also have the ACK flag set to acknowledge the previous packet received. Because a TCP header with the FIN flag set but the ACK flag not set is anomalous TCP behavior, there is no uniform response to this. When you enable the fin-no-ack screen option, Junos OS checks if the FIN flag is set but not the ACK flag in TCP headers. If it discovers a packet with such a header, it drops the packet.

In this example, you create a screen called screen-1 to block packets with the FIN flag set but the ACK flag not set.

Configuration

Step-by-Step Procedure

To block packets with the FIN flag set but the ACK flag not set:

1. Configure the screen.

```
[edit]  
user@host# set security screen ids-option screen-1 tcp fin-no-ack
```
2. If you are done configuring the device, commit the configuration.

```
[edit]  
user@host# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 146](#)
- [Verifying the Security Screen Configuration on page 146](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]  
user@host> show security zones  
  
Security zone: zone-1  
  Send reset for non-SYN session TCP packets: Off  
  Policy configurable: Yes  
  Screen: screen-1  
  Interfaces bound: 1  
  Interfaces:  
    ge-1/0/0.0
```

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option screen-name** command.

```
[edit]  
user@host> show security screen ids-option screen-1  
Screen object status:
```

Name	Value
TCP FIN no ACK	enabled

- Related Documentation**
- [Reconnaissance Deterrence Feature Guide for Security Devices](#)

Example: Blocking Packets with No Flags Set

Supported Platforms [LN Series, SRX Series](#)

This example shows how to create a screen to block packets with no flags set.

- [Requirements on page 147](#)
- [Overview on page 147](#)
- [Configuration on page 147](#)
- [Verification on page 148](#)

Requirements

Before you begin, understand how a TCP header with no flags set works. See [“Understanding TCP Header with No Flags Set” on page 127](#).

Overview

A normal TCP segment header has at least one flag control set. A TCP segment with no control flags set is an anomalous event. Because different operating systems respond differently to such anomalies, the response (or lack of response) from the targeted device can provide a clue as to the type of OS it is running.

When you enable the device to detect TCP segment headers with no flags set, the device drops all TCP packets with a missing or malformed flags field.

In this example, you create a screen called screen-1 to block packets with no flags set.

Configuration

Step-by-Step Procedure To block packets with no flags set:

1. Configure the screen.

```
[edit ]
user@host# set security screen ids-option screen-1 tcp tcp-no-flag
```
2. Enable the screen in the security zone.

```
[edit ]
user@host# set security zones security-zone zone-1 screen screen-1
```
3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 148](#)
- [Verifying the Security Screen Configuration on page 148](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones

Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: screen-1
  Interfaces bound: 1
  Interfaces:
    ge-1/0/0.0
```

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option screen-name** command.

```
[edit]
user@host> show security screen ids-option screen-1
Screen object status:

      Name                               Value
      TCP no flag                         enabled
```

Related Documentation • [Reconnaissance Deterrence Feature Guide for Security Devices](#)

Attacker Evasion Techniques

- [Thwarting a FIN Scan \(CLI Procedure\) on page 149](#)
- [Setting TCP SYN Checking \(CLI Procedure\) on page 149](#)
- [Setting Strict SYN Checking \(CLI Procedure\) on page 149](#)
- [Configuring IP Spoofing in Layer 2 Transparent Mode on page 150](#)
- [Example: Blocking IP Spoofing on page 151](#)

- [Example: Blocking Packets with Either a Loose or a Strict Source Route Option Set on page 152](#)
- [Example: Detecting Packets with Either a Loose or a Strict Source Route Option Set on page 154](#)

Thwarting a FIN Scan (CLI Procedure)

Supported Platforms [LN Series, SRX Series](#)

To thwart FIN scans, take either or both of the following actions:

- Enable the screen option that specifically blocks TCP segments with the FIN flag set but not the ACK flag, which is anomalous for a TCP segment:

```
user@host#set security screen fin-no-ack tcp fin-no-ack
user@host#set security zones security-zone name screen fin-no-ack
```

where *name* is the name of the zone to which you want to apply this screen option .

- Change the packet processing behavior to reject all non-SYN packets that do not belong to an existing session. The SYN check flag is set as the default.



NOTE: Changing the packet flow to check that the SYN flag is set for packets that do not belong to existing sessions also thwarts other types of non-SYN scans, such as a null scan (when no TCP flags are set).

Related Documentation

- [Reconnaissance Deterrence Feature Guide for Security Devices](#)

Setting TCP SYN Checking (CLI Procedure)

Supported Platforms [LN Series, SRX Series](#)

With SYN checking enabled, the device rejects TCP segments with non-SYN flags set unless they belong to an established session. Enabling SYN checking can help prevent attacker reconnaissance and session table floods. TCP SYN checking is enabled by default.

To disable SYN checking:

```
user@host#set security flow tcp-session no-syn-check
```

Related Documentation

- [Reconnaissance Deterrence Feature Guide for Security Devices](#)

Setting Strict SYN Checking (CLI Procedure)

Supported Platforms [LN Series, SRX Series](#)

With strict SYN checking enabled, the device enables the strict three-way handshake check for the TCP session. It enhances security by dropping data packets before the three-way handshake is done. TCP strict SYN checking is disabled by default.



NOTE: The `strict-syn-check` option cannot be enabled if `no-syn-check` or `no-syn-check-in-tunnel` is enabled.

To enable strict SYN checking:

```
user@host# set security flow tcp-session strict-syn-check
```

Related Documentation

- *Reconnaissance Deterrence Feature Guide for Security Devices*

Configuring IP Spoofing in Layer 2 Transparent Mode

Supported Platforms [SRX Series](#)

You can configure the IP spoof-checking mechanism to determine whether or not an IP is being spoofed.

To configure IP spoofing in Layer 2 transparent mode:

1. Set the interface in Layer 2 transparent mode.

[edit]

```
user@host# set interfaces ge-0/0/1 unit 0 family bridge
```



NOTE: If the interface is in Layer 2 mode, the device is in Layer 2 mode. If the interface is switched between Layer 3 and Layer 2 mode, the system must be rebooted.

2. (Optional) Set the zone in Layer 2 transparent mode.

[edit]

```
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0
```

3. Configure the address book.

[edit]

```
user@host# set security address-book my-book address myadd1 10.1.1.0/24
```

```
user@host# set security address-book my-book address myadd2 10.1.2.0/24
```

4. Apply the address book to the zone.

[edit]

```
user@host# set security address-book my-book attach zone untrust
```

5. Configure screen IP spoofing.

[edit]

```
user@host# set security screen ids-option my-screen ip spoofing
```

6. Apply the screen to the zone.

[edit]

```
user@host# set security zones security-zone untrust screen my-screen
```

7. (Optional) Configure the `alarm-without-drop` option.


```
[edit]
user@host# set security screen ids-option my-screen alarm-without-drop
```



NOTE: If the `alarm-without-drop` option is configured, the Layer 2 spoofing packet only triggers an alarm message, but the packet is not dropped.

Related Documentation

- [Understanding IP Spoofing in Layer 2 Transparent Mode on page 132](#)

Example: Blocking IP Spoofing

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to configure a screen to block IP spoof attacks.

- [Requirements on page 151](#)
- [Overview on page 151](#)
- [Configuration on page 151](#)
- [Verification on page 152](#)

Requirements

Before you begin, understand how IP Spoofing works. See “[Understanding IP Spoofing](#)” on page 131.

Overview

One method of attempting to gain access to a restricted area of a network is to insert a bogus source address in the packet header to make the packet appear to come from a trusted source. This technique is called IP spoofing.

In this example, you configure a screen called `screen-1` to block IP spoof attacks and enable the screen in the `zone-1` security zone.

Configuration

Step-by-Step Procedure

To block IP spoofing:

1. Configure the screen.


```
[edit]
user@host# set security screen ids-option screen-1 ip spoofing
```
2. Enable the screen in the security zone.


```
[edit]
user@host# set security zone security-zone zone-1 screen screen-1
```
3. If you are done configuring the device, commit the configuration.


```
[edit]
user@host# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 152](#)
- [Verifying the Security Screen Configuration on page 152](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones

Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: screen-1
  Interfaces bound: 1
  Interfaces:
    ge-1/0/0.0
```

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option screen-name** command.

```
[edit]
user@host> show security screen ids-option screen-1
Screen object status:

      Name                Value
      IP spoofing         enabled
```

Related Documentation

- *Reconnaissance Deterrence Feature Guide for Security Devices*

Example: Blocking Packets with Either a Loose or a Strict Source Route Option Set

Supported Platforms [LN Series, SRX Series](#)

This example shows how to block packets with either a loose or a strict source route option set.

- [Requirements on page 153](#)
- [Overview on page 153](#)
- [Configuration on page 153](#)
- [Verification on page 153](#)

Requirements

Before you begin, understand how IP source route options work. See [“Understanding IP Source Route Options” on page 133](#).

Overview

Source routing allows users at the source of an IP packet transmission to specify the IP addresses of the devices (also referred to as “hops”) along the path that they want an IP packet to take on its way to its destination. The original intent of the IP source route options was to provide routing control tools to aid diagnostic analysis.

You can enable the device to either block any packets with loose or strict source route options set or detect such packets and then record the event in the counters list for the ingress interface.

In this example you create the screen called screen-1 to block packets with either a loose or a strict source route option set and enable the screen in the zone-1 security zone.

Configuration

Step-by-Step Procedure

To block packets with either the loose or the strict source route option set:

1. Configure the screen.

```
[edit ]
user@host# set security screen ids-option screen-1 ip source-route-option
```
2. Enable the screen in the security zone.

```
[edit ]
user@host# set security zones security-zone zone-1 screen screen-1
```
3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 153](#)
- [Verifying the Security Screen Configuration on page 154](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones
Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: screen-1
```

```
Interfaces bound: 1
Interfaces:
  ge-1/0/0.0
```

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option *screen-name*** command.

[edit]

```
user@host> show security screen ids-option screen-1
```

Screen object status:

Name	Value
IP source route option	enabled

Related Documentation

- *Reconnaissance Deterrence Feature Guide for Security Devices*

Example: Detecting Packets with Either a Loose or a Strict Source Route Option Set

Supported Platforms [LN Series, SRX Series](#)

This example shows how to detect packets with either a loose or a strict source route option set.

- [Requirements on page 154](#)
- [Overview on page 154](#)
- [Configuration on page 155](#)
- [Verification on page 155](#)

Requirements

Before you begin, understand how IP source route options work. See “[Understanding IP Source Route Options](#)” on page 133.

Overview

Source routing allows users at the source of an IP packet transmission to specify the IP addresses of the devices (also referred to as “hops”) along the path that they want an IP packet to take on its way to its destination. The original intent of the IP source route options was to provide routing control tools to aid diagnostic analysis.

You can enable the device to either block any packets with loose or strict source route options set or detect such packets and then record the event in the counters list for the ingress interface.

In this example, you create two screens called screen-1 and screen-2 to detect and record, but not block, packets with a loose or strict source route option set and enable the screens in zones zone-1 and zone-2.

Configuration

Step-by-Step Procedure To detect and record, but not block, packets with a loose or strict source route option set:

1. Configure the loose source screen.

```
[edit]
user@host# set security screen ids-option screen-1 ip loose-source-route-option
```
2. Configure the strict source route screen.

```
[edit]
user@host# set security screen ids-option screen-2 ip strict-source-route-option
```



NOTE: Currently, this screen option supports IPv4 only.

3. Enable the screens in the security zones.

```
[edit]
user@host# set security zones security-zone zone-1 screen screen-1
user@host# set security zones security-zone zone-2 screen screen-2
```
4. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Screens in the Security Zone on page 155](#)
- [Verifying the Security Screen Configuration on page 156](#)

Verifying the Screens in the Security Zone

Purpose Verify that the screen is enabled in the security zone.

Action From operational mode, enter the **show security zones** command.

```
[edit]
user@host> show security zones

Security zone: zone-1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: screen-1
  Interfaces bound: 1
  Interfaces:
    ge-1/0/0.0
Security zone: zone-2
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: screen-2
  Interfaces bound: 1
```

Interfaces:
ge-2/0/0.0

Verifying the Security Screen Configuration

Purpose Display the configuration information about the security screen.

Action From operational mode, enter the **show security screen ids-option *screen-name*** command.

```
[edit]
user@host> show security screen ids-option screen-1
Screen object status:

Screen object status:

Name                                     Value
IP loose source route option           enabled
```

```
[edit]
user@host> show security screen ids-option screen-2
Screen object status:

Screen object status:

Name                                     Value
IP strict source route option          enabled
```

Related Documentation • *Reconnaissance Deterrence Feature Guide for Security Devices*

Configuration Statements

- [\[edit security screen\] Hierarchy Level on page 157](#)
- [attack-threshold on page 160](#)
- [description \(Security Screen\) on page 161](#)
- [destination-ip-based on page 162](#)
- [destination-threshold on page 163](#)
- [fin-no-ack on page 164](#)
- [flood \(Security ICMP\) on page 165](#)
- [flood \(Security UDP\) on page 166](#)
- [icmp \(Security Screen\) on page 167](#)
- [ids-option on page 168](#)
- [ip \(Security Screen\) on page 171](#)
- [ip-sweep on page 173](#)
- [land on page 174](#)
- [large on page 174](#)
- [limit-session on page 175](#)

- [no-syn-check](#) on page 175
- [no-syn-check-in-tunnel](#) on page 176
- [ping-death](#) on page 176
- [port-scan](#) on page 177
- [screen \(Security Zones\)](#) on page 178
- [source-ip-based](#) on page 178
- [source-threshold](#) on page 179
- [strict-syn-check](#) on page 179
- [syn-ack-ack-proxy](#) on page 180
- [syn-check-required](#) on page 180
- [syn-fin](#) on page 181
- [syn-flood](#) on page 182
- [syn-flood-protection-mode](#) on page 183
- [syn-frag](#) on page 183
- [tcp \(Security Screen\)](#) on page 184
- [tcp-no-flag](#) on page 185
- [tcp-sweep](#) on page 186
- [timeout \(Security Screen\)](#) on page 187
- [traceoptions \(Security Screen\)](#) on page 188
- [udp \(Security Screen\)](#) on page 190
- [udp-sweep](#) on page 191
- [white-list](#) on page 192
- [winnuke](#) on page 193

[edit security screen] Hierarchy Level

Supported Platforms [LN Series, SRX Series](#)

```

security {
  screen {
    ids-option screen-name {
      alarm-without-drop;
      description text;
      icmp {
        flood {
          threshold number;
        }
        fragment;
        icmpv6-malformed;
        ip-sweep {
          threshold number;
        }
        large;
        ping-death;
      }
    }
  }
}

```

```
}
ip {
  bad-option;
  block-frag;
  ipv6-extension-header {
    AH-header;
    ESP-header;
    HIP-header;
    destination-header {
      ILNP-nonce-option;
      home-address-option;
      line-identification-option;
      tunnel-encapsulation-limit-option;
      user-defined-option-type low | <to high>;
    }
    fragment-header;
    hop-by-hop-header {
      CALIPSO-option;
      RPL-option;
      SFM-DPD-option;
      jumbo-payload-option;
      quick-start-option;
      router-alert-option;
      user-defined-option-type low | <to high>;
    }
    mobility-header;
    no-next-header;
    routing-header;
    shim6-header;
    user-defined-option-type low | <to high>;
  }
  ipv6-extension-header-limit limit;
  ipv6-malformed-header;
  loose-source-route-option;
  record-route-option;
  security-option;
  source-route-option;
  spoofing;
  stream-option;
  strict-source-route-option;
  tear-drop;
  timestamp-option;
  unknown-protocol;
}
limit-session {
  destination-ip-based number;
  source-ip-based number;
}
tcp {
  fin-no-ack;
  land;
  port-scan {
    threshold number;
  }
  syn-ack-ack-proxy {
    threshold number;
  }
}
```



```

    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
        threshold threshold number;
    }
    winnuke;
}
udp {
    flood {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
}
}
traceoptions {
    file filename {
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
}
```

Related Documentation

- *Security Configuration Statement Hierarchy*
- *Junos OS Logical Systems Library for Security Devices*

attack-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `attack-threshold number;`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Define the number of SYN packets per second required to trigger the SYN proxy response.

Options *number*—Number of SYN packets per second required to trigger the SYN proxy response.

Range: 1 through 500,000 per second

Default: 200 per second



NOTE: For SRX Series devices, the applicable range is 1 through 1,000,000 per second.

Required Privilege security—To view this statement in the configuration.

Level security-control—To add this statement to the configuration.

- Related Documentation**
- [Security Configuration Statement Hierarchy](#)
 - [destination-threshold on page 65](#)

description (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `description text;`

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 12.1 of Junos OS.

Description Specify descriptive text for a screen.



NOTE: The descriptive text should not include characters, such as "<", ">", "&", or "\n".

Options *text*—Descriptive text about a screen.

Range: 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

Required Privilege security—To view this statement in the configuration.

Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

destination-ip-based

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax destination-ip-based *number*;

Hierarchy Level [edit security screen ids-option *screen-name* limit-session]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Limit the number of concurrent sessions the device can direct to a single destination IP address.

Options *number*—Maximum number of concurrent sessions that can be directed to a destination IP address.

Range: 1 through 1,000,000

Default: 128



NOTE: For SRX Series devices, the applicable range is 1 through 8,000,000.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

destination-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax destination-threshold *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based only on the destination IP address, regardless of the destination port number.

Options *number* —Number of SYN segments received per second before the device begins dropping connection requests.

Range: 4 through 500,000 per second

Default: 2048 per second



NOTE: For SRX Series devices, the applicable range is 4 through 1,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)
- [attack-threshold on page 62](#)

fin-no-ack

Supported Platforms	LN Series , SRX Series
Syntax	fin-no-ack;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of an illegal combination of flags, and reject packets that have this combination.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

flood (Security ICMP)

Supported Platforms

Syntax flood {
 threshold *number*;
 }

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the device to detect and prevent Internet Control Message Protocol (ICMP) floods. An ICMP flood occurs when ICMP echo requests are broadcast with the purpose of flooding a system with so much data that it first slows down, and then times out and is disconnected. The threshold defines the number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Options **threshold *number*** —Number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Range: 1 through 1,000,000 per second

Default: 1,000 per second



NOTE: For SRX Series devices the applicable range is 1 through 4,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation • [flood \(Security UDP\) on page 68](#)
 • *Security Configuration Statement Hierarchy*

flood (Security UDP)

Supported Platforms

Syntax flood {
 threshold *number*;
 }

Hierarchy Level [edit security screen ids-option *screen-name* udp]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the device to detect and prevent UDP floods. UDP flooding occurs when an attacker sends UDP packets to slow down the system to the point that it can no longer process valid connection requests.

The threshold defines the number of UDP packets per second allowed to ping the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options threshold *number* —Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.

Range: 1 through 1,000,000 per second

Default: 1,000 per second



NOTE: For SRX series devices the applicable range is 1 through 4,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation • *Security Configuration Statement Hierarchy*
 • [flood \(Security ICMP\) on page 67](#)

icmp (Security Screen)

Supported Platforms

Syntax

```
icmp {
    flood {
        threshold number;
    }
    fragment;
    icmpv6-malformed;
    ip-sweep {
        threshold number;
    }
    large;
    ping-death;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure ICMP intrusion detection service (IDS) options.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

ids-option

Supported Platforms

Syntax `ids-option screen-name {
 alarm-without-drop;
 description text;
 icmp {
 flood {
 threshold number;
 }
 fragment;
 icmpv6-malformed;
 ip-sweep {
 threshold number;
 }
 large;
 ping-death;
 }
 ip {
 bad-option;
 block-frag;
 ipv6-extension-header {
 AH-header;
 ESP-header;
 HIP-header;
 destination-header {
 ILNP-nonce-option;
 home-address-option;
 line-identification-option;
 tunnel-encapsulation-limit-option;
 user-defined-option-type low | <to high>;
 }
 fragment-header;
 hop-by-hop-header {
 CALIPSO-option;
 RPL-option;
 SFM-DPD-option;
 jumbo-payload-option;
 quick-start-option;
 router-alert-option;
 user-defined-option-type low | <to high>;
 }
 mobility-header;
 no-next-header;
 routing-header;
 shim6-header;
 user-defined-option-type low | <to high>;
 }
 ipv6-extension-header-limit limit;
 ipv6-malformed-header;
 loose-source-route-option;
 record-route-option;
 security-option;
 source-route-option;
 }
 }`

```

spoofing;
stream-option;
strict-source-route-option;
tear-drop;
timestamp-option;
unknown-protocol;
}
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
tcp {
    fin-no-ack;
    land;
    port-scan {
        threshold number;
    }
    syn-ack-ack-proxy {
        threshold number;
    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
        threshold threshold number;
    }
    winnuke;
}
udp {
    flood {
        threshold number;
    }
    port-scan {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
}
}

```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Junos OS Release 8.5. Support for the **description** option added in Junos OS Release 12.1. Support for the port scan for UDP option added in Junos OS Release 12.1X47-D10.

Description Define screens for intrusion detection service (IDS).

Options **description text**—Descriptive text about screen.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

ip (Security Screen)

Supported Platforms

Syntax

```
ip {
  bad-option;
  block-frag;
  ipv6-extension-header {
    AH-header;
    ESP-header;
    HIP-header;
    destination-header {
      ILNP-nonce-option;
      home-address-option;
      line-identification-option;
      tunnel-encapsulation-limit-option;
      user-defined-option-type low | <to high>;
    }
    fragment-header;
    hop-by-hop-header {
      CALIPSO-option;
      RPL-option;
      SFM-DPD-option;
      jumbo-payload-option;
      quick-start-option;
      router-alert-option;
      user-defined-option-type low | <to high>;
    }
    mobility-header;
    no-next-header;
    routing-header;
    shim6-header
    user-defined-option-type low | <to high>;
  }
  ipv6-extension-header-limit limit;
  ipv6-malformed-header;
  loose-source-route-option;
  record-route-option;
  security-option;
  source-route-option;
  spoofing;
  stream-option;
  strict-source-route-option;
  tear-drop;
  timestamp-option;
  unknown-protocol;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for IPv6 bad-option extension header screens added in Junos OS Release 12.1X46-D10.

Description Configure IP layer IDS options.

- Options**
- **bad-option**—Detect and drop any packet with an incorrectly formatted IP option in the IP packet header. The device records the event in the screen counters list for the ingress interface. This screen option is applicable to IPv4 and IPv6.
 - **block-frag**—Enable IP packet fragmentation blocking.
 - **loose-source-route-option**—Detect packets where the IP option is 3 (loose source routing), and record the event in the screen counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other devices in between those specified. The type 0 routing header of the loose source route option is the only related header defined in IPv6 .
 - **record-route-option**—Detect packets where the IP option is 7 (record route), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **security-option**—Detect packets where the IP option is 2 (security), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **source-route-option**—Detect packets, and record the event in the screen counters list for the ingress interface.
 - **spoofing**—Prevent spoofing attacks. Spoofing attacks occur when unauthorized agents attempt to bypass firewall security by imitating valid client IP addresses. Using the spoofing option invalidates such false source IP address connections.

The default behavior is to base spoofing decisions on individual interfaces.
 - **stream-option**—Detect packets where the IP option is 8 (stream ID), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **strict-source-route-option**—Detect packets where the IP option is 9 (strict source routing), and record the event in the screen counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field. Currently, this screen option is applicable only to IPv4.
 - **tear-drop**—Block the teardrop attack. Teardrop attacks occur when fragmented IP packets overlap and cause the host attempting to reassemble the packets to crash. The teardrop option directs the device to drop any packets that have such a discrepancy.
 - **timestamp-option**—Detect packets where the IP option list includes option 4 (Internet timestamp), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **unknown-protocol**—Discard all received IP frames with protocol numbers greater than 137 for IPv4 and 139 for IPv6. Such protocol numbers are undefined or reserved.

Required Privilege	security—To view this statement in the configuration.
Level	security-control—To add this statement to the configuration.

Related Documentation • [Security Configuration Statement Hierarchy](#)

ip-sweep

Supported Platforms [LN Series, SRX Series](#)

Syntax

```
ip-sweep {
    threshold number;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and prevent an IP Sweep attack. An IP Sweep attack occurs when an attacker sends ICMP echo requests (pings) to multiple destination addresses. If a target host replies, the reply reveals the target's IP address to the attacker. If the device receives 10 ICMP echo requests within the number of microseconds specified in this statement, it flags this as an IP Sweep attack, and rejects the 11th and all further ICMP packets from that host for the remainder of the second.

Options **threshold *number***—Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device. More than 10 requests from a host during this period triggers an IP Sweep attack response on the device during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation • [Security Configuration Statement Hierarchy](#)

land

Supported Platforms	LN Series , SRX Series
Syntax	land;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable prevention of Land attacks by combining the SYN flood defense with IP spoofing protection. Land attacks occur when an attacker sends spoofed IP packets with headers containing the target's IP address for the source and destination IP addresses. The attacker sends these packets with the SYN flag set to any available port. The packets induce the target to create empty sessions with itself, filling its session table and overwhelming its resources.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

large

Supported Platforms	LN Series , SRX Series
Syntax	large;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> icmp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Configure the device to detect and drop any ICMP frame with an IP length greater than 1024 bytes.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Reconnaissance Deterrence Feature Guide for Security Devices</i>

limit-session

Supported Platforms	LN Series , SRX Series
Syntax	<pre>limit-session { destination-ip-based <i>number</i>; source-ip-based <i>number</i>; }</pre>
Hierarchy Level	[edit security screen ids-option <i>screen-name</i>]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Limit the number of concurrent sessions the device can initiate from a single source IP address or the number of sessions it can direct to a single destination IP address.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Security Configuration Statement Hierarchy</i>

no-syn-check

Supported Platforms	LN Series , SRX Series
Syntax	no-syn-check;
Hierarchy Level	[edit security flow tcp-session]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Disable checking of the TCP SYN bit before creating a session. By default, the device checks that the SYN bit is set in the first packet of a session. If the bit is not set, the device drops the packet.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Reconnaissance Deterrence Feature Guide for Security Devices</i>

no-syn-check-in-tunnel

Supported Platforms	LN Series , SRX Series
Syntax	no-syn-check-in-tunnel;
Hierarchy Level	[edit security flow tcp-session]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Disable checking of the TCP SYN bit before creating a session for tunneled packets. By default, the device checks that the SYN bit is set in the first packet of a VPN session. If the bit is not set, the device drops the packet.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Reconnaissance Deterrence Feature Guide for Security Devices</i>

ping-death

Supported Platforms	LN Series , SRX Series
Syntax	ping-death;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> icmp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Configure the device to detect and reject oversized and irregular ICMP packets. Although the TCP/IP specification requires a specific packet size, many ping implementations allow larger packet sizes. Larger packets can trigger a range of adverse system reactions, including crashing, freezing, and restarting.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

port-scan

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
port-scan {
    threshold number;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Prevent port scan attacks. A port scan attack occurs when an attacker sends packets with different port numbers to scan available services. The attack succeeds if a port responds. To prevent this attack, the device internally logs the number of different ports scanned from a single remote source. For example, if a remote host scans 10 ports in 0.005 seconds (equivalent to 5000 microseconds, the default threshold setting), the device flags this behavior as a port scan attack, and rejects further packets from the remote source.

Options **threshold *number*** —Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers. If the number of ports during the threshold period reaches 10 or more, the device rejects additional packets from the source.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

screen (Security Zones)

Supported Platforms

Syntax `screen screen-name;`

Hierarchy Level [edit security zones functional-zone management],
[edit security zones security-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify a security screen for a security zone.

Options *screen-name* —Name of the screen.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Zones and Interfaces Feature Guide for Security Devices*

source-ip-based

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `source-ip-based number;`

Hierarchy Level [edit security screen ids-option *screen-name* limit-session]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Limit the number of concurrent sessions the device can initiate from a single source IP address.

Options *number* —Maximum number of concurrent sessions that can be initiated from a source IP address.

Range: 1 through 1,000,000

Default: 128



NOTE: For SRX Series devices the applicable range is 1 through 8,000,000.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

source-threshold

Supported Platforms	LN Series, SRX Series
Syntax	source-threshold <i>number</i> ;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp syn-flood]
Release Information	Statement modified in Release 9.2 of Junos OS.
Description	Specify the number of SYN segments that the device can receive per second from a single source IP address (regardless of the destination IP address and port number) before the device begins dropping connection requests from that source.
Options	<p><i>number</i> —Number of SYN segments to be received per second before the device starts dropping connection requests.</p> <p>Range: 4 through 500,000 per second</p> <p>Default: 4000 per second</p>



NOTE: For SRX Series devices the applicable range is 4 through 1,000,000 per second.

Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Security Configuration Statement Hierarchy</i>

strict-syn-check

Supported Platforms	LN Series, SRX Series
Syntax	strict-syn-check;
Hierarchy Level	[edit security flow tcp-session]
Release Information	Statement introduced in Release 9.4 of Junos OS.
Description	Enable the strict three-way handshake check for the TCP session. It enhances security by dropping data packets before the three-way handshake is done. By default, strict-syn-check is disabled.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Reconnaissance Deterrence Feature Guide for Security Devices</i>

syn-ack-ack-proxy

Supported Platforms	LN Series , SRX Series
Syntax	<pre>syn-ack-ack-proxy; { threshold <i>number</i>, }</pre>
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.
Description	Prevent the SYN-ACK-ACK attack, which occurs when the attacker establishes multiple telnet sessions without allowing each session to terminate. This behavior consumes all open slots, generating a denial-of-service (DoS) condition.
Options	threshold <i>number</i> — Number of connections from any single IP address. Range: 1 through 250,000 Default: 512
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

syn-check-required

Supported Platforms	LN Series , SRX Series
Syntax	<pre>syn-check-required;</pre>
Hierarchy Level	[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> then permit tcp-options]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Enable sync check per policy. The syn-check-required value overrides the global value no-syn-check.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Policies Feature Guide for Security Devices</i>

syn-fin

Supported Platforms	LN Series , SRX Series
Syntax	syn-fin;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of an illegal combination of flags that attackers can use to consume sessions on the target device, thus resulting in a denial-of-service (DoS) condition.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

syn-flood

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
syn-flood {  
    alarm-threshold number;  
    attack-threshold number;  
    destination-threshold number;  
    source-threshold number;  
    timeout seconds;  
    white-list name {  
        destination-address destination-address;  
        source-address source-address;  
    }  
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure detection and prevention of SYN flood attacks. Such attacks occur when the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses.



NOTE: On all SRX Series devices, the TCP synchronization flood alarm threshold value does not indicate the number of packets dropped, however the value does show the packet information after the alarm threshold has been reached.

The synchronization cookie or proxy never drops packets; therefore the **alarm-without-drop (not drop)** action is shown in the system log.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)

syn-flood-protection-mode

Supported Platforms	LN Series , SRX Series
Syntax	syn-flood-protection-mode (syn-cookie syn-proxy);
Hierarchy Level	[edit security flow]
Release Information	Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.
Description	Enable SYN cookie or SYN proxy defenses against SYN attacks. SYN flood protection mode is enabled globally on the device and is activated when the configured syn-flood attack-threshold value is exceeded.
Options	<ul style="list-style-type: none"> • syn-cookie—Uses a cryptographic hash to generate a unique Initial Sequence Number (ISN). This is enabled by default. • syn-proxy—Uses a proxy to handle the SYN attack.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Flow-Based Processing Feature Guide for Security Devices</i>

syn-frag

Supported Platforms	LN Series , SRX Series
Syntax	syn-frag;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of a SYN fragment attack and drops any packet fragments used for the attack. A SYN fragment attack floods the target host with SYN packet fragments. The host caches these fragments, waiting for the remaining fragments to arrive so it can reassemble them. The flood of connections that cannot be completed eventually fills the host's memory buffer. No further connections are possible, and damage to the host's operating system can occur.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Security Configuration Statement Hierarchy</i>

tcp (Security Screen)

Supported Platforms

Syntax

```
tcp {  
    fin-no-ack;  
    land;  
    port-scan {  
        threshold number;  
    }  
    syn-ack-ack-proxy {  
        threshold number;  
    }  
    syn-fin;  
    syn-flood {  
        alarm-threshold number;  
        attack-threshold number;  
        destination-threshold number;  
        source-threshold number;  
        timeout seconds;  
        white-list name {  
            destination-address destination-address;  
            source-address source-address;  
        }  
    }  
    syn-frag;  
    tcp-no-flag;  
    tcp-sweep {  
        threshold threshold number;  
    }  
    winnuke;  
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure TCP-layer intrusion detection service (IDS) options.



NOTE: On all SRX Series devices, the TCP synchronization flood alarm threshold value does not indicate the number of packets dropped, however the value does show the packet information after the alarm threshold has been reached.

The synchronization cookie or proxy never drops packets; therefore the alarm-without-drop (not drop) action is shown in the system log.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

tcp-no-flag

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax tcp-no-flag;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to drop illegal TCP packets with a missing or malformed flag field.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

tcp-sweep

Supported Platforms

Syntax tcp-sweep {
 threshold *number*;
 }

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the device to detect and prevent TCP sweep attack. In a TCP sweep attack, an attacker sends TCP SYN packets to the target device as part of the TCP handshake. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends TCP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as a TCP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further TCP packets from that host for the remainder of the specified threshold period.

Options **threshold *number***—Maximum number of microseconds during which up to 10 TCP SYN packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers TCP Sweep attack response on the router during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation • *Security Configuration Statement Hierarchy*

timeout (Security Screen)

Supported Platforms

Syntax `timeout seconds;`

Hierarchy Level `[edit security screen ids-option screen-name tcp syn-flood]`

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum length of time before a half-completed connection is dropped from the queue. You can decrease the timeout value until you see any connections dropped during normal traffic conditions.

Options **seconds** —Time interval before a half-completed connection is dropped from the queue.
Range: 1 through 50 seconds
Default: 20 seconds

Required Privilege Level `security`—To view this statement in the configuration.
 `security-control`—To add this statement to the configuration.

Related Documentation • *Security Configuration Statement Hierarchy*

traceoptions (Security Screen)

Supported Platforms

Syntax

```
traceoptions {  
  file {  
    filename;  
    files number;  
    match regular-expression;  
    size maximum-file-size;  
    (world-readable | no-world-readable);  
  }  
  flag flag;  
  no-remote-trace;  
}
```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure screen tracing options.

To specify more than one tracing option, include multiple **flag** statements.

Options

- **file**—Configure the trace file options.

- **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.

- **files number**—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10 files

- **match regular-expression**—Refine the output to include lines that contain the regular expression.
- **size maximum-file-size**—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: **x K** to specify KB, **x m** to specify MB, or **x g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
 - **all**—Trace all screen events
 - **configuration**—Trace screen configuration events
 - **flow**—Trace flow events
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none"> • <i>Security Configuration Statement Hierarchy</i>
------------------------------	---

udp (Security Screen)

Supported Platforms

Syntax

```
udp {  
  flood {  
    threshold number;  
  }  
  udp-sweep {  
    threshold threshold number;  
  }  
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the number of packets allowed per second to the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

udp-sweep

Supported Platforms

Syntax `udp-sweep {
 threshold number;
 }`

Hierarchy Level `[edit security screen ids-option screen-name udp]`

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the device to detect and prevent UDP sweep attack. In a UDP sweep attack, an attacker sends UDP packets to the target device. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends UDP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as an UDP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further UDP packets from that host for the remainder of the specified threshold period.

Options **threshold *number***—Maximum number of microseconds during which up to 10 UDP packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers an UDP Sweep attack response on the device during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation • *Security Configuration Statement Hierarchy*

white-list

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `white-list name {
 destination-address [address];
 source-address [address];
}`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement introduced in Release 12.1 of Junos OS.

Description Configure a whitelist of IP addresses that are to be exempt from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process.

Both IP version 4 (IPv4) and IP version 6 (IPv6) whitelists are supported. Addresses in a whitelist must be all IPv4 or all IPv6. Each whitelist can have up to 32 IP address prefixes.

- Options**
- **destination-address *address***—Destination IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.
 - **source-address *address***—Source IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

winnuke

Supported Platforms	LN Series , SRX Series
Syntax	winnuke;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of attacks on Windows NetBios communications. Packets are modified as necessary and passed on. Each WinNuke attack triggers an attack log entry in the event alarm log.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

CHAPTER 6

Administration

- [Operational Commands on page 195](#)

Operational Commands

- [clear security screen statistics](#)
- [clear security screen statistics interface](#)
- [clear security screen statistics zone](#)
- [show security screen ids-option](#)
- [show security screen statistics](#)

clear security screen statistics

Supported Platforms

Syntax clear security screen statistics
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 9.0 of Junos OS.

Description Clear intrusion detection service (IDS) security screen statistics on the device.

Options **node**—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.

- **node-id** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level clear

Related Documentation

- [show security screen statistics on page 106](#)

List of Sample Output [clear security screen statistics node 0 on page 196](#)

Output Fields This command produces no output.

Sample Output

[clear security screen statistics node 0](#)

```
user@host> clear security screen statistics node 0
```

clear security screen statistics interface

Supported Platforms

Syntax clear security screen statistics interface *interface-name*

Release Information Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description Clear intrusion detection service (IDS) security screen statistics for an interface.

- Options**
- **interface** *interface-name* —Name of the interface on which to clear security screen statistics.
 - **node**—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.
 - **node-id** —Identification number of the node. It can be 0 or 1.
 - **all** —Clear all nodes.
 - **local** —Clear the local node.
 - **primary**—Clear the primary node.

Required Privilege Level clear

Related Documentation • [show security screen statistics on page 106](#)

List of Sample Output [clear security screen statistics interface fab0 on page 197](#)
[clear security screen statistics interface fab0 node 0 on page 197](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security screen statistics interface fab0

```
user@host> clear security screen statistics interface fab0
node0:
```

```
-----
IDS statistics has been cleared.
```

```
node1:
```

```
-----
IDS statistics has been cleared.
```

Sample Output

clear security screen statistics interface fab0 node 0

```
user@host> clear security screen statistics interface fab0 node 0
node0:
```

```
-----
IDS statistics has been cleared.
```


clear security screen statistics zone

Supported Platforms

Syntax	clear security screen statistics zone <i>zone-name</i> <node (<i>node-id</i> all local primary)>
Release Information	Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS.
Description	Clear IDS security screen statistics for a security zone.
Options	<ul style="list-style-type: none"> • zone zone-name—Name of the security zone for which to clear security screen statistics. • node—(Optional) For chassis cluster configurations, clear security screen statistics for a security zone on a specific node. <ul style="list-style-type: none"> • <i>node-id</i>—Identification number of the node. It can be 0 or 1. • all—Clear all nodes. • local—Clear the local node. • primary—Clear the primary node.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show security screen statistics on page 106
List of Sample Output	clear security screen statistics zone abc node all on page 199 clear security screen statistics node 0 zone my-zone on page 199
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security screen statistics zone abc node all

```

user@host> clear security screen statistics zone abc node all
node0:
-----
IDS statistics has been cleared.
node1:
-----
IDS statistics has been cleared.
```

Sample Output

clear security screen statistics node 0 zone my-zone

```

user@host> clear security screen statistics node 0 zone my-zone
node0:
-----
IDS statistics has been cleared.
```


show security screen ids-option

Supported Platforms

Syntax show security screen ids-option
screen-name
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Junos OS Release 8.5. Support for **node** options added in Junos OS Release 9.0. Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10. Support for UDP **port scan** added in Junos OS Release 12.1X47-D10.

Description Display configuration information about the specified security screen.

- Options**
- **screen-name** —Name of the screen.
 - **node**—(Optional) For chassis cluster configurations, display the configuration status of the security screen on a specific node.
 - **node-id** —Identification number of the node. It can be 0 or 1.
 - **all**—Display information about all nodes.
 - **local**—Display information about the local node.
 - **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation

- [ids-option on page 70](#)

List of Sample Output [show security screen ids-option jscreen on page 203](#)
[show security screen ids-option jscreen \(IPv6\) on page 204](#)
[show security screen ids-option jscreen1 node all on page 204](#)

Output Fields [Table 4 on page 101](#) lists the output fields for the **show security screen ids-option** command. Output fields are listed in the approximate order in which they appear.

Table 7: show security screen ids-option Output Fields

Field Name	Field Description
TCP address sweep threshold	Number of microseconds for which the device accepts 10 TCP packets from the same remote source to different destination addresses.
TCP port scan threshold	Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers.
ICMP address sweep threshold	Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device.

Table 7: show security screen ids-option Output Fields (*continued*)

Field Name	Field Description
UDP flood threshold	Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.
UDP port scan threshold	Number of microseconds during which the device accepts packets from the same remote source IP with up to 10 different destination port numbers.
TCP winnuke	Enable or disable the detection of TCP WinNuke attacks.
TCP SYN flood attack threshold	Number of SYN packets per second required to trigger the SYN proxy response.
TCP SYN flood alarm threshold	Number of half-complete proxy connections per second at which the device makes entries in the event alarm log.
TCP SYN flood source threshold	Number of SYN segments to be received per second before the device begins dropping connection requests.
TCP SYN flood destination threshold	Number of SYN segments received per second before the device begins dropping connection requests.
TCP SYN flood timeout	Maximum length of time before a half-completed connection is dropped from the queue.
TCP SYN flood queue size	Number of proxy connection requests that can be held in the proxy connection queue before the device begins rejecting new connection requests.
ICMP large packet	Enable or disable the detection of any ICMP frame with an IP length greater than 1024 bytes.
UDP address sweep threshold	Number of microseconds for which the device accepts 10 UDP packets from the same remote source to different destination addresses.
IPv6 extension routing	Enable or disable the IPv6 extension routing screen option.
IPv6 extension shim6	Enable or disable the IPv6 extension shim6 screen option.
IPv6 extension fragment	Enable or disable the IPv6 extension fragment screen option.
IPv6 extension AH	Enable or disable the IPv6 extension Authentication Header Protocol screen option.
IPv6 extension ESP	Enable or disable the IPv6 extension Encapsulating Security Payload screen option.
IPv6 extension mobility	Enable or disable the IPv6 extension mobility screen option.
IPv6 extension HIP	Enable or disable the IPv6 extension Host Identify Protocol screen option.
IPv6 extension no next	Enable or disable the IPv6 extension no-next screen option.
IPv6 extension user-defined	Enable or disable the IPv6 extension user-defined screen option.

Table 7: show security screen ids-option Output Fields (*continued*)

Field Name	Field Description
IPv6 extension HbyH jumbo	Enable or disable the IPv6 extension HbyH jumbo screen option.
IPv6 extension HbyH RPL	Enable or disable the IPv6 extension HbyH RPL screen option.
IPv6 extension HbyH router alert	Enable or disable the IPv6 extension HbyH router screen option.
IPv6 extension HbyH quick start	Enable or disable the IPv6 extension HbyH quick-start screen option.
IPv6 extension HbyH CALIPSO	Enable or disable the IPv6 extension HbyH Common Architecture Label IPv6 Security Screen option.
IPv6 extension HbyH SMF DPD	Enable or disable the IPv6 extension HbyH Simplified Multicast Forwarding IPv6 Duplicate Packet Detection screen option.
IPv6 extension HbyH user-defined	Enable or disable the IPv6 extension HbyH user-defined screen option.
IPv6 extension Dst tunnel encap limit	Enable or disable the IPv6 extension distributed (network) storage tunnel encapsulation limit screen option.
IPv6 extension Dst home address	Enable or disable the IPv6 extension DST home address screen option.
IPv6 extension Dst ILNP nonce	Enable or disable the IPv6 extension DST Identifier-Locator Network Protocol nonce screen option.
IPv6 extension Dst line-id	Enable or disable the IPv6 extension DST line-ID screen option.
IPv6 extension Dst user-defined	Enable or disable the IPv6 extension DST user-defined screen option.
IPv6 extension header limit	Threshold for the number of IPv6 extension headers that can pass through the screen.
IPv6 malformed header	Enable or disable the IPv6 malformed header screen option.
ICMPv6 malformed header	Enable or disable the ICMPv6 malformed packet screen option.

Sample Output

show security screen ids-option jscreen

```

user@host> show security screen ids-option jscreen
Screen object status:
Name                                     Value
TCP port scan threshold                 5000
UDP port scan threshold                 10000
ICMP address sweep threshold             5000

```

Sample Output

show security screen ids-option jscreen (IPv6)

```
user@host> show security screen ids-option jscreen
```

```
Screen object status:
```

Name	Value
ICMP ping of death	enabled
.....	
IPv6 extension routing	enabled
IPv6 extension shim6	enabled
IPv6 extension fragment	enabled
IPv6 extension AH	enabled
IPv6 extension ESP	enabled
IPv6 extension mobility	enabled
IPv6 extension HIP	enabled
IPv6 extension no next	enabled
IPv6 extension user-defined	enabled
IPv6 extension HbyH jumbo	enabled
IPv6 extension HbyH RPL	enabled
IPv6 extension HbyH router alert	enabled
IPv6 extension HbyH quick start	enabled
IPv6 extension HbyH CALIPSO	enabled
IPv6 extension HbyH SMF DPD	enabled
IPv6 extension HbyH user-defined	enabled
IPv6 extension Dst tunnel encap limit	enabled
IPv6 extension Dst home address	enabled
IPv6 extension Dst ILNP nonce	enabled
IPv6 extension Dst line-id	enabled
IPv6 extension Dst user-defined	enabled
IPv6 extension header limit	20
IPv6 Malformed header	enabled
ICMPv6 malformed packet	enabled

Sample Output

show security screen ids-option jscreen1 node all

```
user@host> show security screen ids-option jscreen1 node all
```

```
node0:
```

```
-----  
Screen object status:
```

Name	Value
UDP flood threshold	1000
TCP winnuke	enabled
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	4000
TCP SYN flood destination threshold	4000
TCP SYN flood timeout	20
TCP SYN flood queue size	1024
ICMP large packet	enabled

```
node1:
```

```
-----  
Screen object status:
```

Name	Value
UDP flood threshold	1000

TCP winnuke	enabled
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	4000
TCP SYN flood destination threshold	4000
TCP SYN flood timeout	20
TCP SYN flood queue size	1024
ICMP large packet	enabled

show security screen statistics

Supported Platforms

Syntax show security screen statistics (zone *zone-name* | interface *interface-name*)
<logical-system (*logical-system-name* | all)>
<node (*node-id* | all | local | primary)>
<root-logical-system>

Release Information Command introduced in Release 8.5 of Junos OS. **node** options added in Release 9.0 of Junos OS. **logical-system all** option added in Junos OS Release 11.2R6. Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10.

Description Display intrusion detection service (IDS) security screen statistics.

- Options**
- **zone *zone-name***—Display screen statistics for this security zone.
 - **interface *interface-name***—Display screen statistics for this interface.
 - **logical-system**—(Optional) Display screen statistics for configured logical systems.
 - ***logical-system-name***—Display screen statistics for the named logical system.
 - **all**—Display screen statistics for all logical systems, including the master (root) logical system.
 - **node**—(Optional) For chassis cluster configurations, display screen statistics on a specific node.
 - ***node-id***—Identification number of a node. It can be 0 or 1.
 - **all**—Display information about all nodes.
 - **local**—Display information about the local node.
 - **primary**—Display information about the primary node.
 - **root-logical-system**—(Optional) Display screen statistics for the master logical system only.

Required Privilege Level view

- Related Documentation**
- [clear security screen statistics on page 96](#)
 - [clear security screen statistics interface on page 97](#)
 - [clear security screen statistics zone on page 99](#)
 - *Junos OS Logical Systems Library for Security Devices*

List of Sample Output [show security screen statistics zone scrzone on page 209](#)
[show security screen statistics zone untrust \(IPv6\) on page 209](#)
[show security screen statistics interface ge-0/0/3 on page 210](#)
[show security screen statistics interface ge-0/0/1 \(IPv6\) on page 210](#)

[show security screen statistics interface ge-0/0/1 node primary on page 211](#)
[show security screen statistics zone trust logical-system all on page 211](#)

Output Fields [Table 5 on page 107](#) lists the output fields for the **show security screen statistics** command. Output fields are listed in the approximate order in which they appear.

Table 8: show security screen statistics Output Fields

Field Name	Field Description
ICMP flood	Internet Control Message Protocol (ICMP) flood counter. An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
UDP flood	User Datagram Protocol (UDP) flood counter. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks. WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP port scan	Number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP address sweep	Number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.
IP tear drop	Number of teardrop attacks. Teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN flood	Number of TCP SYN attacks.
IP spoofing	Number of IP spoofs. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP ping of death	ICMP ping of death counter. Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP source route option	Number of IP source route attacks.
TCP address sweep	Number of TCP address sweeps.
TCP land attack	Number of land attacks. Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN fragment	Number of TCP SYN fragments.
TCP no flag	Number of TCP headers without flags set. A normal TCP segment header has at least one control flag set.
IP unknown protocol	Number of IPs.
IP bad options	Number of invalid options.

Table 8: show security screen statistics Output Fields (*continued*)

Field Name	Field Description
IP record route option	Number of packets with the IP record route option enabled. This option records the IP addresses of the network devices along the path that the IP packet travels.
IP timestamp option	Number of IP timestamp option attacks. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
IP security option	Number of IP security option attacks.
IP loose source route option	Number of IP loose source route option attacks. This option specifies a partial route list for a packet to take on its journey from source to destination.
IP strict source route option	Number of IP strict source route option attacks. This option specifies the complete route list for a packet to take on its journey from source to destination.
IP stream option	Number of stream option attacks. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.
ICMP fragment	Number of ICMP fragments. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP large packet	Number of large ICMP packets.
TCP SYN FIN	Number of TCP SYN FIN packets.
TCP FIN no ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.
Source session limit	Number of concurrent sessions that can be initiated from a source IP address.
TCP SYN-ACK-ACK proxy	Number of TCP flags enabled with SYN-ACK-ACK. To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold and SRX Series devices running Junos OS reject further connection requests from that IP address.
IP block fragment	Number of IP block fragments.
Destination session limit	Number of concurrent sessions that can be directed to a single destination IP address.
UDP address sweep	Number of UDP address sweeps.
IPv6 extension header	Number of packets filtered for the defined IPv6 extension headers.
IPv6 extension hop by hop option	Number of packets filtered for the defined IPv6 hop-by-hop option types.
IPv6 extension destination option	Number of packets filtered for the defined IPv6 destination option types.
IPv6 extension header limit	Number of packets filtered for crossing the defined IPv6 extension header limit.

Table 8: show security screen statistics Output Fields (*continued*)

IPv6 malformed header	Number of IPv6 malformed headers defined for the intrusion detection service (IDS).
ICMPv6 malformed packet	Number of ICMPv6 malformed packets defined for the IDS options.

Sample Output

show security screen statistics zone scrzone

```

user@host> show security screen statistics zone scrzone
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                    0
UDP flood                                     0
TCP winnuke                                   0
TCP port scan                                91
ICMP address sweep                           0
TCP sweep                                     0
UDP sweep                                     0
IP tear drop                                 0
TCP SYN flood                                0
IP spoofing                                  0
ICMP ping of death                           0
IP source route option                       0
TCP land attack                              0
TCP SYN fragment                             0
TCP no flag                                  0
IP unknown protocol                          0
IP bad options                               0
IP record route option                       0
IP timestamp option                         0
IP security option                           0
IP loose source route option                 0
IP strict source route option                0
IP stream option                             0
ICMP fragment                                0
ICMP large packet                            0
TCP SYN FIN                                  0
TCP FIN no ACK                               0
Source session limit                         0
TCP SYN-ACK-ACK proxy                        0
IP block fragment                            0
Destination session limit                    0

```

Sample Output

show security screen statistics zone untrust (IPv6)

```

user@host> show security screen statistics zone untrust
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                    0
UDP flood                                     0
TCP winnuke                                   0
.....
IPv6 extension header                        0
IPv6 extension hop by hop option             0

```

IPv6	extension destination option	0
IPv6	extension header limit	0
IPv6	malformed header	0
ICMPv6	malformed packet	0

Sample Output

show security screen statistics interface ge-0/0/3

```
user@host> show security screen statistics interface ge-0/0/3
Screen statistics:
IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
TCP winnuke               0
TCP port scan             91
ICMP address sweep        0
TCP sweep                 0
UDP sweep                 0
IP tear drop              0
TCP SYN flood             0
IP spoofing               0
ICMP ping of death        0
IP source route option    0
TCP land attack           0
TCP SYN fragment          0
TCP no flag               0
IP unknown protocol       0
IP bad options            0
IP record route option    0
IP timestamp option       0
IP security option        0
IP loose source route option 0
IP strict source route option 0
IP stream option          0
ICMP fragment             0
ICMP large packet         0
TCP SYN FIN               0
TCP FIN no ACK            0
Source session limit      0
TCP SYN-ACK-ACK proxy     0
IP block fragment         0
Destination session limit 0
```

Sample Output

show security screen statistics interface ge-0/0/1 (IPv6)

```
user@host> show security screen statistics interface ge-0/0/1
Screen statistics:
IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
.....
IPv6 extension header      0
IPv6 extension hop by hop option 0
IPv6 extension destination option 0
IPv6 extension header limit 0
```

IPv6 malformed header	0
ICMPv6 malformed packet	0

Sample Output

show security screen statistics interface ge-0/0/1 node primary

```
user@host> show security screen statistics interface ge-0/0/1 node primary
node0:
```

```
-----
Screen statistics:
IDS attack type      Statistics
ICMP flood           1
UDP flood             1
TCP winnuke          1
TCP port scan         1
ICMP address sweep    1
TCP sweep             1
UDP sweep             1
IP tear drop          1
TCP SYN flood         1
IP spoofing           1
ICMP ping of death    1
IP source route option 1
TCP land attack       1
TCP SYN fragment      1
TCP no flag           1
IP unknown protocol   1
IP bad options        1
IP record route option 1
IP timestamp option   1
IP security option     1
IP loose source route option 1
IP strict source route option 1
IP stream option      1
ICMP fragment         1
ICMP large packet     1
TCP SYN FIN           1
TCP FIN no ACK        1
Source session limit  1
TCP SYN-ACK-ACK proxy 1
IP block fragment     1
Destination session limit 1
```

Sample Output

show security screen statistics zone trust logical-system all

```
user@host> show security screen statistics zone trust logical-system all
Logical system: root-logical-system
Screen statistics:
```

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0

TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls1

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls2

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

PART 3

Suspicious Packet Attributes Feature Guide for Security Devices

- [Overview on page 217](#)
- [Configuration on page 227](#)
- [Administration on page 269](#)

CHAPTER 7

Overview

- [Attack Detection and Prevention on page 217](#)
- [ICMP and SYN Fragment Protection on page 218](#)
- [IP Protection on page 221](#)

Attack Detection and Prevention

- [Attack Detection and Prevention Overview on page 217](#)

Attack Detection and Prevention Overview

Supported Platforms [LN Series](#), [SRX Series](#)

The Juniper Networks Intrusion Detection and Prevention (IDP) feature, also known as a *stateful firewall*, detects and prevents attacks in network traffic.

An exploit can be either an information-gathering probe or an attack to compromise, disable, or harm a network or network resource. In some cases, the distinction between the two objectives of an exploit can be unclear. For example, a barrage of TCP SYN segments might be an IP address sweep with the intent of triggering responses from active hosts, or it might be a SYN flood attack with the intent of overwhelming a network so that it can no longer function properly. Furthermore, because an attacker usually precedes an attack by performing reconnaissance on the target, we can consider information-gathering efforts as a precursor to an impending attack—that is, they constitute the first stage of an attack. Thus, the term *exploit* encompasses both reconnaissance and attack activities, and the distinction between the two is not always clear.

Juniper Networks provides various detection and defense mechanisms at the zone and policy levels to combat exploits at all stages of their execution:

- Screen options at the zone level.
- Firewall policies at the inter-, intra-, and super-zone policy levels (*super-zone* here means in global policies, where no security zones are referenced).

To secure all connection attempts, Junos OS uses a dynamic packet-filtering method known as stateful inspection. Using this method, Junos OS identifies various components in the IP packet and TCP segment headers—source and destination IP addresses, source

and destination port numbers, and packet sequence numbers—and maintains the state of each TCP session and pseudo UDP session traversing the firewall. (Junos OS also modifies session states based on changing elements such as dynamic port changes or session termination.) When a responding TCP packet arrives, Junos OS compares the information reported in its header with the state of its associated session stored in the inspection table. If they match, the responding packet is allowed to pass the firewall. If the two do not match, the packet is dropped.

Junos OS screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone. Junos OS then applies firewall policies, which can contain content filtering and IDP components, to the traffic that passes the screen filters.

Related Documentation • [Denial-of-Service Attacks Feature Guide for Security Devices](#)

ICMP and SYN Fragment Protection

- [Suspicious Packet Attributes Overview on page 218](#)
- [Understanding ICMP Fragment Protection on page 218](#)
- [Understanding Large ICMP Packet Protection on page 219](#)
- [Understanding SYN Fragment Protection on page 220](#)

Suspicious Packet Attributes Overview

Supported Platforms [LN Series, SRX Series](#)

Attackers can craft packets to perform reconnaissance or launch denial-of-service (DoS) attacks. Sometimes it is unclear what the intent of a crafted packet is, but the very fact that it is crafted suggests that it is being put to some kind of insidious use.

The following topics describe screen options that block suspicious packets that might contain hidden threats:

- [Understanding ICMP Fragment Protection on page 218](#)
- [Understanding Large ICMP Packet Protection on page 219](#)
- [Understanding Bad IP Option Protection on page 222](#)
- [Understanding Unknown Protocol Protection on page 223](#)
- [Understanding IP Packet Fragment Protection on page 224](#)
- [Understanding SYN Fragment Protection on page 220](#)

Related Documentation • [Suspicious Packet Attributes Feature Guide for Security Devices](#)

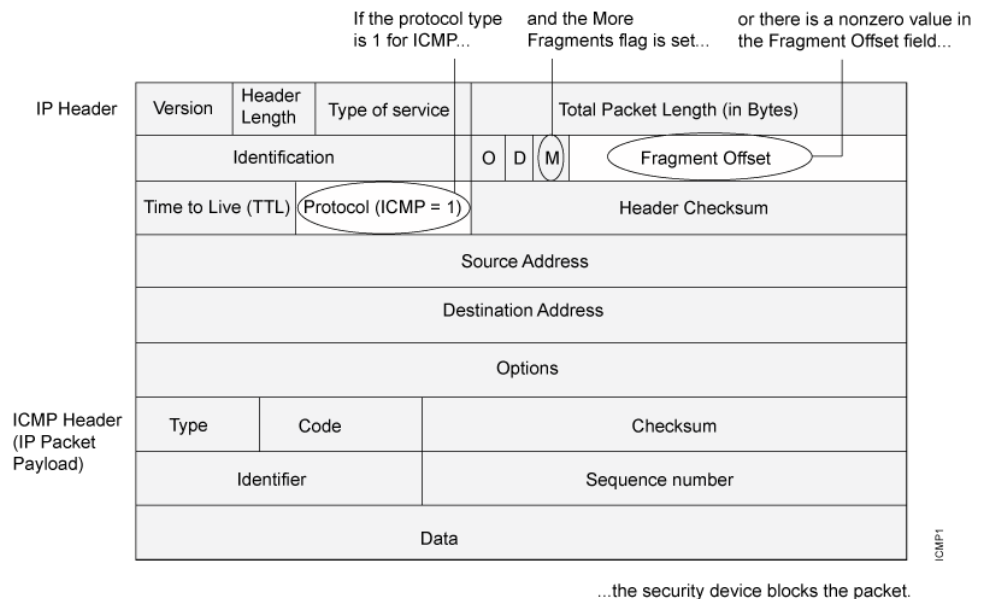
Understanding ICMP Fragment Protection

Supported Platforms [LN Series, SRX Series](#)

Internet Control Message Protocol (ICMP) provides error reporting and network probe capabilities. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.

When you enable the ICMP fragment protection screen option, Junos OS blocks any ICMP packet that has the More Fragments flag set or that has an offset value indicated in the offset field. See [Figure 25 on page 219](#).

Figure 25: Blocking ICMP Fragments



NOTE: Junos OS supports ICMP fragment protection for ICMPv6 packets.

Related Documentation

- *Suspicious Packet Attributes Feature Guide for Security Devices*

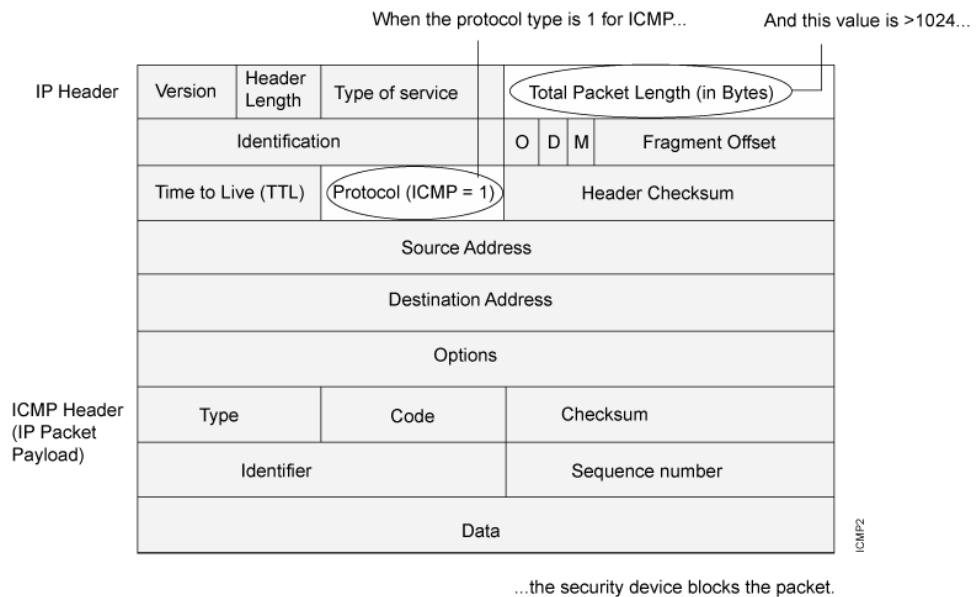
Understanding Large ICMP Packet Protection

Supported Platforms [LN Series, SRX Series](#)

Internet Control Message Protocol (ICMP) provides error reporting and network probe capabilities. Because ICMP packets contain very short messages, there is no legitimate reason for large ICMP packets. If an ICMP packet is unusually large, something is amiss.

For example, the SRX 210 uses ICMP as a channel for transmitting covert messages. The presence of large ICMP packets might expose a compromised machine acting as a SRX 210 agent. It also might indicate some other kind of questionable activity. See [Figure 26 on page 220](#).

Figure 26: Blocking Large ICMP Packets



When you enable the large size ICMP packet protection screen option, Junos OS drops ICMP packets with a length greater than 1024 bytes.



NOTE: Junos OS supports large ICMP packet protection for both ICMP and ICMPv6 packets.

Related Documentation

- *Suspicious Packet Attributes Feature Guide for Security Devices*

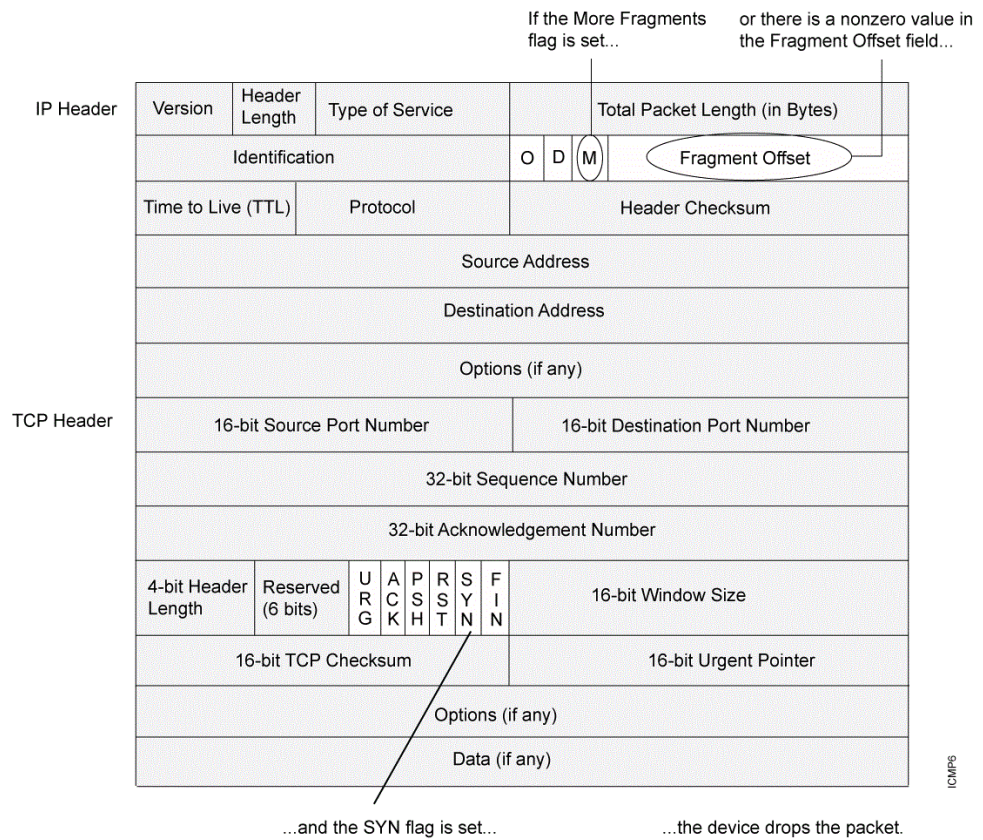
Understanding SYN Fragment Protection

Supported Platforms LN Series, SRX Series

The IP encapsulates a TCP SYN segment in the IP packet that initiates a TCP connection. Because the purpose of this packet is to initiate a connection and invoke a SYN/ACK segment in response, the SYN segment typically does not contain any data. Because the IP packet is small, there is no legitimate reason for it to be fragmented.

A fragmented SYN packet is anomalous, and, as such, it is suspect. To be cautious, block such unknown elements from entering your protected network. See [Figure 27 on page 221](#).

Figure 27: SYN Fragments



When you enable the SYN fragment detection screen option, Junos OS detects packets when the IP header indicates that the packet has been fragmented and the SYN flag is set in the TCP header. Junos OS records the event in the screen counters list for the ingress interface.



NOTE: Junos OS supports SYN fragment protection for both IPv4 and IPv6 packets.

Related Documentation

- [Suspicious Packet Attributes Feature Guide for Security Devices](#)

IP Protection

- [Suspicious Packet Attributes Overview on page 222](#)
- [Understanding Bad IP Option Protection on page 222](#)
- [Understanding Unknown Protocol Protection on page 223](#)
- [Understanding IP Packet Fragment Protection on page 224](#)

Suspicious Packet Attributes Overview

Supported Platforms [LN Series](#), [SRX Series](#)

Attackers can craft packets to perform reconnaissance or launch denial-of-service (DoS) attacks. Sometimes it is unclear what the intent of a crafted packet is, but the very fact that it is crafted suggests that it is being put to some kind of insidious use.

The following topics describe screen options that block suspicious packets that might contain hidden threats:

- [Understanding ICMP Fragment Protection on page 218](#)
- [Understanding Large ICMP Packet Protection on page 219](#)
- [Understanding Bad IP Option Protection on page 222](#)
- [Understanding Unknown Protocol Protection on page 223](#)
- [Understanding IP Packet Fragment Protection on page 224](#)
- [Understanding SYN Fragment Protection on page 220](#)

**Related
Documentation**

- *Suspicious Packet Attributes Feature Guide for Security Devices*

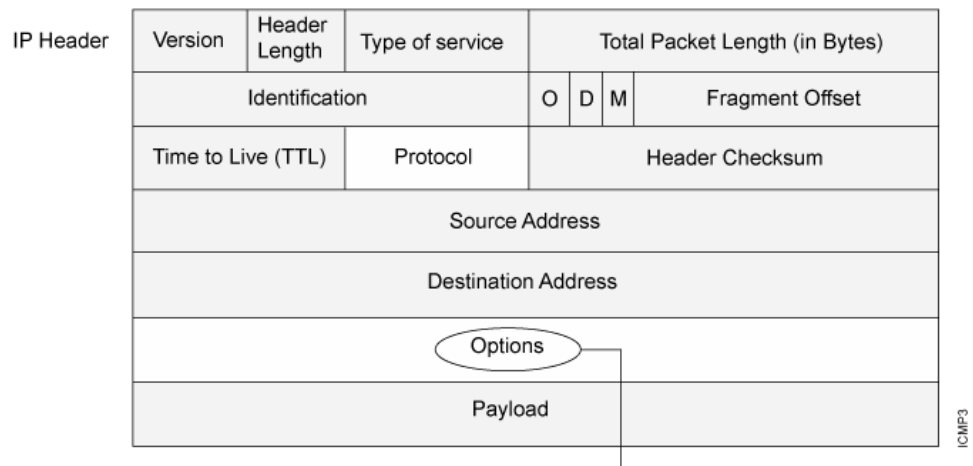
Understanding Bad IP Option Protection

Supported Platforms [LN Series](#), [SRX Series](#)

The IP standard RFC 791, *Internet Protocol*, specifies a set of eight options that provide special routing controls, diagnostic tools, and security. Although the original, intended uses for these options served worthy ends, people have figured out ways to twist these options to accomplish less commendable objectives.

Either intentionally or accidentally, attackers sometimes configure IP options incorrectly, producing either incomplete or malformed fields. Regardless of the intentions of the person who crafted the packet, the incorrect formatting is anomalous and potentially harmful to the intended recipient. See [Figure 28 on page 223](#).

Figure 28: Incorrectly Formatted IP Options



If the IP options are incorrectly formatted, the security device records the event in the screen counters for the ingress interface.

When you enable the bad IP option protection screen option, Junos OS blocks packets when any IP option in the IP packet header is incorrectly formatted. Additionally, Junos OS records the event in the event log.



NOTE: Junos OS supports bad IP option protection for both IPv4 and IPv6 packets.

Related Documentation

- [Suspicious Packet Attributes Feature Guide for Security Devices](#)

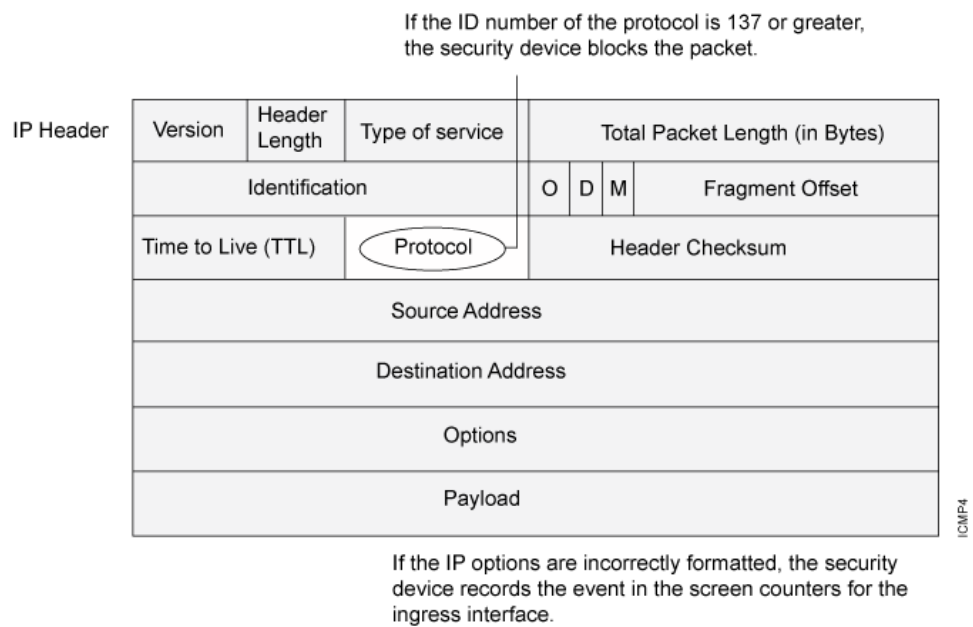
Understanding Unknown Protocol Protection

Supported Platforms [LN Series, SRX Series](#)

Based on RFC 1700, the protocol types with ID numbers of 137 or greater are reserved and undefined at this time. Precisely because these protocols are undefined, there is no way to know in advance if a particular unknown protocol is benign or malicious.

Unless your network makes use of a nonstandard protocol with an ID number of 137 or greater, a cautious stance is to block such unknown elements from entering your protected network. See [Figure 29 on page 224](#).

Figure 29: Unknown Protocols



When you enable the unknown protocol protection screen option, Junos OS drops packets when the protocol field contains a protocol ID number of 137 or greater by default.



NOTE: When you enable the unknown protocol protection screen option for IPv6 protocol, Junos OS drops packets when the protocol field contains a protocol ID number of 139 or greater by default.

Related Documentation

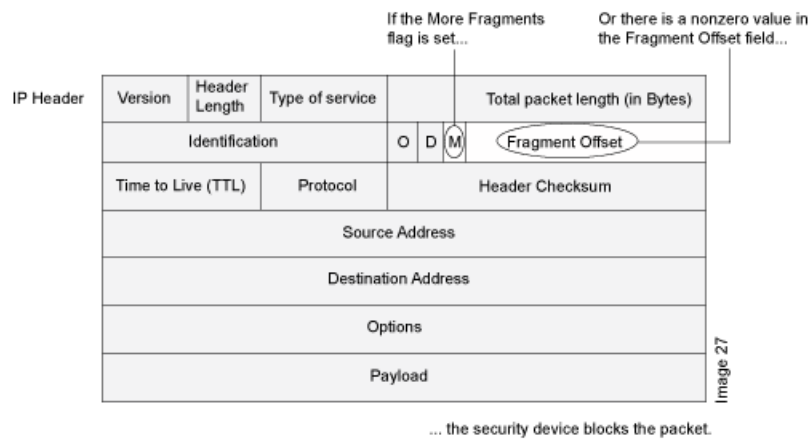
- *Suspicious Packet Attributes Feature Guide for Security Devices*

Understanding IP Packet Fragment Protection

Supported Platforms [LN Series](#), [SRX Series](#)

As packets traverse different networks, it is sometimes necessary to break a packet into smaller pieces (fragments) based upon the maximum transmission unit (MTU) of each network. IP fragments might contain an attacker's attempt to exploit the vulnerabilities in the packet reassembly code of specific IP stack implementations. When the victim receives these packets, the results can range from processing the packets incorrectly to crashing the entire system. See [Figure 30 on page 225](#).

Figure 30: IP Packet Fragments



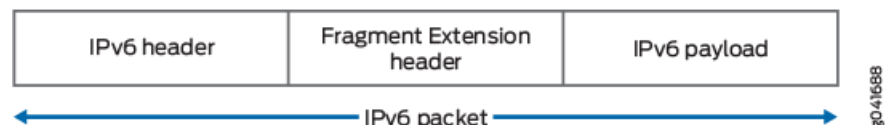
When you enable Junos OS to deny IP fragments on a security zone, it blocks all IP packet fragments that it receives at interfaces bound to that zone.



NOTE: Junos OS supports IP fragment protection for both IPv4 and IPv6 packets.

In IPv6 packets, fragment information is not present in the IPv6 header. The fragment information is present in the fragment extension header, which is responsible for IPv6 fragmentation and reassembly. The source node inserts the fragment extension header between the IPv6 header and the payload header if fragmentation is required. See [Figure 31 on page 225](#).

Figure 31: IPv6 Packet



The general format of the fragment extension header is shown in [Figure 32 on page 225](#).

Figure 32: Fragment Extension Header



Related Documentation

- [Suspicious Packet Attributes Feature Guide for Security Devices](#)

CHAPTER 8

Configuration

- [ICMP and SYN Fragment Protection on page 227](#)
- [IP Protection on page 230](#)
- [Configuration Statements on page 232](#)

ICMP and SYN Fragment Protection

- [Example: Blocking Fragmented ICMP Packets on page 227](#)
- [Example: Blocking Large ICMP Packets on page 228](#)
- [Example: Dropping IP Packets Containing SYN Fragments on page 229](#)

Example: Blocking Fragmented ICMP Packets

Supported Platforms [LN Series, SRX Series](#)

This example shows how to block fragmented ICMP packets.

Requirements

Before you begin, Understand ICMP fragment protection. See “[Suspicious Packet Attributes Overview](#)” on page 218.

Overview

When you enable the ICMP fragment protection screen option, Junos OS blocks any ICMP packet that has the more fragments flag set or that has an offset value indicated in the offset field.

In this example, you configure the ICMP fragment screen to block fragmented ICMP packets originating from the zone1 security zone.

Configuration

Step-by-Step Procedure

To block fragmented ICMP packets:

1. Configure the screen.

 [edit]
 user@host# **set security screen ids-option icmp-fragment icmp fragment**
2. Configure a security zone.

```
[edit]
user@host# set security zones security-zone zone1 screen icmp-fragment
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen statistics zone *zone-name*** command.

Related Documentation

- *Suspicious Packet Attributes Feature Guide for Security Devices*

Example: Blocking Large ICMP Packets

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to block large ICMP packets.

Requirements

Before you begin, Understand large ICMP packet protection. See “[Suspicious Packet Attributes Overview](#)” on page 218.

Overview

When you enable the large ICMP packet protection screen option, Junos OS drops ICMP packets that are larger than 1024 bytes.

In this example, you configure the ICMP large screen to block large ICMP packets originating from the zone1 security zone.

Configuration

Step-by-Step Procedure

To block large ICMP packets:

1. Configure the screen.

```
[edit]
user@host# set security screen ids-option icmp-large icmp large
```

2. Configure a security zone.

```
[edit]
user@host# set security zones security-zone zone1 screen icmp-large
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen statistics zone *zone-name*** command.

Related Documentation

- *Suspicious Packet Attributes Feature Guide for Security Devices*

Example: Dropping IP Packets Containing SYN Fragments

Supported Platforms LN Series, SRX Series

This example shows how to drop IP packets containing SYN fragments.

Requirements

Before you begin, Understand IP packet fragment protection. See “[Suspicious Packet Attributes Overview](#)” on page 218.

Overview

When you enable the SYN fragment detection screen option, Junos OS detects packets when the IP header indicates that the packet has been fragmented and the SYN flag is set in the TCP header. Also, Junos OS records the event in the screen counters list for the ingress interface.

In this example, you configure the SYN fragment screen to drop fragmented SYN packets originating from the zone1 security zone.

Configuration

Step-by-Step Procedure

To drop IP packets containing SYN fragments:

1. Configure the screen.

```
[edit]
user@host# set security screen ids-option syn-frag tcp syn-frag
```
2. Configure the security zone.

```
[edit]
user@host# set security zones security-zone zone1 screen syn-frag
```
3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen statistics zone *zone-name*** command.

Related Documentation

- *Suspicious Packet Attributes Feature Guide for Security Devices*

IP Protection

- [Example: Blocking IP Packets with Incorrectly Formatted Options on page 230](#)
- [Example: Dropping Packets Using an Unknown Protocol on page 231](#)
- [Example: Dropping Fragmented IP Packets on page 231](#)

Example: Blocking IP Packets with Incorrectly Formatted Options

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to block large ICMP packets with incorrectly formatted options.

Requirements

Before you begin, Understand bad IP option protection. See “[Suspicious Packet Attributes Overview](#)” on page 218.

Overview

When you enable the bad IP option protection screen option, Junos OS blocks packets when any IP option in the IP packet header is incorrectly formatted. Additionally, Junos OS records the event in the event log.

In this example, you configure the IP bad option screen to block large ICMP packets originating from the zone1 security zone.

Configuration

Step-by-Step Procedure

To detect and block IP packets with incorrectly formatted IP options:

1. Configure the screen.

[edit]

```
user@host# set security screen ids-option ip-bad-option ip bad-option
```



NOTE: Currently this screen option is applicable only to IPv4.

2. Configure a security zone.

[edit]

```
user@host# set security zones security-zone zone1 screen ip-bad-option
```

3. If you are done configuring the device, commit the configuration.

[edit]

```
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen statistics zone zone-name** command.

Related Documentation • *Suspicious Packet Attributes Feature Guide for Security Devices*

Example: Dropping Packets Using an Unknown Protocol

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to drop packets using an unknown protocol.

Requirements

Before you begin, Understand unknown protocol protection. See “[Suspicious Packet Attributes Overview](#)” on page 218.

Overview

When you enable the unknown protocol protection screen option, Junos OS drops packets when the protocol field contains a protocol ID number of 137 or greater by default.

In this example, you configure the unknown protocol screen to block packets with an unknown protocol originating from the zone1 security zone.

Configuration

Step-by-Step Procedure

To drop packets that use an unknown protocol:

1. Configure the unknown protocol screen.

```
[edit]
user@host# set security screen ids-option unknown-protocol ip unknown-protocol
```
2. Configure a security zone.

```
[edit]
user@host# set security zones security-zone zone1 screen unknown-protocol
```
3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen statistics zone *zone-name*** command.

Related Documentation • *Suspicious Packet Attributes Feature Guide for Security Devices*

Example: Dropping Fragmented IP Packets

Supported Platforms [LN Series](#), [SRX Series](#)

This example shows how to drop fragmented IP packets.

Requirements

Before you begin, Understand IP packet fragment protection. See [“Suspicious Packet Attributes Overview”](#) on page 218.

Overview

When this feature is enabled, Junos OS denies IP fragments on a security zone and blocks all IP packet fragments that are received at interfaces bound to that zone.

In this example, you configure the block fragment screen to drop fragmented IP packets originating from the zone1 security zone.

Configuration

Step-by-Step Procedure

To drop fragmented IP packets:

1. Configure the screen.

```
[edit]  
user@host# set security screen ids-option block-frag ip block-frag
```
2. Configure the security zone.

```
[edit]  
user@host# set security zones security-zone zone1 screen block-frag
```
3. If you are done configuring the device, commit the configuration.

```
[edit]  
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security screen statistics zone *zone-name*** command.

Related Documentation

- [Suspicious Packet Attributes Feature Guide for Security Devices](#)

Configuration Statements

- [\[edit security screen\] Hierarchy Level](#) on page 233
- [attack-threshold](#) on page 236
- [description \(Security Screen\)](#) on page 237
- [destination-ip-based](#) on page 238
- [destination-threshold](#) on page 239
- [fin-no-ack](#) on page 240
- [flood \(Security ICMP\)](#) on page 241
- [flood \(Security UDP\)](#) on page 242
- [icmp](#) on page 243

- [icmp \(Security Screen\) on page 243](#)
- [ids-option on page 244](#)
- [ip \(Security Screen\) on page 247](#)
- [ip-sweep on page 249](#)
- [land on page 250](#)
- [limit-session on page 250](#)
- [ping-death on page 251](#)
- [port-scan on page 252](#)
- [screen \(Security Zones\) on page 253](#)
- [source-ip-based on page 253](#)
- [source-threshold on page 254](#)
- [syn-ack-ack-proxy on page 255](#)
- [syn-check-required on page 255](#)
- [syn-fin on page 256](#)
- [syn-flood on page 257](#)
- [syn-flood-protection-mode on page 258](#)
- [syn-frag on page 258](#)
- [tcp \(Security Screen\) on page 259](#)
- [tcp-no-flag on page 260](#)
- [tcp-sweep on page 261](#)
- [timeout \(Security Screen\) on page 262](#)
- [traceoptions \(Security Screen\) on page 263](#)
- [udp \(Security Screen\) on page 265](#)
- [udp-sweep on page 266](#)
- [white-list on page 267](#)
- [winnuke on page 268](#)

[edit security screen] Hierarchy Level

Supported Platforms [LN Series, SRX Series](#)

```

security {
  screen {
    ids-option screen-name {
      alarm-without-drop;
      description text;
      icmp {
        flood {
          threshold number;
        }
        fragment;
        icmpv6-malformed;
        ip-sweep {

```

```
        threshold number;  
    }  
    large;  
    ping-death;  
}  
ip {  
    bad-option;  
    block-frag;  
    ipv6-extension-header {  
        AH-header;  
        ESP-header;  
        HIP-header;  
        destination-header {  
            ILNP-nonce-option;  
            home-address-option;  
            line-identification-option;  
            tunnel-encapsulation-limit-option;  
            user-defined-option-type low | <to high>;  
        }  
        fragment-header;  
        hop-by-hop-header {  
            CALIPSO-option;  
            RPL-option;  
            SFM-DPD-option;  
            jumbo-payload-option;  
            quick-start-option;  
            router-alert-option;  
            user-defined-option-type low | <to high>;  
        }  
        mobility-header;  
        no-next-header;  
        routing-header;  
        shim6-header  
        user-defined-option-type low | <to high>;  
    }  
    ipv6-extension-header-limit limit;  
    ipv6-malformed-header;  
    loose-source-route-option;  
    record-route-option;  
    security-option;  
    source-route-option;  
    spoofing;  
    stream-option;  
    strict-source-route-option;  
    tear-drop;  
    timestamp-option;  
    unknown-protocol;  
}  
limit-session {  
    destination-ip-based number;  
    source-ip-based number;  
}  
tcp {  
    fin-no-ack;  
    land;  
    port-scan {
```

```
threshold number;
}
syn-ack-ack-proxy {
    threshold number;
}
syn-fin;
syn-flood {
    alarm-threshold number;
    attack-threshold number;
    destination-threshold number;
    source-threshold number;
    timeout seconds;
    white-list name {
        destination-address destination-address;
        source-address source-address;
    }
}
syn-frag;
tcp-no-flag;
tcp-sweep {
    threshold threshold number;
}
winnuke;
}
udp {
    flood {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
}
}
traceoptions {
    file filename {
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
```

Related Documentation

- *Security Configuration Statement Hierarchy*
- *Junos OS Logical Systems Library for Security Devices*

attack-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `attack-threshold number;`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Define the number of SYN packets per second required to trigger the SYN proxy response.

Options *number*—Number of SYN packets per second required to trigger the SYN proxy response.

Range: 1 through 500,000 per second

Default: 200 per second



NOTE: For SRX Series devices, the applicable range is 1 through 1,000,000 per second.

Required Privilege security—To view this statement in the configuration.

Level security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)
- [destination-threshold on page 65](#)

description (Security Screen)

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `description text;`

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 12.1 of Junos OS.

Description Specify descriptive text for a screen.



NOTE: The descriptive text should not include characters, such as "<", ">", "&", or "\n".

Options *text*—Descriptive text about a screen.

Range: 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

Required Privilege security—To view this statement in the configuration.

Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

destination-ip-based

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax destination-ip-based *number*;

Hierarchy Level [edit security screen ids-option *screen-name* limit-session]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Limit the number of concurrent sessions the device can direct to a single destination IP address.

Options *number*—Maximum number of concurrent sessions that can be directed to a destination IP address.

Range: 1 through 1,000,000

Default: 128



NOTE: For SRX Series devices, the applicable range is 1 through 8,000,000.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

destination-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax destination-threshold *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based only on the destination IP address, regardless of the destination port number.

Options *number* —Number of SYN segments received per second before the device begins dropping connection requests.

Range: 4 through 500,000 per second

Default: 2048 per second



NOTE: For SRX Series devices, the applicable range is 4 through 1,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)
- [attack-threshold on page 62](#)

fin-no-ack

Supported Platforms	LN Series , SRX Series
Syntax	fin-no-ack;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of an illegal combination of flags, and reject packets that have this combination.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

flood (Security ICMP)

Supported Platforms

Syntax flood {
 threshold *number*;
 }

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the device to detect and prevent Internet Control Message Protocol (ICMP) floods. An ICMP flood occurs when ICMP echo requests are broadcast with the purpose of flooding a system with so much data that it first slows down, and then times out and is disconnected. The threshold defines the number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Options **threshold *number*** —Number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Range: 1 through 1,000,000 per second

Default: 1,000 per second



NOTE: For SRX Series devices the applicable range is 1 through 4,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation • [flood \(Security UDP\) on page 68](#)
 • *Security Configuration Statement Hierarchy*

flood (Security UDP)

Supported Platforms

Syntax flood {
 threshold *number*;
 }

Hierarchy Level [edit security screen ids-option *screen-name* udp]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the device to detect and prevent UDP floods. UDP flooding occurs when an attacker sends UDP packets to slow down the system to the point that it can no longer process valid connection requests.

The threshold defines the number of UDP packets per second allowed to ping the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options threshold *number* —Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.

Range: 1 through 1,000,000 per second

Default: 1,000 per second



NOTE: For SRX series devices the applicable range is 1 through 4,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*
- [flood \(Security ICMP\) on page 67](#)

icmp

Supported Platforms	LN Series, SRX Series
Syntax	<pre>icmp{ destination-interface <i>interface-name</i>; }</pre>
Hierarchy Level	[edit services rpm probe-server]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Specify the port information for the ICMP server.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding ICMP Fragment Protection on page 218

icmp (Security Screen)

Supported Platforms	
Syntax	<pre>icmp { flood { threshold <i>number</i>; } fragment; icmpv6-malformed; ip-sweep { threshold <i>number</i>; } large; ping-death; }</pre>
Hierarchy Level	[edit security screen ids-option <i>screen-name</i>]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Configure ICMP intrusion detection service (IDS) options.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Security Configuration Statement Hierarchy

ids-option

Supported Platforms

Syntax `ids-option screen-name {`
 `alarm-without-drop;`
 `description text;`
 `icmp {`
 `flood {`
 `threshold number;`
 `}`
 `fragment;`
 `icmpv6-malformed;`
 `ip-sweep {`
 `threshold number;`
 `}`
 `large;`
 `ping-death;`
 `}`
 `ip {`
 `bad-option;`
 `block-frag;`
 `ipv6-extension-header {`
 `AH-header;`
 `ESP-header`
 `HIP-header;`
 `destination-header {`
 `ILNP-nonce-option;`
 `home-address-option;`
 `line-identification-option;`
 `tunnel-encapsulation-limit-option;`
 `user-defined-option-type low | <to high>;`
 `}`
 `fragment-header;`
 `hop-by-hop-header {`
 `CALIPSO-option;`
 `RPL-option;`
 `SFM-DPD-option;`
 `jumbo-payload-option;`
 `quick-start-option;`
 `router-alert-option;`
 `user-defined-option-type low | <to high>;`
 `}`
 `mobility-header;`
 `no-next-header;`
 `routing-header;`
 `shim6-header`
 `user-defined-option-type low | <to high>;`
 `}`
 `ipv6-extension-header-limit limit;`
 `ipv6-malformed-header;`
 `loose-source-route-option;`
 `record-route-option;`
 `security-option;`
 `source-route-option;`

```

spoofing;
stream-option;
strict-source-route-option;
tear-drop;
timestamp-option;
unknown-protocol;
}
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
tcp {
    fin-no-ack;
    land;
    port-scan {
        threshold number;
    }
    syn-ack-ack-proxy {
        threshold number;
    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
        threshold threshold number;
    }
    winnuke;
}
udp {
    flood {
        threshold number;
    }
    port-scan {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
}
}

```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Junos OS Release 8.5. Support for the **description** option added in Junos OS Release 12.1. Support for the port scan for UDP option added in Junos OS Release 12.1X47-D10.

Description Define screens for intrusion detection service (IDS).

Options **description text**—Descriptive text about screen.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

ip (Security Screen)

Supported Platforms

```
Syntax  ip {
        bad-option;
        block-frag;
        ipv6-extension-header {
            AH-header;
            ESP-header;
            HIP-header;
            destination-header {
                ILNP-nonce-option;
                home-address-option;
                line-identification-option;
                tunnel-encapsulation-limit-option;
                user-defined-option-type low | <to high>;
            }
            fragment-header;
            hop-by-hop-header {
                CALIPSO-option;
                RPL-option;
                SFM-DPD-option;
                jumbo-payload-option;
                quick-start-option;
                router-alert-option;
                user-defined-option-type low | <to high>;
            }
            mobility-header;
            no-next-header;
            routing-header;
            shim6-header
            user-defined-option-type low | <to high>;
        }
        ipv6-extension-header-limit limit;
        ipv6-malformed-header;
        loose-source-route-option;
        record-route-option;
        security-option;
        source-route-option;
        spoofing;
        stream-option;
        strict-source-route-option;
        tear-drop;
        timestamp-option;
        unknown-protocol;
    }
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for IPv6 bad-option extension header screens added in Junos OS Release 12.1X46-D10.

Description Configure IP layer IDS options.

- Options**
- **bad-option**—Detect and drop any packet with an incorrectly formatted IP option in the IP packet header. The device records the event in the screen counters list for the ingress interface. This screen option is applicable to IPv4 and IPv6.
 - **block-frag**—Enable IP packet fragmentation blocking.
 - **loose-source-route-option**—Detect packets where the IP option is 3 (loose source routing), and record the event in the screen counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other devices in between those specified. The type 0 routing header of the loose source route option is the only related header defined in IPv6 .
 - **record-route-option**—Detect packets where the IP option is 7 (record route), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **security-option**—Detect packets where the IP option is 2 (security), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **source-route-option**—Detect packets, and record the event in the screen counters list for the ingress interface.
 - **spoofing**—Prevent spoofing attacks. Spoofing attacks occur when unauthorized agents attempt to bypass firewall security by imitating valid client IP addresses. Using the spoofing option invalidates such false source IP address connections.

The default behavior is to base spoofing decisions on individual interfaces.
 - **stream-option**—Detect packets where the IP option is 8 (stream ID), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **strict-source-route-option**—Detect packets where the IP option is 9 (strict source routing), and record the event in the screen counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field. Currently, this screen option is applicable only to IPv4.
 - **tear-drop**—Block the teardrop attack. Teardrop attacks occur when fragmented IP packets overlap and cause the host attempting to reassemble the packets to crash. The teardrop option directs the device to drop any packets that have such a discrepancy.
 - **timestamp-option**—Detect packets where the IP option list includes option 4 (Internet timestamp), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
 - **unknown-protocol**—Discard all received IP frames with protocol numbers greater than 137 for IPv4 and 139 for IPv6. Such protocol numbers are undefined or reserved.

Required Privilege	security—To view this statement in the configuration.
Level	security-control—To add this statement to the configuration.

Related Documentation • [Security Configuration Statement Hierarchy](#)

ip-sweep

Supported Platforms [LN Series, SRX Series](#)

Syntax

```
ip-sweep {
    threshold number;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and prevent an IP Sweep attack. An IP Sweep attack occurs when an attacker sends ICMP echo requests (pings) to multiple destination addresses. If a target host replies, the reply reveals the target's IP address to the attacker. If the device receives 10 ICMP echo requests within the number of microseconds specified in this statement, it flags this as an IP Sweep attack, and rejects the 11th and all further ICMP packets from that host for the remainder of the second.

Options **threshold *number***—Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device. More than 10 requests from a host during this period triggers an IP Sweep attack response on the device during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation • [Security Configuration Statement Hierarchy](#)

land

Supported Platforms	LN Series , SRX Series
Syntax	land;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable prevention of Land attacks by combining the SYN flood defense with IP spoofing protection. Land attacks occur when an attacker sends spoofed IP packets with headers containing the target's IP address for the source and destination IP addresses. The attacker sends these packets with the SYN flag set to any available port. The packets induce the target to create empty sessions with itself, filling its session table and overwhelming its resources.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

limit-session

Supported Platforms	LN Series , SRX Series
Syntax	limit-session { destination-ip-based <i>number</i> ; source-ip-based <i>number</i> ; }
Hierarchy Level	[edit security screen ids-option <i>screen-name</i>]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Limit the number of concurrent sessions the device can initiate from a single source IP address or the number of sessions it can direct to a single destination IP address.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

ping-death

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax ping-death;

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and reject oversized and irregular ICMP packets. Although the TCP/IP specification requires a specific packet size, many ping implementations allow larger packet sizes. Larger packets can trigger a range of adverse system reactions, including crashing, freezing, and restarting.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

port-scan

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
port-scan {  
    threshold number;  
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Prevent port scan attacks. A port scan attack occurs when an attacker sends packets with different port numbers to scan available services. The attack succeeds if a port responds. To prevent this attack, the device internally logs the number of different ports scanned from a single remote source. For example, if a remote host scans 10 ports in 0.005 seconds (equivalent to 5000 microseconds, the default threshold setting), the device flags this behavior as a port scan attack, and rejects further packets from the remote source.

Options **threshold *number*** —Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers. If the number of ports during the threshold period reaches 10 or more, the device rejects additional packets from the source.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)

screen (Security Zones)

Supported Platforms

Syntax `screen screen-name;`

Hierarchy Level [edit security zones functional-zone management],
[edit security zones security-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify a security screen for a security zone.

Options *screen-name* —Name of the screen.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Security Zones and Interfaces Feature Guide for Security Devices*

source-ip-based

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `source-ip-based number;`

Hierarchy Level [edit security screen ids-option *screen-name* limit-session]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Limit the number of concurrent sessions the device can initiate from a single source IP address.

Options *number* —Maximum number of concurrent sessions that can be initiated from a source IP address.

Range: 1 through 1,000,000

Default: 128



NOTE: For SRX Series devices the applicable range is 1 through 8,000,000.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Security Configuration Statement Hierarchy*

source-threshold

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax `source-threshold number;`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the number of SYN segments that the device can receive per second from a single source IP address (regardless of the destination IP address and port number) before the device begins dropping connection requests from that source.

Options *number* —Number of SYN segments to be received per second before the device starts dropping connection requests.

Range: 4 through 500,000 per second

Default: 4000 per second



NOTE: For SRX Series devices the applicable range is 4 through 1,000,000 per second.

Required Privilege security—To view this statement in the configuration.

Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

syn-ack-ack-proxy

Supported Platforms	LN Series, SRX Series
Syntax	syn-ack-ack-proxy; { threshold <i>number</i> , }
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.
Description	Prevent the SYN-ACK-ACK attack, which occurs when the attacker establishes multiple telnet sessions without allowing each session to terminate. This behavior consumes all open slots, generating a denial-of-service (DoS) condition.
Options	threshold <i>number</i> — Number of connections from any single IP address. Range: 1 through 250,000 Default: 512
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Security Configuration Statement Hierarchy</i>

syn-check-required

Supported Platforms	LN Series, SRX Series
Syntax	syn-check-required;
Hierarchy Level	[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> then permit tcp-options]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Enable sync check per policy. The syn-check-required value overrides the global value no-syn-check.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Security Policies Feature Guide for Security Devices</i>

syn-fin

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax syn-fin;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of an illegal combination of flags that attackers can use to consume sessions on the target device, thus resulting in a denial-of-service (DoS) condition.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

syn-flood

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax

```
syn-flood {
    alarm-threshold number;
    attack-threshold number;
    destination-threshold number;
    source-threshold number;
    timeout seconds;
    white-list name {
        destination-address destination-address;
        source-address source-address;
    }
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure detection and prevention of SYN flood attacks. Such attacks occur when the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses.



NOTE: On all SRX Series devices, the TCP synchronization flood alarm threshold value does not indicate the number of packets dropped, however the value does show the packet information after the alarm threshold has been reached.

The synchronization cookie or proxy never drops packets; therefore the **alarm-without-drop (not drop)** action is shown in the system log.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

Related Documentation

- [Security Configuration Statement Hierarchy](#)

syn-flood-protection-mode

Supported Platforms	LN Series , SRX Series
Syntax	syn-flood-protection-mode (syn-cookie syn-proxy);
Hierarchy Level	[edit security flow]
Release Information	Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.
Description	Enable SYN cookie or SYN proxy defenses against SYN attacks. SYN flood protection mode is enabled globally on the device and is activated when the configured syn-flood attack-threshold value is exceeded.
Options	<ul style="list-style-type: none">• syn-cookie—Uses a cryptographic hash to generate a unique Initial Sequence Number (ISN). This is enabled by default.• syn-proxy—Uses a proxy to handle the SYN attack.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Flow-Based Processing Feature Guide for Security Devices</i>

syn-frag

Supported Platforms	LN Series , SRX Series
Syntax	syn-frag;
Hierarchy Level	[edit security screen ids-option <i>screen-name</i> tcp]
Release Information	Statement introduced in Release 8.5 of Junos OS.
Description	Enable detection of a SYN fragment attack and drops any packet fragments used for the attack. A SYN fragment attack floods the target host with SYN packet fragments. The host caches these fragments, waiting for the remaining fragments to arrive so it can reassemble them. The flood of connections that cannot be completed eventually fills the host's memory buffer. No further connections are possible, and damage to the host's operating system can occur.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>

tcp (Security Screen)

Supported Platforms

Syntax

```
tcp {
  fin-no-ack;
  land;
  port-scan {
    threshold number;
  }
  syn-ack-ack-proxy {
    threshold number;
  }
  syn-fin;
  syn-flood {
    alarm-threshold number;
    attack-threshold number;
    destination-threshold number;
    source-threshold number;
    timeout seconds;
    white-list name {
      destination-address destination-address;
      source-address source-address;
    }
  }
  syn-frag;
  tcp-no-flag;
  tcp-sweep {
    threshold threshold number;
  }
  winnuke;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure TCP-layer intrusion detection service (IDS) options.



NOTE: On all SRX Series devices, the TCP synchronization flood alarm threshold value does not indicate the number of packets dropped, however the value does show the packet information after the alarm threshold has been reached.

The synchronization cookie or proxy never drops packets; therefore the alarm-without-drop (not drop) action is shown in the system log.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

tcp-no-flag

Supported Platforms [LN Series](#), [SRX Series](#)

Syntax tcp-no-flag;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to drop illegal TCP packets with a missing or malformed flag field.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

tcp-sweep

Supported Platforms

Syntax tcp-sweep {
 threshold *number*;
 }

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the device to detect and prevent TCP sweep attack. In a TCP sweep attack, an attacker sends TCP SYN packets to the target device as part of the TCP handshake. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends TCP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as a TCP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further TCP packets from that host for the remainder of the specified threshold period.

Options **threshold *number***—Maximum number of microseconds during which up to 10 TCP SYN packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers TCP Sweep attack response on the router during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation • *Security Configuration Statement Hierarchy*

timeout (Security Screen)

Supported Platforms

Syntax `timeout seconds;`

Hierarchy Level `[edit security screen ids-option screen-name tcp syn-flood]`

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum length of time before a half-completed connection is dropped from the queue. You can decrease the timeout value until you see any connections dropped during normal traffic conditions.

Options **seconds** —Time interval before a half-completed connection is dropped from the queue.
Range: 1 through 50 seconds
Default: 20 seconds

Required Privilege Level `security`—To view this statement in the configuration.
 `security-control`—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

traceoptions (Security Screen)

Supported Platforms

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure screen tracing options.

To specify more than one tracing option, include multiple **flag** statements.

Options

- **file**—Configure the trace file options.

- **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
- **files number**—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10 files

- **match regular-expression**—Refine the output to include lines that contain the regular expression.
- **size maximum-file-size**—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: **x K** to specify KB, **x m** to specify MB, or **x g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
 - **all**—Trace all screen events
 - **configuration**—Trace screen configuration events
 - **flow**—Trace flow events
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• <i>Security Configuration Statement Hierarchy</i>
------------------------------	---

udp (Security Screen)

Supported Platforms

Syntax

```

udp {
    flood {
        threshold number;
    }
    udp-sweep {
        threshold threshold number;
    }
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the number of packets allowed per second to the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

udp-sweep

Supported Platforms

Syntax `udp-sweep {
 threshold number;
 }`

Hierarchy Level `[edit security screen ids-option screen-name udp]`

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the device to detect and prevent UDP sweep attack. In a UDP sweep attack, an attacker sends UDP packets to the target device. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends UDP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as an UDP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further UDP packets from that host for the remainder of the specified threshold period.

Options **threshold *number***—Maximum number of microseconds during which up to 10 UDP packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers an UDP Sweep attack response on the device during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

white-list

Supported Platforms [LN Series, SRX Series](#)

Syntax `white-list name {
 destination-address [address];
 source-address [address];
}`

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement introduced in Release 12.1 of Junos OS.

Description Configure a whitelist of IP addresses that are to be exempt from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process.

Both IP version 4 (IPv4) and IP version 6 (IPv6) whitelists are supported. Addresses in a whitelist must be all IPv4 or all IPv6. Each whitelist can have up to 32 IP address prefixes.

- Options**
- **destination-address *address***—Destination IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.
 - **source-address *address***—Source IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

winnuke

Supported Platforms [LN Series, SRX Series](#)

Syntax winnuke;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of attacks on Windows NetBios communications. Packets are modified as necessary and passed on. Each WinNuke attack triggers an attack log entry in the event alarm log.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- *Security Configuration Statement Hierarchy*

CHAPTER 9

Administration

- [Operational Commands on page 269](#)

Operational Commands

- [clear security screen statistics](#)
- [clear security screen statistics interface](#)
- [clear security screen statistics zone](#)
- [show security screen ids-option](#)
- [show security screen statistics](#)

clear security screen statistics

Supported Platforms

Syntax clear security screen statistics
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 9.0 of Junos OS.

Description Clear intrusion detection service (IDS) security screen statistics on the device.

Options **node**—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.

- **node-id** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level clear

Related Documentation

- [show security screen statistics on page 106](#)

List of Sample Output [clear security screen statistics node 0 on page 270](#)

Output Fields This command produces no output.

Sample Output

[clear security screen statistics node 0](#)

```
user@host> clear security screen statistics node 0
```


clear security screen statistics interface

Supported Platforms

Syntax clear security screen statistics interface *interface-name*

Release Information Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description Clear intrusion detection service (IDS) security screen statistics for an interface.

- Options**
- **interface** *interface-name* —Name of the interface on which to clear security screen statistics.
 - **node**—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.
 - **node-id** —Identification number of the node. It can be 0 or 1.
 - **all** —Clear all nodes.
 - **local** —Clear the local node.
 - **primary**—Clear the primary node.

Required Privilege Level clear

Related Documentation

- [show security screen statistics on page 106](#)

List of Sample Output [clear security screen statistics interface fab0 on page 271](#)
[clear security screen statistics interface fab0 node 0 on page 271](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security screen statistics interface fab0

```
user@host> clear security screen statistics interface fab0
node0:
```

```
-----
IDS statistics has been cleared.
```

```
node1:
```

```
-----
IDS statistics has been cleared.
```

Sample Output

clear security screen statistics interface fab0 node 0

```
user@host> clear security screen statistics interface fab0 node 0
node0:
```

```
-----
IDS statistics has been cleared.
```


clear security screen statistics zone

Supported Platforms

Syntax	clear security screen statistics zone <i>zone-name</i> <node (<i>node-id</i> all local primary)>
Release Information	Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS.
Description	Clear IDS security screen statistics for a security zone.
Options	<ul style="list-style-type: none"> • zone zone-name—Name of the security zone for which to clear security screen statistics. • node—(Optional) For chassis cluster configurations, clear security screen statistics for a security zone on a specific node. <ul style="list-style-type: none"> • <i>node-id</i>—Identification number of the node. It can be 0 or 1. • all—Clear all nodes. • local—Clear the local node. • primary—Clear the primary node.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show security screen statistics on page 106
List of Sample Output	clear security screen statistics zone abc node all on page 273 clear security screen statistics node 0 zone my-zone on page 273
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security screen statistics zone abc node all

```

user@host> clear security screen statistics zone abc node all
node0:
-----
IDS statistics has been cleared.
node1:
-----
IDS statistics has been cleared.
```

Sample Output

clear security screen statistics node 0 zone my-zone

```

user@host> clear security screen statistics node 0 zone my-zone
node0:
-----
IDS statistics has been cleared.
```


show security screen ids-option

Supported Platforms

Syntax show security screen ids-option
screen-name
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Junos OS Release 8.5. Support for **node** options added in Junos OS Release 9.0. Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10. Support for UDP **port scan** added in Junos OS Release 12.1X47-D10.

Description Display configuration information about the specified security screen.

- Options**
- **screen-name** —Name of the screen.
 - **node**—(Optional) For chassis cluster configurations, display the configuration status of the security screen on a specific node.
 - **node-id** —Identification number of the node. It can be 0 or 1.
 - **all**—Display information about all nodes.
 - **local**—Display information about the local node.
 - **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation

- [ids-option on page 70](#)

List of Sample Output [show security screen ids-option jscreen on page 277](#)
[show security screen ids-option jscreen \(IPv6\) on page 278](#)
[show security screen ids-option jscreen1 node all on page 278](#)

Output Fields [Table 4 on page 101](#) lists the output fields for the **show security screen ids-option** command. Output fields are listed in the approximate order in which they appear.

Table 9: show security screen ids-option Output Fields

Field Name	Field Description
TCP address sweep threshold	Number of microseconds for which the device accepts 10 TCP packets from the same remote source to different destination addresses.
TCP port scan threshold	Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers.
ICMP address sweep threshold	Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device.

Table 9: show security screen ids-option Output Fields (*continued*)

Field Name	Field Description
UDP flood threshold	Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.
UDP port scan threshold	Number of microseconds during which the device accepts packets from the same remote source IP with up to 10 different destination port numbers.
TCP winnuke	Enable or disable the detection of TCP WinNuke attacks.
TCP SYN flood attack threshold	Number of SYN packets per second required to trigger the SYN proxy response.
TCP SYN flood alarm threshold	Number of half-complete proxy connections per second at which the device makes entries in the event alarm log.
TCP SYN flood source threshold	Number of SYN segments to be received per second before the device begins dropping connection requests.
TCP SYN flood destination threshold	Number of SYN segments received per second before the device begins dropping connection requests.
TCP SYN flood timeout	Maximum length of time before a half-completed connection is dropped from the queue.
TCP SYN flood queue size	Number of proxy connection requests that can be held in the proxy connection queue before the device begins rejecting new connection requests.
ICMP large packet	Enable or disable the detection of any ICMP frame with an IP length greater than 1024 bytes.
UDP address sweep threshold	Number of microseconds for which the device accepts 10 UDP packets from the same remote source to different destination addresses.
IPv6 extension routing	Enable or disable the IPv6 extension routing screen option.
IPv6 extension shim6	Enable or disable the IPv6 extension shim6 screen option.
IPv6 extension fragment	Enable or disable the IPv6 extension fragment screen option.
IPv6 extension AH	Enable or disable the IPv6 extension Authentication Header Protocol screen option.
IPv6 extension ESP	Enable or disable the IPv6 extension Encapsulating Security Payload screen option.
IPv6 extension mobility	Enable or disable the IPv6 extension mobility screen option.
IPv6 extension HIP	Enable or disable the IPv6 extension Host Identify Protocol screen option.
IPv6 extension no next	Enable or disable the IPv6 extension no-next screen option.
IPv6 extension user-defined	Enable or disable the IPv6 extension user-defined screen option.

Table 9: show security screen ids-option Output Fields (*continued*)

Field Name	Field Description
IPv6 extension HbyH jumbo	Enable or disable the IPv6 extension HbyH jumbo screen option.
IPv6 extension HbyH RPL	Enable or disable the IPv6 extension HbyH RPL screen option.
IPv6 extension HbyH router alert	Enable or disable the IPv6 extension HbyH router screen option.
IPv6 extension HbyH quick start	Enable or disable the IPv6 extension HbyH quick-start screen option.
IPv6 extension HbyH CALIPSO	Enable or disable the IPv6 extension HbyH Common Architecture Label IPv6 Security Screen option.
IPv6 extension HbyH SMF DPD	Enable or disable the IPv6 extension HbyH Simplified Multicast Forwarding IPv6 Duplicate Packet Detection screen option.
IPv6 extension HbyH user-defined	Enable or disable the IPv6 extension HbyH user-defined screen option.
IPv6 extension Dst tunnel encap limit	Enable or disable the IPv6 extension distributed (network) storage tunnel encapsulation limit screen option.
IPv6 extension Dst home address	Enable or disable the IPv6 extension DST home address screen option.
IPv6 extension Dst ILNP nonce	Enable or disable the IPv6 extension DST Identifier-Locator Network Protocol nonce screen option.
IPv6 extension Dst line-id	Enable or disable the IPv6 extension DST line-ID screen option.
IPv6 extension Dst user-defined	Enable or disable the IPv6 extension DST user-defined screen option.
IPv6 extension header limit	Threshold for the number of IPv6 extension headers that can pass through the screen.
IPv6 malformed header	Enable or disable the IPv6 malformed header screen option.
ICMPv6 malformed header	Enable or disable the ICMPv6 malformed packet screen option.

Sample Output

show security screen ids-option jscreen

```

user@host> show security screen ids-option jscreen
Screen object status:
Name                                     Value
TCP port scan threshold                 5000
UDP port scan threshold                 10000
ICMP address sweep threshold             5000

```

Sample Output

show security screen ids-option jscreen (IPv6)

```
user@host> show security screen ids-option jscreen
```

Screen object status:

Name	Value
ICMP ping of death	enabled
.....	
IPv6 extension routing	enabled
IPv6 extension shim6	enabled
IPv6 extension fragment	enabled
IPv6 extension AH	enabled
IPv6 extension ESP	enabled
IPv6 extension mobility	enabled
IPv6 extension HIP	enabled
IPv6 extension no next	enabled
IPv6 extension user-defined	enabled
IPv6 extension HbyH jumbo	enabled
IPv6 extension HbyH RPL	enabled
IPv6 extension HbyH router alert	enabled
IPv6 extension HbyH quick start	enabled
IPv6 extension HbyH CALIPSO	enabled
IPv6 extension HbyH SMF DPD	enabled
IPv6 extension HbyH user-defined	enabled
IPv6 extension Dst tunnel encap limit	enabled
IPv6 extension Dst home address	enabled
IPv6 extension Dst ILNP nonce	enabled
IPv6 extension Dst line-id	enabled
IPv6 extension Dst user-defined	enabled
IPv6 extension header limit	20
IPv6 Malformed header	enabled
ICMPv6 malformed packet	enabled

Sample Output

show security screen ids-option jscreen1 node all

```
user@host> show security screen ids-option jscreen1 node all
```

node0:

Screen object status:

Name	Value
UDP flood threshold	1000
TCP winnuke	enabled
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	4000
TCP SYN flood destination threshold	4000
TCP SYN flood timeout	20
TCP SYN flood queue size	1024
ICMP large packet	enabled

node1:

Screen object status:

Name	Value
UDP flood threshold	1000

TCP winnuke	enabled
TCP SYN flood attack threshold	200
TCP SYN flood alarm threshold	512
TCP SYN flood source threshold	4000
TCP SYN flood destination threshold	4000
TCP SYN flood timeout	20
TCP SYN flood queue size	1024
ICMP large packet	enabled

show security screen statistics

Supported Platforms

Syntax show security screen statistics (zone *zone-name* | interface *interface-name*)
<logical-system (*logical-system-name* | all)>
<node (*node-id* | all | local | primary)>
<root-logical-system>

Release Information Command introduced in Release 8.5 of Junos OS. **node** options added in Release 9.0 of Junos OS. **logical-system all** option added in Junos OS Release 11.2R6. Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10.

Description Display intrusion detection service (IDS) security screen statistics.

- Options**
- **zone *zone-name***—Display screen statistics for this security zone.
 - **interface *interface-name***—Display screen statistics for this interface.
 - **logical-system**—(Optional) Display screen statistics for configured logical systems.
 - ***logical-system-name***—Display screen statistics for the named logical system.
 - **all**—Display screen statistics for all logical systems, including the master (root) logical system.
 - **node**—(Optional) For chassis cluster configurations, display screen statistics on a specific node.
 - ***node-id***—Identification number of a node. It can be 0 or 1.
 - **all**—Display information about all nodes.
 - **local**—Display information about the local node.
 - **primary**—Display information about the primary node.
 - **root-logical-system**—(Optional) Display screen statistics for the master logical system only.

Required Privilege Level view

- Related Documentation**
- [clear security screen statistics on page 96](#)
 - [clear security screen statistics interface on page 97](#)
 - [clear security screen statistics zone on page 99](#)
 - *Junos OS Logical Systems Library for Security Devices*

List of Sample Output [show security screen statistics zone scrzone on page 283](#)
[show security screen statistics zone untrust \(IPv6\) on page 283](#)
[show security screen statistics interface ge-0/0/3 on page 284](#)
[show security screen statistics interface ge-0/0/1 \(IPv6\) on page 284](#)

[show security screen statistics interface ge-0/0/1 node primary on page 285](#)
[show security screen statistics zone trust logical-system all on page 285](#)

Output Fields [Table 5 on page 107](#) lists the output fields for the **show security screen statistics** command. Output fields are listed in the approximate order in which they appear.

Table 10: show security screen statistics Output Fields

Field Name	Field Description
ICMP flood	Internet Control Message Protocol (ICMP) flood counter. An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
UDP flood	User Datagram Protocol (UDP) flood counter. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks. WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP port scan	Number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP address sweep	Number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.
IP tear drop	Number of teardrop attacks. Teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN flood	Number of TCP SYN attacks.
IP spoofing	Number of IP spoofs. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP ping of death	ICMP ping of death counter. Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP source route option	Number of IP source route attacks.
TCP address sweep	Number of TCP address sweeps.
TCP land attack	Number of land attacks. Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN fragment	Number of TCP SYN fragments.
TCP no flag	Number of TCP headers without flags set. A normal TCP segment header has at least one control flag set.
IP unknown protocol	Number of IPs.
IP bad options	Number of invalid options.

Table 10: show security screen statistics Output Fields (*continued*)

Field Name	Field Description
IP record route option	Number of packets with the IP record route option enabled. This option records the IP addresses of the network devices along the path that the IP packet travels.
IP timestamp option	Number of IP timestamp option attacks. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
IP security option	Number of IP security option attacks.
IP loose source route option	Number of IP loose source route option attacks. This option specifies a partial route list for a packet to take on its journey from source to destination.
IP strict source route option	Number of IP strict source route option attacks. This option specifies the complete route list for a packet to take on its journey from source to destination.
IP stream option	Number of stream option attacks. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.
ICMP fragment	Number of ICMP fragments. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP large packet	Number of large ICMP packets.
TCP SYN FIN	Number of TCP SYN FIN packets.
TCP FIN no ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.
Source session limit	Number of concurrent sessions that can be initiated from a source IP address.
TCP SYN-ACK-ACK proxy	Number of TCP flags enabled with SYN-ACK-ACK. To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold and SRX Series devices running Junos OS reject further connection requests from that IP address.
IP block fragment	Number of IP block fragments.
Destination session limit	Number of concurrent sessions that can be directed to a single destination IP address.
UDP address sweep	Number of UDP address sweeps.
IPv6 extension header	Number of packets filtered for the defined IPv6 extension headers.
IPv6 extension hop by hop option	Number of packets filtered for the defined IPv6 hop-by-hop option types.
IPv6 extension destination option	Number of packets filtered for the defined IPv6 destination option types.
IPv6 extension header limit	Number of packets filtered for crossing the defined IPv6 extension header limit.

Table 10: show security screen statistics Output Fields (*continued*)

IPv6 malformed header	Number of IPv6 malformed headers defined for the intrusion detection service (IDS).
ICMPv6 malformed packet	Number of ICMPv6 malformed packets defined for the IDS options.

Sample Output

show security screen statistics zone scrzone

```

user@host> show security screen statistics zone scrzone
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                    0
UDP flood                                    0
TCP winnuke                                   0
TCP port scan                                91
ICMP address sweep                           0
TCP sweep                                    0
UDP sweep                                    0
IP tear drop                                0
TCP SYN flood                                0
IP spoofing                                  0
ICMP ping of death                          0
IP source route option                      0
TCP land attack                              0
TCP SYN fragment                            0
TCP no flag                                  0
IP unknown protocol                         0
IP bad options                              0
IP record route option                      0
IP timestamp option                        0
IP security option                         0
IP loose source route option                0
IP strict source route option               0
IP stream option                           0
ICMP fragment                               0
ICMP large packet                           0
TCP SYN FIN                                 0
TCP FIN no ACK                              0
Source session limit                        0
TCP SYN-ACK-ACK proxy                      0
IP block fragment                          0
Destination session limit                   0

```

Sample Output

show security screen statistics zone untrust (IPv6)

```

user@host> show security screen statistics zone untrust
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                    0
UDP flood                                    0
TCP winnuke                                   0
.....
IPv6 extension header                        0
IPv6 extension hop by hop option            0

```

IPv6	extension destination option	0
IPv6	extension header limit	0
IPv6	malformed header	0
ICMPv6	malformed packet	0

Sample Output

show security screen statistics interface ge-0/0/3

```
user@host> show security screen statistics interface ge-0/0/3
Screen statistics:
IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
TCP winnuke               0
TCP port scan             91
ICMP address sweep        0
TCP sweep                 0
UDP sweep                 0
IP tear drop              0
TCP SYN flood             0
IP spoofing               0
ICMP ping of death        0
IP source route option    0
TCP land attack           0
TCP SYN fragment          0
TCP no flag               0
IP unknown protocol       0
IP bad options            0
IP record route option    0
IP timestamp option       0
IP security option        0
IP loose source route option 0
IP strict source route option 0
IP stream option          0
ICMP fragment             0
ICMP large packet         0
TCP SYN FIN               0
TCP FIN no ACK            0
Source session limit      0
TCP SYN-ACK-ACK proxy     0
IP block fragment         0
Destination session limit 0
```

Sample Output

show security screen statistics interface ge-0/0/1 (IPv6)

```
user@host> show security screen statistics interface ge-0/0/1
Screen statistics:
IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
.....
IPv6 extension header     0
IPv6 extension hop by hop option 0
IPv6 extension destination option 0
IPv6 extension header limit 0
```

IPv6 malformed header	0
ICMPv6 malformed packet	0

Sample Output

show security screen statistics interface ge-0/0/1 node primary

```
user@host> show security screen statistics interface ge-0/0/1 node primary
node0:
```

```
-----
Screen statistics:
IDS attack type      Statistics
ICMP flood           1
UDP flood            1
TCP winnuke          1
TCP port scan        1
ICMP address sweep   1
TCP sweep            1
UDP sweep            1
IP tear drop         1
TCP SYN flood        1
IP spoofing          1
ICMP ping of death   1
IP source route option 1
TCP land attack      1
TCP SYN fragment     1
TCP no flag          1
IP unknown protocol  1
IP bad options       1
IP record route option 1
IP timestamp option  1
IP security option   1
IP loose source route option 1
IP strict source route option 1
IP stream option     1
ICMP fragment        1
ICMP large packet    1
TCP SYN FIN          1
TCP FIN no ACK       1
Source session limit 1
TCP SYN-ACK-ACK proxy 1
IP block fragment    1
Destination session limit 1
```

Sample Output

show security screen statistics zone trust logical-system all

```
user@host> show security screen statistics zone trust logical-system all
Logical system: root-logical-system
Screen statistics:
```

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0

TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls1

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls2

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

PART 4

Index

- [Index on page 291](#)

Index

Symbols

#, comments in configuration statements.....	xvi
(), in syntax descriptions.....	xvi
< >, in syntax descriptions.....	xvi
[], in configuration statements.....	xvi
{ }, in configuration statements.....	xvi
(pipe), in syntax descriptions.....	xvi

A

address sweep.....	118
agents, zombie.....	4
attack detection	
overview.....	3, 117, 217
attack-threshold statement.....	62, 160, 236
attacks	
DOS.....	4, 7, 25
ICMP	
floods.....	19, 50
fragments.....	218
IP packet fragments.....	224
Land.....	21, 54
large ICMP packets.....	219
Ping of Death.....	23
session table floods.....	7, 129
SYN floods.....	12, 38
SYN fragments.....	220
Teardrop.....	24, 57
UDP floods.....	20, 52
unknown protocols.....	223
WinNuke.....	25, 58

B

braces, in configuration statements.....	xvi
brackets	
angle, in syntax descriptions.....	xvi
square, in configuration statements.....	xvi

C

clear security screen statistics	
command.....	96, 196, 270

clear security screen statistics interface	
command.....	97, 197, 271
clear security screen statistics zone	
command.....	99, 199, 273
comments, in configuration statements.....	xvi
conventions	
text and syntax.....	xv
cookies, SYN.....	17
curly braces, in configuration statements.....	xvi
customer support.....	xvii
contacting JTAC.....	xvii

D

DDoS.....	4
description statement.....	63, 161, 237
destination-ip-based statement.....	64, 162, 238
destination-threshold statement.....	65, 163, 239
documentation	
comments on.....	xvii
DoS	
firewall.....	10
session table floods.....	7, 129
DoS attacks.....	4
DoS Attacks	
network.....	11
OS-specific.....	22
dynamic packet filtering.....	3, 117, 217

F

FIN scans.....	129
FIN without ACK flag attack detection	
overview.....	126
fin-no-ack statement.....	66, 164, 240
flood statement	
(ICMP).....	67, 165, 241
(UDP).....	68, 166, 242
floods	
ICMP.....	19, 50
session table.....	7
SYN.....	12, 17, 38
UDP.....	20, 52
font conventions.....	xv

I

ICMP	
floods.....	19, 50
fragments.....	218
large packets.....	219

icmp statement	
(Security Screen).....	69, 167, 243
RPM.....	243
ids-option statement.....	70, 168, 244
inspections.....	3, 117, 217
IP options	
incorrectly formatted.....	222
loose source route.....	122
record route.....	122, 124
security.....	122, 124
source route.....	133
stream ID.....	122, 124
strict source route.....	122
timestamp.....	122, 124
IP packet fragments.....	224
IP spoofing.....	131
ip statement	
(Security Screen).....	73, 171, 247
ip-sweep statement.....	75, 173, 249

L

land attack detection	
configuration.....	54
overview.....	21
land statement.....	76, 174, 250
large statement.....	174
limit-session statement.....	76, 175, 250
loose source route IP detection	
configuration.....	122

M

manuals	
comments on.....	xvii

N

no-syn-check statement.....	175
no-syn-check-in-tunnel statement.....	176

P

parentheses, in syntax descriptions.....	xvi
ping of death attack protection	
configuration.....	56
overview.....	23
ping-death statement.....	77, 176, 251
policies	
core section.....	129
port scan attack protection	
overview.....	119, 120
port-scan statement.....	78, 177, 252

probes

network.....	118
open ports.....	119, 120
operating systems.....	125, 127

R

reconnaissance	
address sweep.....	118
FIN scans.....	129
IP options.....	121, 124
port scan.....	119, 120
SYN and FIN flags set.....	126
TCP packet without flags.....	127
reconnaissance deterrence	
IP address sweeps.....	118
blocking.....	118
overview.....	118, 125, 128
record route IP option.....	122, 124
RFCs	
1038, Revised IP Security Option.....	122
791, Internet Protocol.....	121, 122
793, Transmission Control Protocol.....	126

S

screen

address sweep.....	118
bad IP options, drop.....	222
FIN with no ACK.....	129
FIN without ACK flag, drop.....	126
ICMP	
fragments, block.....	218
ICMP floods.....	19, 50
IP options.....	121, 124
IP packet fragments, block.....	224
IP spoofing.....	131
Land attacks.....	21, 54
large ICMP packets, block.....	219
loose source route IP option, detect.....	133
Ping of Death.....	23
port scan.....	119, 120
source route IP option, deny.....	133
strict source route IP option, detect.....	133
SYN and FIN flags set.....	126
SYN floods.....	12, 38
SYN fragments, detect.....	220
SYN-ACK-ACK proxy floods.....	10, 31
TCP packet without flags, detect.....	127
Teardrop.....	24, 57
UDP floods.....	20, 52

- unknown protocols, drop.....223
 - WinNuke attacks.....25, 58
 - screen statement
 - (Zones).....79, 178, 253
 - security IP option.....122, 124
 - session limits.....8
 - source-based.....8, 27, 29
 - session table floods.....7, 129
 - show security screen ids-option
 - command.....101, 201, 275
 - show security screen statistics
 - command.....106, 206, 280
 - source IP route attack protection
 - overview.....133
 - source-ip-based statement.....79, 178, 253
 - source-threshold statement.....80, 179, 254
 - stateful.....3, 117, 217
 - stateful inspection.....3, 117, 217
 - stream ID IP option.....122, 124
 - strict source route IP option.....122
 - strict-syn-check statement.....179
 - support, technical See technical support
 - SYN and FIN flags protection
 - overview.....126
 - syn check statement.....81, 180, 255
 - SYN checking.....129
 - asymmetric routing.....129
 - reconnaissance hole.....129
 - session table floods.....129
 - SYN cookies.....17
 - SYN floods.....12, 38
 - about whitelists.....17
 - alarm threshold.....15
 - attack threshold.....15
 - configuring whitelists.....46
 - destination threshold.....15
 - source threshold.....15
 - SYN cookies.....17
 - threshold.....13
 - timeout.....15
 - SYN fragment protection
 - overview.....220
 - SYN-ACK-ACK proxy floods.....10
 - SYN-ACK-ACK-proxy flood protection
 - configuration.....31
 - syn-ack-ack-proxy statement.....81, 180, 255
 - syn-fin statement.....82, 181, 256
 - syn-flood statement.....83, 182, 257
 - syn-flood-protection-mode
 - statement.....84, 183, 258
 - syn-frag statement.....84, 183, 258
 - syntax conventions.....xv
- ## T
- TCP header flag attack protection
 - overview.....127
 - tcp statement
 - (Security Screen).....85, 184, 259
 - tcp-no-flag statement.....86, 185, 260
 - tcp-sweep statement.....87, 186, 261
 - teardrop attack protection
 - configuration.....57
 - overview.....24
 - technical support
 - contacting JTAC.....xvii
 - three-way handshakes.....12
 - timeout statement
 - (Security Screen).....88, 187, 262
 - timestamp IP option.....122, 124
 - traceoptions statement
 - (Screen).....89, 188, 263
- ## U
- udp statement
 - (Security Screen).....91, 190, 265
 - udp-sweep statement.....92, 191, 266
 - unknown protocol attack protection
 - overview.....223
- ## W
- white-list statement.....93, 192, 267
 - whitelists
 - SYN flood screens, about.....17
 - SYN flood screens, configuring.....46
 - WinNuke attack protection
 - configuration.....58
 - overview.....25
 - winnuke statement.....94, 193, 268
- ## Z
- zombie agents.....4

