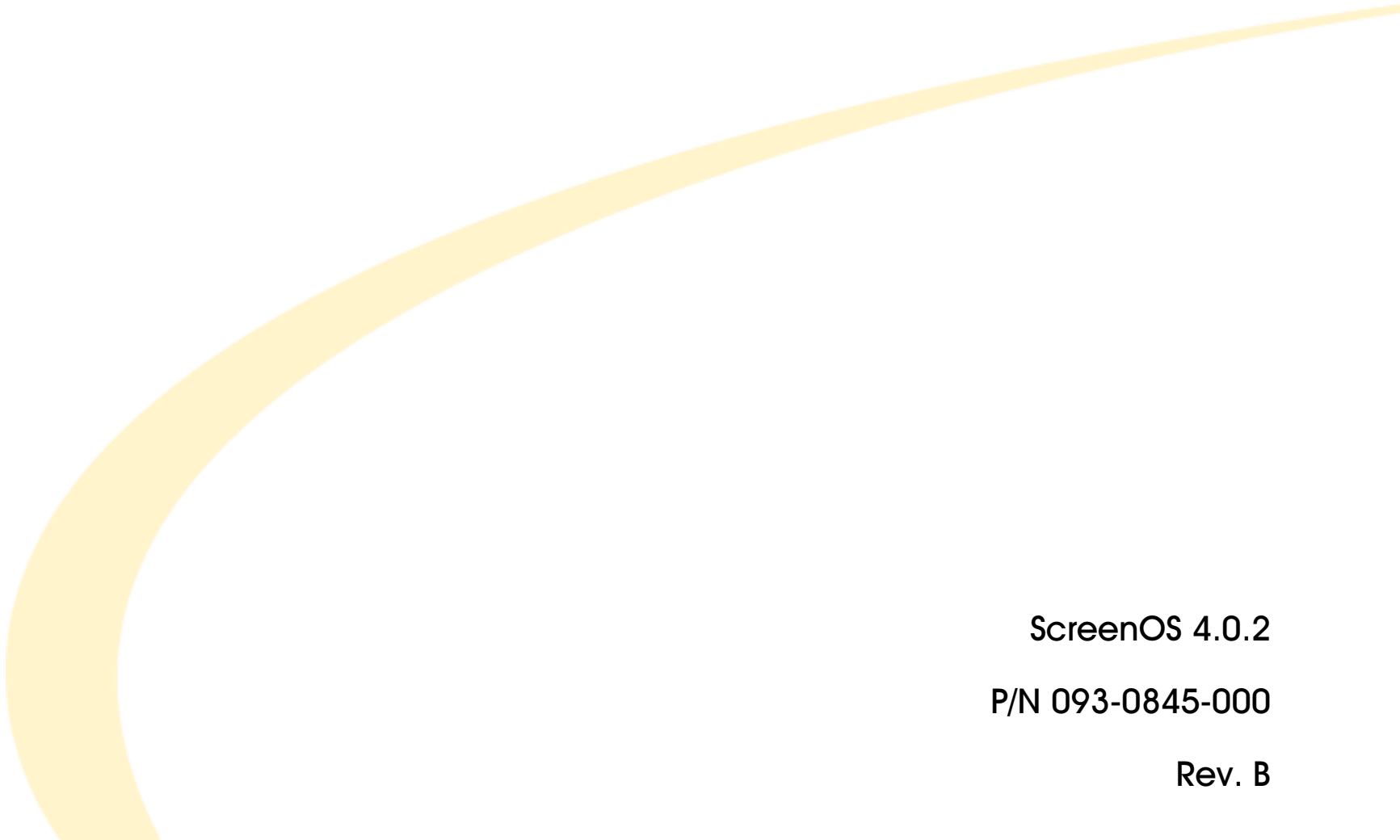


# *NetScreen New Features Guide*



ScreenOS 4.0.2

P/N 093-0845-000

Rev. B

---

---

## Copyright Notice

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-1000, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies. Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from

NetScreen Technologies, Inc.  
350 Oakmead Parkway  
Sunnyvale, CA 94085 U.S.A.  
[www.netscreen.com](http://www.netscreen.com)

## FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

**Caution:** Changes or modifications to this product could void the user's warranty and authority to operate this device.

## Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

---

# Contents

Preface .....	V		
Conventions .....	vi		
WebUI Navigation Conventions .....	vi		
Example: Objects > Addresses > List > New .....	vi		
CLI Conventions .....	vii		
Dependency Delimiters .....	vii		
Nested Dependencies .....	vii		
Availability of CLI Commands and Features .....	viii		
NetScreen Documentation .....	ix		
Chapter 1 ScreenOS 4.0.1 New Features and Enhancements .....	1		
Granular Blocking of HTTP Components .....	3		
ActiveX Controls .....	3		
Java Applets .....	4		
EXE Files .....	4		
ZIP Files .....	4		
Example: Blocking Java Applets and .exe Files .....	5		
Fragment Reassembly .....	6		
Malicious URL Protection .....	6		
Application Layer Gateway .....	7		
Example: Blocking Malicious URLs in Packet Fragments .....	8		
Session Table Flooding .....	10		
Source- and Destination-Based Session Limits .....	10		
Example: Source-Based Session Limiting .....	12		
Example: Destination-Based Session Limiting .....	13		
Aggressive Aging .....	13		
		Example: Aggressively Aging Out Sessions .....	15
		Layer 2 IP Spoof Checking .....	16
		Example: IP Spoof Protection in Transparent Mode .....	18
		Attack Monitoring .....	20
		Example: Monitoring Attacks from the Untrust Zone .....	20
		FQDN for Dynamic IKE Gateways .....	21
		Aliases .....	22
		Example: IKE Peer with FQDN .....	23
		Bidirectional Policies for Dialup VPN Users .....	37
		Example: Bidirectional Dialup-to-LAN VPN Policies .....	37
		VPN Monitoring .....	44
		Example: Specifying Source and Destination Addresses for VPN Monitoring .....	46
		SNMP .....	57
		Example: Defining an SNMP Community .....	58
		Virtual System Zones .....	60
		IP Classification for Virtual System Traffic .....	61
		Example: Configuring IP-Based Traffic Classification .....	62
		TCP/IP Settings Propagation .....	67
		Example: Forwarding TCP/IP Settings .....	68
		DNS Refresh .....	71
		Example: Setting a DNS Refresh Interval .....	71
		RADIUS Access-Challenge .....	72

**Chapter 2 ScreenOS 4.0.2 New Features and Enhancements** ..... 75

- Administration ..... 76
  - Root Admin ..... 76
    - Password Minimum Length ..... 76
    - Example: Setting the Minimum Length of the Root Admin Password ..... 77
    - Console Access ..... 77
      - Example: Restricting the Root Admin to Console Access ..... 78
      - Common Criteria ..... 78
      - Example: Disabling Internal Commands ..... 79
  - Admin Users ..... 79
    - Limiting Telnet Login Attempts ..... 79
      - Example: Limiting the Number of Login Attempts ..... 80
      - Telnet Through VPN ..... 80
        - Example: Securing Telnet Connections through VPNs ..... 81
- Counting Statistics in the WebUI ..... 82
  - Example: Viewing Traffic Log Details ..... 82
- SCREENS for MGT Zone ..... 83
  - Example: Enabling SCREEN Options for the MGT Zone ..... 83

**Chapter 3 ScreenOS 4.0.1 Modified CLI Commands** ..... 85

- dns ..... 86
  - Syntax ..... 86
  - Keywords and Variables ..... 86
- flow ..... 87
  - Syntax ..... 87

- Keywords and Variables ..... 88
- ike ..... 89
  - Syntax ..... 89
  - Keywords and Variables ..... 89
- log ..... 90
  - Syntax ..... 90
  - Keywords and Variables ..... 90
- snmp ..... 91
  - Syntax ..... 91
  - Keywords and Variables ..... 91
- vpn ..... 92
  - Syntax ..... 92
  - Keywords and Variables ..... 92
- zone ..... 94
  - Syntax ..... 94
  - Keywords and Variables ..... 94

**Chapter 4 ScreenOS 4.0.2 Modified CLI Commands** ..... 97

- admin ..... 98
  - Syntax ..... 98
  - Keywords and Variables ..... 101
  - Defaults ..... 102
- common-criteria ..... 103
  - Syntax ..... 103

**Chapter 5 ScreenOS 4.0.1 New and Modified Messages** ..... 105

- Authentication ..... 106
  - Information (00544) ..... 106
- DNS ..... 107

Notification (00004) ..... 107

Firewall ..... 108

    Critical (00033) ..... 108

    Critical (00400) ..... 109

    Notification (00005) ..... 109

IKE ..... 111

    Information (00536) ..... 111

Sessions ..... 113

    Notification (00040) ..... 113

VPN ..... 114

    Notification (00017) ..... 114

    Information (00536) ..... 114

Zones ..... 115

    Notification (00037) ..... 115

**Chapter 6 ScreenOS 4.0.2 New and Modified**

**Messages ..... 117**

    Admin ..... 118

    Notification (00002) ..... 118



# Preface

This document presents the new features in release 4.0.1 and 4.0.2 of NetScreen ScreenOS software. It is organized into the following chapters:

- [Chapter 1, “ScreenOS 4.0.1 New Features and Enhancements” on page 1](#)
- [Chapter 2, “ScreenOS 4.0.2 New Features and Enhancements” on page 75](#)
- [Chapter 3, “ScreenOS 4.0.1 Modified CLI Commands” on page 85](#)
- [Chapter 4, “ScreenOS 4.0.2 Modified CLI Commands” on page 97](#)
- [Chapter 5, “ScreenOS 4.0.1 New and Modified Messages” on page 105](#)
- [Chapter 6, “ScreenOS 4.0.2 New and Modified Messages” on page 117](#)

For more information about ScreenOS features, CLI commands, and messages refer to the following documents:

- *NetScreen Concepts & Examples ScreenOS Reference Guide*
- *NetScreen CLI Reference Guide*
- *NetScreen Messages Reference Guide*

## CONVENTIONS

This book presents two management methods for configuring a NetScreen device: the Web user interface (WebUI) and the command line interface (CLI). The conventions used for both are introduced below.

### WebUI Navigation Conventions

Throughout this book, a single chevron ( > ) is used to indicate navigation through the WebUI by clicking menu options and links.

#### Example: **Objects > Addresses > List > New**

To access the new address configuration dialog box, do the following:

1. Click **Objects** in the menu column.  
The Objects menu option expands to reveal a subset of options for Objects.
2. (Applet menu) Hover the mouse over **Addresses**.  
(DHTML menu) Click **Addresses**.  
The Addresses option expands to reveal a subset of options for Addresses.
3. Click **List**.  
The address book table appears.
4. Click the **New** link in the upper right corner.  
The new address configuration dialog box appears.

## CLI Conventions

Each CLI command description in this manual reveals some aspect of command syntax. This syntax may include options, switches, parameters, and other features. To illustrate syntax rules, some command descriptions use *dependency delimiters*. Such delimiters indicate which command features are mandatory, and in which contexts.

### Dependency Delimiters

Each syntax description shows the dependencies between command features by using special characters.

- The { and } symbols denote a mandatory feature. Features enclosed by these symbols are essential for execution of the command.
- The [ and ] symbols denote an optional feature. Features enclosed by these symbols are not essential for execution of the command, although omitting such features might adversely affect the outcome.
- The | symbol denotes an “or” relationship between two features. When this symbol appears between two features on the same line, you can use either feature (but not both). When this symbol appears at the end of a line, you can use the feature on that line, or the one below it.

### Nested Dependencies

Many CLI commands have *nested* dependencies, which make features optional in some contexts, and mandatory in others. The three hypothetical features shown below demonstrate this principle.

```
[ feature_1 { feature_2 | feature_3 } ]
```

The delimiters [ and ] surround the entire clause. Consequently, you can omit **feature\_1**, **feature\_2**, and **feature\_3**, and still execute the command successfully. However, because the { and } delimiters surround **feature\_2** and **feature\_3**, you must include either **feature\_2** or **feature\_3** if you include **feature\_1**. Otherwise, you cannot successfully execute the command.

The following example shows some of the feature dependencies of the **set interface** command.

```
set interface vlan1 broadcast { flood | arp [ trace-route ] }
```

The { and } brackets indicate that specifying either **flood** or **arp** is mandatory. By contrast, the [ and ] brackets indicate that the **trace-route** option for **arp** is not mandatory. Thus, the command might take any of the following forms:

```
ns-> set interface vlan1 broadcast flood
ns-> set interface vlan1 broadcast arp
ns-> set interface vlan1 broadcast arp trace-route
```

## Availability of CLI Commands and Features

As you execute CLI commands using the syntax descriptions in this manual, you may find that certain commands and command features are unavailable for your NetScreen device model.

Because NetScreen devices treat unavailable command features as improper syntax, attempting to use such a feature usually generates the **unknown keyword** error message. When this message appears, confirm the feature's availability using the ? switch. For example, the following commands list available options for the **set vpn** command:

```
ns-> set vpn ?
ns-> set vpn vpn_name ?
ns-> set vpn gateway gate_name ?
```

## NETSCREEN DOCUMENTATION

To obtain technical documentation for any NetScreen product, visit [www.netscreen.com/support/manuals.html](http://www.netscreen.com/support/manuals.html). To access the latest NetScreen documentation, see the **Current Manuals** section. To access archived documentation from previous releases, see the **Archived Manuals** section.

To obtain the latest technical information on a NetScreen product release, see the release notes document for that release. To obtain release notes, visit [www.netscreen.com/support](http://www.netscreen.com/support) and select **Software Download**. Select the product and version, then click **Go**. (To perform this download, you must be a registered user.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

[techpubs@netscreen.com](mailto:techpubs@netscreen.com)



# ScreenOS 4.0.1 New Features and Enhancements

---

This chapter presents the new features and feature enhancements introduced in ScreenOS4.0.1. The concepts behind each of the following features is explained and are accompanied by example configurations:

## Firewall

- “Granular Blocking of HTTP Components” on page 3
  - “ActiveX Controls” on page 3
  - “Java Applets” on page 4
  - “ZIP Files” on page 4
  - “EXE Files” on page 4
- “Fragment Reassembly” on page 6
  - “Malicious URL Protection” on page 6
  - “Application Layer Gateway” on page 7
- “Session Table Flooding” on page 10
  - “Source- and Destination-Based Session Limits” on page 10
  - “Aggressive Aging” on page 13
- “Layer 2 IP Spoof Checking” on page 16
- “Attack Monitoring” on page 20

## VPNs

- “FQDN for Dynamic IKE Gateways” on page 21
  - “Aliases” on page 22
- “Bidirectional Policies for Dialup VPN Users” on page 37
- “VPN Monitoring” on page 44

### Administration

- [“SNMP” on page 57](#)

### Virtual Systems

- [“Virtual System Zones” on page 60](#)
- [“IP Classification for Virtual System Traffic” on page 61](#)

### DHCP and DNS

- [“TCP/IP Settings Propagation” on page 67](#)
- [“DNS Refresh” on page 71](#)

### User Authentication

- [“RADIUS Access-Challenge” on page 72](#)

The contents of this chapter focus exclusively on new features added in this release and enhancements made to existing features. For more complete information about ScreenOS features, refer to the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

## GRANULAR BLOCKING OF HTTP COMPONENTS

With ScreenOS 4.0.1, a NetScreen device can selectively block ActiveX controls, Java applets, .zip files, and .exe files sent via HTTP. The danger that these components pose to the security of a network is that they provide a means for an untrusted party to load and then control an application on hosts in a protected network.

When you enable the blocking of one or more of these components in a security zone, the NetScreen device examines every HTTP header that arrives at an interface bound to that zone. It checks if the content type listed in the header indicates that any of the targeted components are in the packet payload. If the content type is Java, .exe, or .zip and you have configured the NetScreen device to block those HTTP component types, the NetScreen device blocks the packet. If the content type lists only “octet stream” instead of a specific component type, then the NetScreen device examines the file type in the payload. If the file type is Java, .exe, or .zip and you have configured the NetScreen device to block those component types, the NetScreen device blocks the packet.

When you enable the blocking of ActiveX controls, the NetScreen device blocks all HTTP packets containing any type of HTTP component in its payload—ActiveX controls, Java applets, .exe files, or .zip files.

**Note:** When ActiveX-blocking is enabled, the NetScreen device blocks Java applets, .exe files, and .zip files whether they are contained within an ActiveX control or not.

### ActiveX Controls

Microsoft ActiveX technology provides a tool for Web designers to create dynamic and interactive Web pages. ActiveX controls are components that allow different programs to interact with each other. For example, ActiveX allows your Web browser to open a spreadsheet or display your personal account from a backend database. ActiveX components might also contain other components such as Java applets, or files such as .exe and .zip files.

When you visit an ActiveX-enabled Web site, the site prompts you to download ActiveX controls to your computer. Microsoft provides a pop-up message displaying the name of the company or programmer who authenticated the ActiveX code that is offered for download. If you trust the source of the code, you can proceed to download the controls. If you distrust the source, you can refuse them.

If you download an ActiveX control to your computer, it can then do whatever its creator designed it to do. If it is malicious code, it can now reformat your hard drive, delete all your files, send all your personal e-mail to your boss, and so on.

## Java Applets

Serving a similar purpose as ActiveX, Java applets also increase the functionality of Web pages by allowing them to interact with other programs. You download Java applets to a Java Virtual Machine (VM) on your computer. In the initial version of Java, the VM did not allow the applets to interact with other resources on your computer. Starting with Java 1.1, some of these restrictions were relaxed to provide greater functionality. As a result, Java applets can now access local resources outside the VM. Because an attacker can program Java applets to operate outside the VM, they pose the same security threat as ActiveX controls do.

## EXE Files

If you download and run an executable file (that is, a file with a .exe extension) obtained off the Web, you cannot guarantee that the file is uncontaminated. Even if you trust the site from which you downloaded it, it is possible that somebody sniffing download requests from that site has intercepted your request and responded with a doctored .exe file that contains malicious code.

## ZIP Files

A zip file (that is, a file with a .zip extension) is a type of file containing one or more compressed files. The danger of downloading a .exe file presented in the previous section about .exe files applies to .zip files, because a .zip file can contain one or more .exe files.

## Example: Blocking Java Applets and .exe Files

In this example, you block any HTTP traffic containing Java applets and .exe files in packets arriving at an Untrust zone interface.

### *WebUI*

Network > Zones > Edit (for Untrust) > SCREEN: Select the **Block Java Component** and **Block EXE Component** check boxes, and then click **OK**.

### *CLI*

1. set zone untrust screen java
2. set zone untrust screen exe
3. save

## FRAGMENT REASSEMBLY

Typically, a network forwarding device such as a router or switch does not reassemble fragmented packets that it receives. It is the responsibility of the destination host to reconstruct the fragmented packets when they all arrive. Because the purpose of forwarding devices is the efficient delivery of traffic, queuing fragmented packets, reassembling them, then refragmenting them, and forwarding them is unnecessary and inefficient. However, passing fragmented packets through a firewall is insecure. An attacker can intentionally break up packets to conceal traffic strings that the firewall otherwise would detect and block.

ScreenOS 4.0.1 allows you to enable fragment reassembly on a per zone basis. Doing so allows the NetScreen device to expand its ability to detect and block malicious URL strings, and to improve its ability to provide an application layer gateway (ALG) to check the data portions of packets.

### Malicious URL Protection

You can define up to 16 malicious URL string patterns, each of which can be up to 24 characters long. With the Malicious URL blocking feature enabled, the NetScreen device examines the data payload of all HTTP and FTP packets. If it locates a URL and detects that the beginning of its string matches the pattern you defined, the NetScreen device blocks that packet from passing the firewall.

A resourceful attacker, realizing that the string is known and might be guarded against, can deliberately fragment the IP packets or TCP segments and thereby make the pattern unrecognizable during a packet-by-packet inspection. For example, if the malicious URL string is **120.3.4.5/level/50/exec**, IP fragmentation might break up the string into the following sections:

- First packet: **120.**
- Second packet: **3.4.5/level/50**
- Third packet: **exec**

Individually, the fragmented strings can pass undetected through the NetScreen device, even if you have the string defined as **120.3.4.5/level/50/exec** with a length of 23 characters. The string in the first packet—"120."— matches the first part of the defined pattern, but it is shorter than the required 23-character URL length. The strings in the second and third packets do not match the beginning of the defined pattern, and so too pass without impedance.

However, if the packets are reassembled, the fragments combine to form a recognizable string that the NetScreen device can block. Using the Fragment Reassembly feature, the NetScreen device can buffer fragments in a queue, reassemble them into a complete packet, and then inspect that packet for a malicious URL. Depending on the results of this reassembly process and subsequent inspection, the NetScreen device performs one of the following steps:

- If the NetScreen device discovers a malicious URL, it drops the packet and enters the event in the log.
- If the NetScreen device cannot complete the reassembly process, a time limit is imposed to age out and discard fragments.
- If the NetScreen device determines that the URL is not malicious but the reassembled packet is too big to forward, the NetScreen device fragments that packet into multiple packets and forwards them.
- If the NetScreen device determines that the URL is not malicious and does not need to fragment it, it then forwards the packet.

## Application Layer Gateway

NetScreen provides an application layer gateway (ALG) for a number of protocols, such as DNS, FTP, H.323, and HTTP. Of these, fragment reassembly can be an important component in the enforcement of policies involving FTP and HTTP services. The ability of the NetScreen firewall to screen packets for protocols such as FTP-Get and FTP-Put requires it to examine not only the packet header but also the data in the payload. For example, there might be two policies, one denying FTP-put from the Untrust to DMZ zones, and another permitting FTP-get from the Untrust to the DMZ zones:

```
set policy from untrust to dmz any any ftp-put deny
```

```
set policy from untrust to dmz any any ftp-get permit
```

To distinguish the two types of traffic, the NetScreen firewall examines the payload. If it reads **RETR filename**, the FTP client has sent a request to get (or “retrieve”) the specified file from the FTP server, and the NetScreen device allows the packet to pass. If the NetScreen device finds **STOR filename**, the client has sent a request to put (or “store”) the specified file on the server, and the NetScreen device blocks the packet.

To get around this defense, an attacker can deliberately fragment a single FTP-put packet into two packets that contain the following text in their respective payloads: packet 1: **ST**; packet 2: **OR filename**. When the NetScreen device inspects each packet individually, it does not find the string **STOR filename**, and consequently allows them both to pass.

However, if the packets are reassembled, the fragments combine to form a recognizable string upon which the NetScreen device can act. Using the Fragment Reassembly feature, the NetScreen device buffers the FTP fragments in a queue, reassembles them into a complete packet, and then inspects that packet for the complete FTP request. Depending on the results of this reassembly process and subsequent inspection, the NetScreen device performs one of the following steps:

- If the NetScreen device discovers an FTP-put request, it drops the packet and enters the event in the log.
- If the NetScreen device cannot complete the reassembly process, a time limit is imposed to age out and discard fragments.
- If the NetScreen device discovers an FTP-get request but the reassembled packet is too big to forward, the NetScreen device fragments that packet into multiple packets and forwards them.
- If the NetScreen device discovers an FTP-get request and does not need to fragment it, it then forwards the packet.

### Example: Blocking Malicious URLs in Packet Fragments

In this example, you define the following three malicious URL strings and enable the malicious URL blocking option:

- Malicious URL #1
  - ID: Perl
  - Pattern: scripts/perl.exe
  - Length: 30
- Malicious URL #2
  - ID: CMF
  - Pattern: cgi-bin/phf
  - Length: 23
- Malicious URL #3
  - ID: DLL
  - Pattern: 210.0.0.1/msad/msads.dll
  - Length: 24

You then enable fragment reassembly for the detection of the URLs in fragmented HTTP and FTP traffic arriving at an Untrust zone interface.

### WebUI

1. Network > Zones > Edit (for Untrust) > Mal-URL: Enter the following, and then click **OK**:  
ID: perl  
Pattern: /scripts/perl.exe  
Length: 30
2. Network > Zones > Edit (for Untrust) > Mal-URL: Enter the following, and then click **OK**:  
ID: cmf  
Pattern: cgi-bin/phf  
Length: 23
3. Network > Zones > Edit (for Untrust) > Mal-URL: Enter the following, and then click **OK**:  
ID: dll  
Pattern: 210.1.1.5/msadcs.dll  
Length: 25
4. Network > Zones > Edit (for Untrust): Select the **IP/TCP Reassembly for ALG** check box, and then click **OK**.

### CLI

1. set zone untrust screen mal-url perl "scripts/perl.exe" 30
2. set zone untrust screen mal-url cmf "cgi-bin/phf" 23
3. set zone untrust screen mal-url dll "210.1.1.5/msadcs.dll" 15
4. set zone untrust screen reassembly-for-alg
5. save

## SESSION TABLE FLOODING

A successful denial-of-service (DoS) attack overwhelms its victim with such a massive barrage of ersatz 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: 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 following SCREEN options help mitigate such attacks:

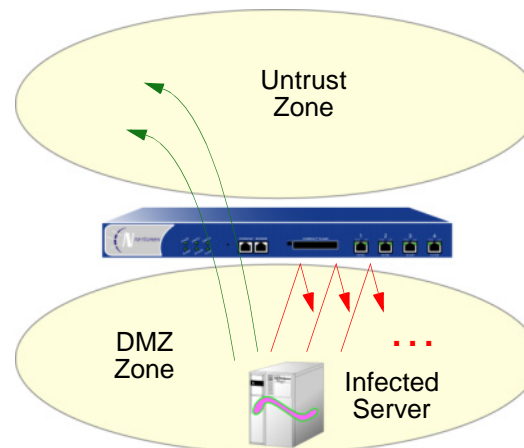
- “Source- and Destination-Based Session Limits”
- “Aggressive Aging” on page 13

### Source- and Destination-Based Session Limits

In addition to limiting the number of sessions from the same source IP address, ScreenOS 4.0.1 permits you to limit the number of 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 NetScreen firewall can curb such excessive amounts of traffic.

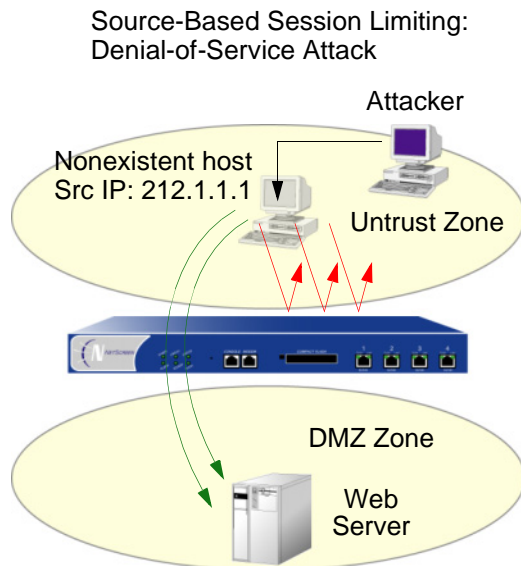
Source-Based Session Limiting:  
Nimda Virus/Worm Traffic  
Containment

A Web server is infected with the Nimda virus/worm hybrid, which causes the server to generate excessive amounts of traffic.

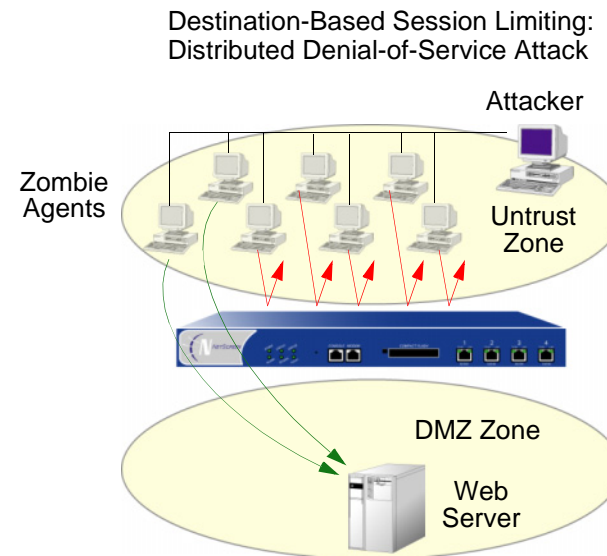


After the number of sessions from the infected server reaches the maximum limit, the NetScreen device begins blocking all further connection attempts from that server.

Another benefit of source-based session limiting is that it can mitigate attempts to fill up the NetScreen session table—if all the connection attempts originate from the same source IP address. However, 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 the attacker. In addition to the SYN, UDP, and ICMP flood detection and prevention SCREEN options, setting a destination-based session limit can ensure that the NetScreen device allows only an acceptable number of connection requests—no matter what the source—to reach any one host.



When the amount of sessions from 212.1.1.1 surpasses the maximum limit, the NetScreen device begins blocking further connection attempts from that IP address.



When the amount of sessions to the Web server surpasses the maximum limit, the NetScreen device begins blocking further connection attempts to that 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 NetScreen platform you are using. To see

the maximum number of sessions that your session table supports, use the CLI command **get session**, and then look at the first line in the output, which lists the number of current (allocated) sessions, the maximum number of sessions, and the number of failed session allocations:

```
alloc 420/max 128000, alloc failed 0
```

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

## Example: Source-Based Session Limiting

In this example, you want to limit the amount of sessions that any one server in the DMZ and Trust zones can initiate. Because the DMZ zone only contains Web servers, none of which should initiate traffic, you set the source-session limit at the lowest possible value: 1 session per second. On the other hand, the Trust zone contains personal computers, servers, printers, and so on, many of which do initiate traffic. The Trust zone contains the corporate network of a company with about 100 employees. For the Trust zone, you set the source-session limit maximum to 50 sessions per second.

### WebUI

1. Network > Zone > Edit (for DMZ) > SCREEN: Enter the following, and then click **OK**:  
    SYN Flood Protection: (select)  
    Source Threshold: 1 pps
2. Network > Zone > Edit (for Trust) > SCREEN: Enter the following, and then click **OK**:  
    SYN Flood Protection: (select)  
    Source Threshold: 50 pps

### CLI

1. set zone dmz screen limit-session source-ip-based 1
2. set zone dmz screen limit-session source-ip-based
3. set zone trust screen limit-session source-ip-based 50
4. set zone trust screen limit-session source-ip-based
5. save

## Example: Destination-Based Session Limiting

In this example, you want to limit the amount of traffic to a Web server at 211.1.1.5. The server is in the DMZ zone. After observing the traffic flow from the Untrust zone to this server for a month, you have determined that the average number of new sessions it receives is 2000 sessions per second. Based on this information, you decide to set the new session limit at 4000 sessions per second. Although your observations show that traffic spikes sometimes exceed that limit, you opt for firewall security over occasional server inaccessibility.

### WebUI

Network > Zone > Edit (for Untrust) > SCREEN: Enter the following, and then click **OK**:

SYN Flood Protection: (select)

Destination Threshold: 4000 pps

### CLI

1. set zone untrust screen limit-session destination-ip-based 4000
2. set zone untrust screen limit-session destination-ip-based
3. save

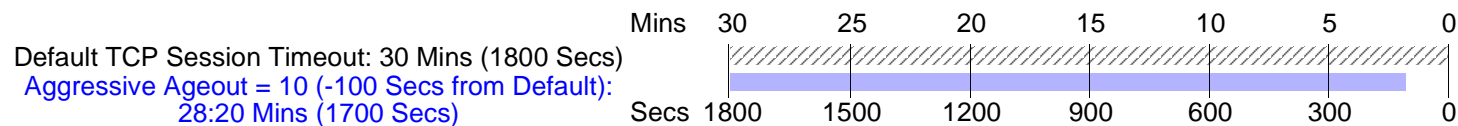
## Aggressive Aging

By default, an initial TCP session 3-way handshake takes 20 seconds to time out (that is, to expire because of inactivity). After a TCP session has been established, the timeout value changes to 30 minutes. For HTTP and UDP sessions, the session timeouts are 5 minutes and 1 minute respectively. The session timeout counter begins when a session starts and is refreshed every 10 seconds if the session is active. If a session becomes idle for more than 10 seconds, the timeout counter begins to decrement.

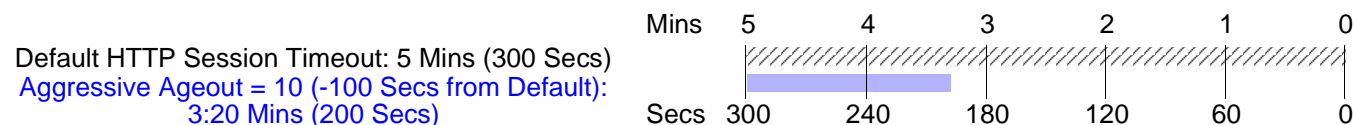
In ScreenOS 4.0.1, NetScreen has implemented a mechanism to accelerate the timeout process when the number of sessions in the session table surpasses a specified high-watermark threshold. When the number of sessions dips below a specified low-watermark threshold, the timeout process returns to normal. During the period when the aggressive aging out process is in effect, a NetScreen device ages out the oldest sessions first, using the aging out rate that you specify. These aged-out sessions are tagged as invalid and are removed in the next garbage sweep, which occurs every 2 seconds.

The aggressive ageout option shortens default session timeouts by the amount you enter. The aggressive ageout value can be between 2 and 10 units, where each unit represents a 10-second interval (that is, the aggressive ageout setting can be between 20 and 100 seconds). The default setting is 2 units, or 20 seconds. If you define the aggressive ageout setting at 100 seconds, for example, you shorten the TCP and HTTP session timeouts as follows:

- **TCP:** The session timeout value shortens from 1800 seconds (30 minutes) to 1700 seconds (28:20 minutes) during the time when the aggressive aging process is in effect. During that period, the NetScreen device automatically deletes all TCP sessions whose timeout value has passed 1700 seconds, beginning with the oldest sessions first.



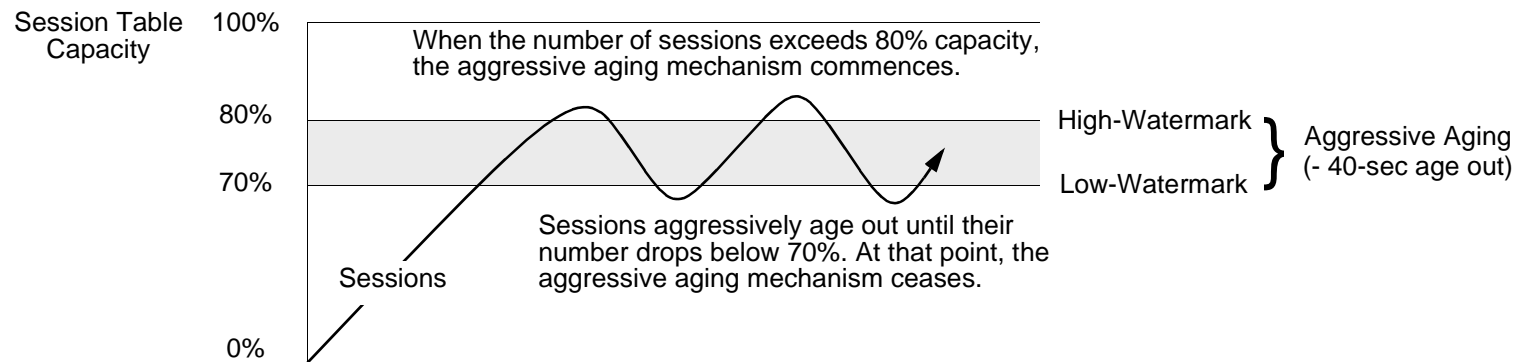
- **HTTP:** The session timeout value shortens from 300 seconds (5 minutes) to 200 seconds (3:20 minutes) during the time when the aggressive aging process is in effect. During that period, the NetScreen device automatically deletes all HTTP sessions whose timeout value has passed 200 seconds, beginning with the oldest sessions first.



- **UDP:** Because the default UDP session timeout is 60 seconds, defining an early ageout setting at 100 seconds causes all UDP sessions to ageout and be marked for deletion in the next garbage sweep.

## Example: Aggressively Aging Out Sessions

In this example, you set the aggressive aging out process to commence when traffic exceeds a high-watermark of 80% and cease when it retreats below a low-watermark of 70%. You specify 40 seconds for the aggressive age-out interval. When the session table is more than 80% full (the high-mark threshold), the NetScreen device decreases the timeout for all sessions by 40 seconds and begins aggressively aging out the oldest sessions until the number of sessions in the table is under 70% (the low-mark threshold).



### WebUI

**Note:** You must use the CLI to configure the aggressive age -out settings.

### CLI

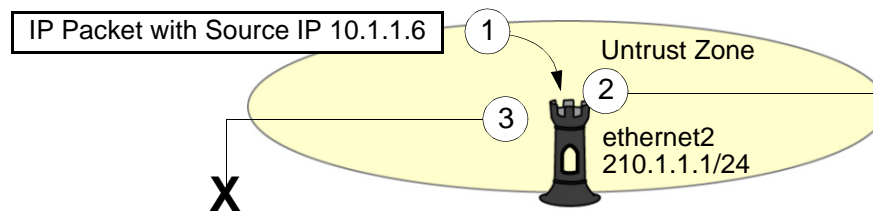
1. set flow aging low-watermark 70
2. set flow aging high-watermark 80
3. set flow aging early-ageout 4
4. save

## LAYER 2 IP SPOOF CHECKING

One method of attempting to gain access to a restricted area of the 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. NetScreen has two IP spoofing detection methods, both of which accomplish the same task: determining that the packet came from a location other than that indicated in its header. The method that a NetScreen device uses depends if it is operating at Layer 3 or Layer 2 in the OSI model.

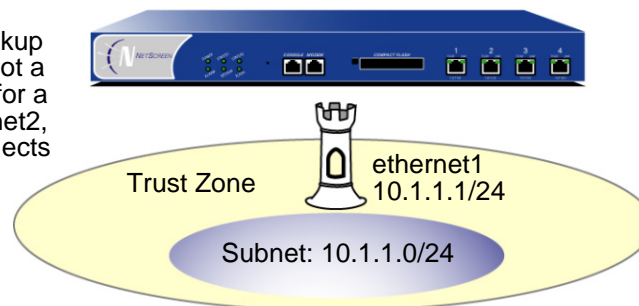
- Layer 3** – When interfaces on the NetScreen device are operating in Route or NAT mode, the mechanism to detect IP spoofing relies on route table entries. If, for example, a packet with source IP address 10.1.1.6 arrives at ethernet2, but the NetScreen device has a route to 10.1.1.0/24 through ethernet1, IP spoof checking notes 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 ethernet1, not ethernet2. Therefore, the device concludes that the packet has a spoofed source IP address and discards it.

- An IP packet arrives at ethernet2. Its source IP address is 10.1.1.6.



- Because IP spoof protection is enabled in the Untrust zone, the NetScreen device checks if 10.1.1.6 is a valid source IP address for a packet arriving on ethernet2.

- When the route table lookup reveals that 10.1.1.6 is not a valid source IP address for a packet arriving on ethernet2, the NetScreen device rejects the packet.



Route Table

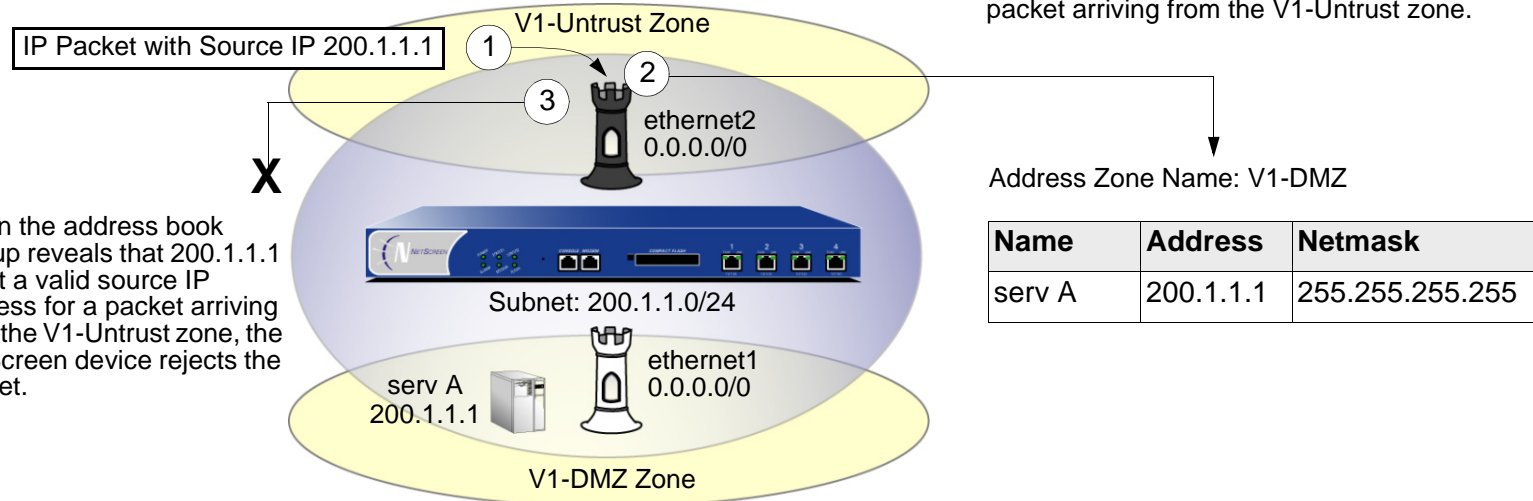
ID	IP-Prefix	Interface	Gateway	P
1	10.1.10/24	eth1	0.0.0.0	C

- Layer 2** – When interfaces on the NetScreen device are operating in Transparent mode, the IP spoof checking mechanism makes use of the address book entries. For example, you have defined an address for “serv A” as 200.1.1.1/32 in the V1-DMZ zone. If a packet with source IP address 200.1.1.1 arrives at a V1-Untrust zone interface, IP spoof checking notes that this address arrived at an invalid interface (the address belongs to the V1-DMZ zone, not to the V1-Untrust zone). Therefore, the device concludes that packet has a spoofed source IP address and discards it.

1. An IP packet arrives from the V1-Untrust zone. Its source IP address is 200.1.1.1.

2. Because IP spoof protection is enabled in the V1-Untrust zone, the NetScreen device checks if 200.1.1.1 is a valid source IP address for a packet arriving from the V1-Untrust zone.

3. When the address book lookup reveals that 200.1.1.1 is not a valid source IP address for a packet arriving from the V1-Untrust zone, the NetScreen device rejects the packet.



## Example: IP Spoof Protection in Transparent Mode

In this example, you protect the V1-DMZ zone from IP spoofing on traffic originating in the V1-Untrust zone. First, you define the following addresses for three Web servers in the V1-DMZ zone:

- servA: 200.1.1.10
- servB: 200.1.1.20
- servC: 200.1.1.30

You then enable IP spoofing in the V1-Untrust zone.

If an attacker in the V1-Untrust zone attempts to spoof the source IP address using any of the three addresses in the V1-DMZ zone, the NetScreen device checks the address against those in the address books. When it finds that the source IP address on a packet coming from the V1-Untrust zone belongs to a defined address in the V1-DMZ zone, the NetScreen device rejects the packet.

### WebUI

1. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: servA

IP Address/Domain Name:

IP/Netmask: (select), 200.1.1.10

Zone: V1-DMZ

2. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: servB

IP Address/Domain Name:

IP/Netmask: (select), 200.1.1.20

Zone: V1-DMZ

3. Objects > Addresses > List > New: Enter the following, and then click **OK**:
  - Address Name: servC
  - IP Address/Domain Name:
    - IP/Netmask: (select), 200.1.1.30
  - Zone: V1-DMZ
4. Network > Zones > Edit (for V1-DMZ) > SCREEN: Select the **IP Address Spoof Protection** check box, and then click **Apply**.

### *CLI*

1. set address v1-dmz servA 200.1.1.10/32
2. set address v1-dmz servB 200.1.1.20/32
3. set address v1-dmz servC 200.1.1.30/32
4. set zone v1-untrust screen ip-spoofing
5. save

## ATTACK MONITORING

If you want to gather information about an attack (and possibly the party responsible for it), you can let the attack occur, monitor it, analyze it, perform forensics, and then respond as delineated in a previously prepared incident response plan. You can instruct the NetScreen device to notify you of an attack, but instead of taking action, it allows the packets to pass. You can then study what occurred, and try to understand the attacker's method, strategy, and objectives. Increased understanding of the threat to the network can then allow you to better fortify your defenses. Although a smart attacker can conceal his or her location and identity, you might be able to gather enough information to discern where the attack originated. You also might be able to estimate the attacker's capabilities. This kind of information allows you to gauge your response: A bored computer science college student warrants a different response than an international cyber terrorist organization.

### Example: Monitoring Attacks from the Untrust Zone

In this example, IP spoofing attacks from the Untrust zone have occurred on a daily basis, usually between 9:00 PM and 12:00 AM. Instead of dropping the packets with the spoofed source IP addresses, you want the NetScreen device to notify you of their arrival but allow them to pass, directing them to a honeypot<sup>1</sup> that you have connected on the DMZ interface connection. At 8:55 PM, you change the firewall behavior from notification and rejection of packets belonging to a detected attack to notification and acceptance. When the attack occurs, you can then use the honeypot to monitor the attacker's activity after crossing the firewall. You might also work in cooperation with the upstream ISP to begin tracking the source of the packets back to their source.

#### WebUI

Network > Zones > Edit (for Untrust): Select the **Generate Alarms without Blocking** check box, and then click **OK**

#### CLI

1. set zone untrust screen alarm-without-drop
2. save

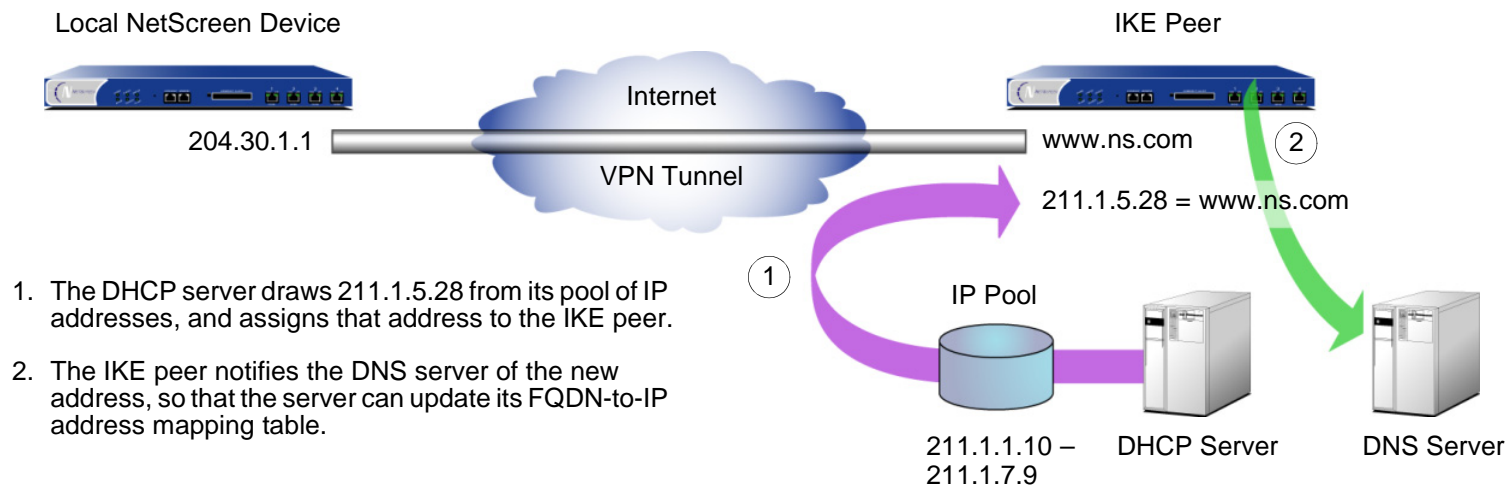
---

1. A honeypot is a decoy network server that is designed to lure attackers and then record their actions during an attack.

## FQDN FOR DYNAMIC IKE GATEWAYS

For an IKE peer that has a static fully qualified domain name (FQDN) but a dynamically assigned IP address, you can specify the FQDN in the local configuration for the remote gateway. For example, an Internet service provider (ISP) might assign IP addresses via DHCP to its customers. The ISP draws addresses from a pool of about 2000 addresses and assigns them when its customers come online. Although the IKE peer has a static FQDN, it has an unpredictably changing IP address. The IKE peer has three methods available for maintaining a Domain Name Service (DNS) mapping of its static FQDN to its dynamically assigned IP address (a process known as dynamic DNS).

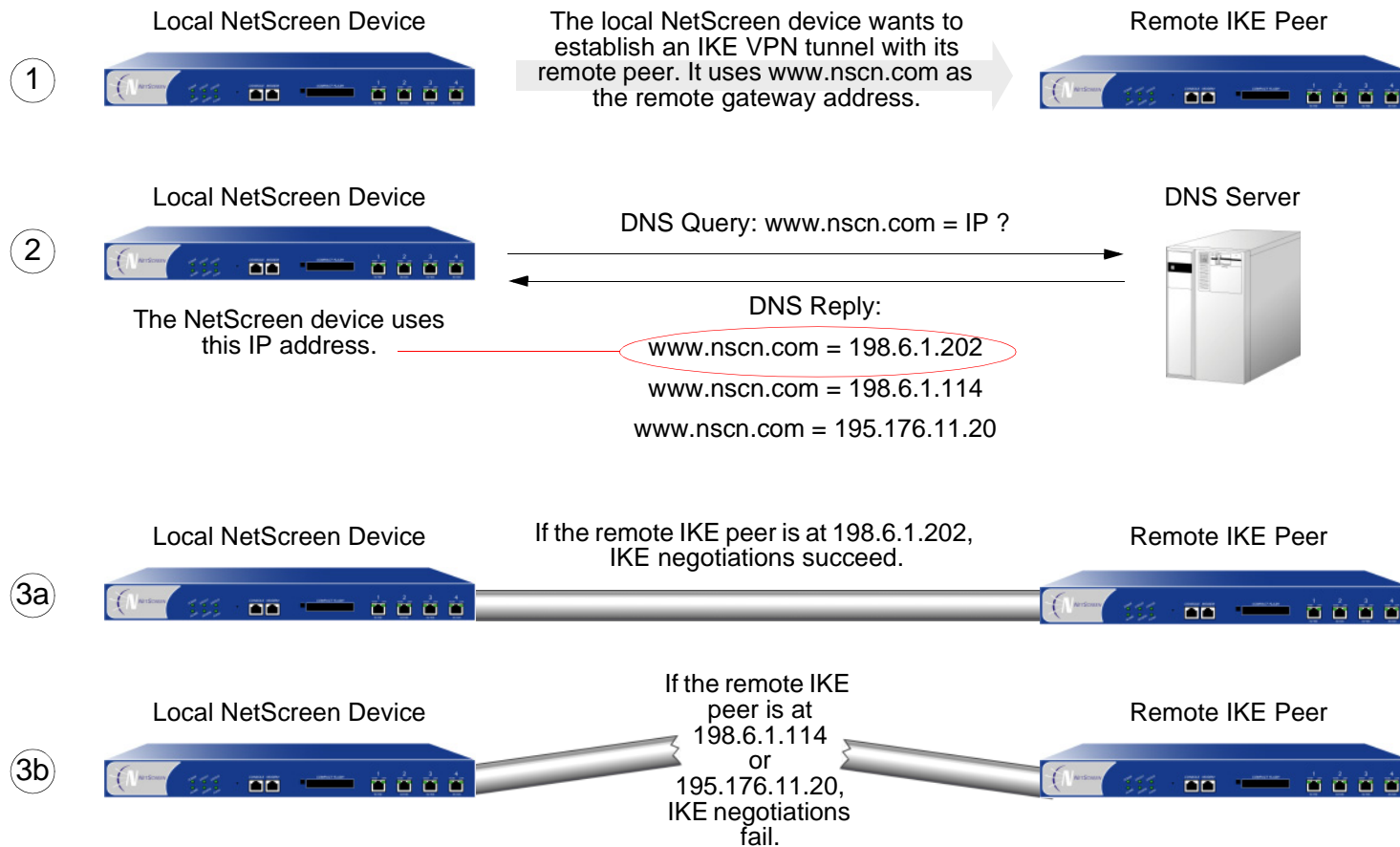
- If the remote IKE peer is a NetScreen device, the admin can manually notify the DNS server to update its FQDN-to-IP address mapping each time the NetScreen device receives a new IP address from its ISP.
- If the remote IKE peer is another kind of VPN termination device that has dynamic DNS software running on it, that software can automatically notify the DNS server of its address changes so the server can update its FQDN-to-IP address mapping table.
- If the remote IKE peer is a NetScreen device or any other kind of VPN termination device, a host behind it can run an FQDN-to-IP address automatic update program that alerts the DNS server of address changes.



Without needing to know the current IP address of a remote IKE peer, you can now configure an AutoKey IKE VPN tunnel to that peer using its FQDN instead of an IP address.

## Aliases

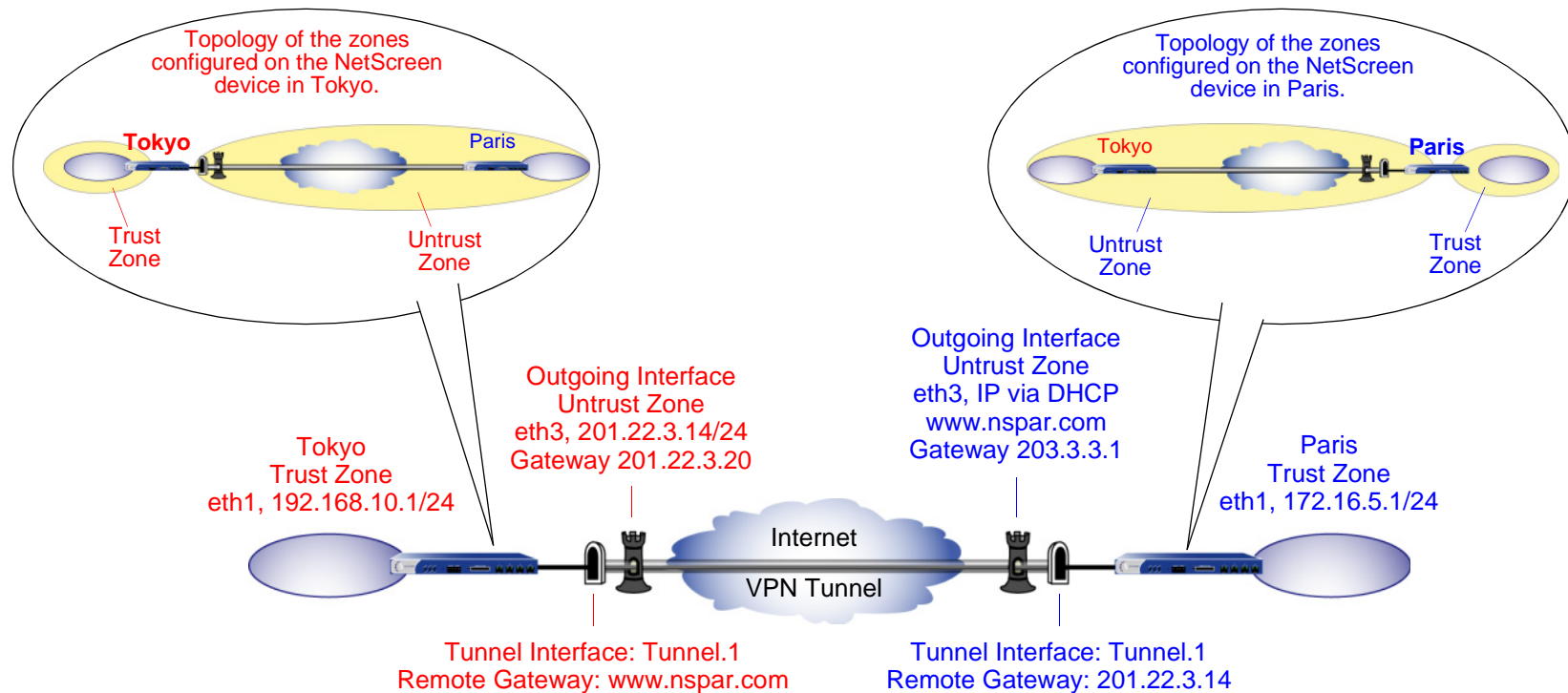
You can also use an alias for the FQDN of the remote IKE peer if the DNS server that the local NetScreen device queries returns only one IP address. If the DNS server returns several IP addresses, the local device uses the first one it receives. Because there is no guarantee for the order of the addresses in the response from the DNS server, the local NetScreen device might use the wrong IP address and IKE negotiations might fail.



## Example: IKE Peer with FQDN

In this example, an AutoKey IKE VPN tunnel using either a preshared secret or a pair of certificates (one at each end of the tunnel) provides a secure connection between two offices in Tokyo and Paris. The Paris office has a dynamically assigned IP address, so the Tokyo office uses the remote peer's FQDN (`www.nspar.com`) as the address of the remote gateway in its VPN tunnel configuration.

The following configuration is for a routing-based VPN tunnel. For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either `pre-g2-3des-sha` for the preshared key method or `rsa-g2-3des-sha` for certificates—and select the predefined “Compatible” set of proposals for Phase 2. All zones are in the trust-vr.



Setting up a routing-based AutoKey IKE tunnel using either a preshared secret or certificates involves the following steps:

1. Assign IP addresses to the physical interfaces bound to the security zones and to the tunnel interface.
2. Define the remote gateway and key exchange mode, and specify either a preshared secret or a certificate
3. Configure the VPN tunnel, designate its outgoing interface in the Untrust zone, bind it to the tunnel interface, and configure its proxy-ID.
4. Enter the IP addresses for the local and remote endpoints in the Trust and Untrust address books.
5. Enter a default route to the external router in the trust-vr, and a route to the destination via the tunnel interface.
6. Set up policies for traffic to pass between each site.

In the following examples, the preshared key is h1p8A24nG5. It is assumed that both participants already have RSA certificates and are using Entrust as the certificate authority (CA). (For information about obtaining and loading certificates, see *NetScreen Concepts & Examples ScreenOS Reference Guide, Volume 4, VPNs.*)

### WebUI (Tokyo)

#### Interfaces – Security Zones and Tunnel

1. Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **OK**:  
Zone Name: Trust  
IP Address/Netmask: 192.168.10.1/24
2. Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:  
Zone Name: Untrust  
IP Address/Netmask: 201.22.3.14
3. Network > Interfaces > Tunnel IF New: Enter the following, and then click **OK**:  
Tunnel Interface Name: tunnel.1  
Zone: Untrust  
Unnumbered: (select)  
Interface: ethernet3(Untrust)

## Addresses

4. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust\_LAN

IP Address/Domain Name:

IP/Netmask: 192.168.10.0/24

Zone: Trust

5. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris\_office

IP Address/Domain Name:

IP/Netmask: 172.16.5.0/24

Zone: Untrust

## VPN

1. VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To\_Paris

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: www.nspar.com

(Preshared Key)

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(Certificates)

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

2. VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Tokyo\_Paris

Security Level: Compatible

Remote Gateway:

Predefined (select), To\_Paris

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible

Bind to Tunnel Interface: (select), tunnel.1

Proxy-ID: (select)

Local IP/Netmask: 192.168.10.0/24

Remote IP/Netmask: 172.16.5.0/24

Service: ANY

## Routes

3. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:
  - Network Address/Netmask: 0.0.0.0/0
  - Gateway: (select)
  - Interface: ethernet3
  - Gateway IP Address: 201.22.3.20
4. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:
  - Network Address/Netmask: 172.16.5.0/24
  - Gateway: (select)
  - Interface: Tunnel.1
  - Gateway IP Address: 0.0.0.0

## Policies

5. Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:
  - Name: To Paris
  - Source Address: Trust\_LAN
  - Destination Address: Paris\_office
  - Service: ANY
  - Action: Permit
  - Position at Top: (select)

6. Policies > Policy (From: Untrust, To: Trust) > New Policy: Enter the following, and then click **OK**:

Name: From Paris

Source Address: Paris\_office

Destination Address: Trust\_LAN

Service: ANY

Action: Permit

Position at Top: (select)

### *WebUI (Paris)*

#### Host Name and Domain Name

1. Network > DNS: Enter the following, and then click **Apply**:

Host Name: www

Domain Name: nspar.com

#### Interfaces – Security Zones

2. Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **OK**:

Zone Name: Trust

IP Address/Netmask: 172.16.5.1/24

3. Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Obtain IP using DHCP: (select)

4. Network > Interfaces > Tunnel IF New: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone: Untrust

Unnumbered: (select)

Interface: ethernet3(Untrust)

### Addresses

5. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust\_LAN

IP Address/Domain Name:

IP/Netmask: (select), 172.16.5.0/24

Zone: Trust

6. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo\_office

IP Address/Domain Name:

IP/Netmask: (select), 192.168.10.0/24

Zone: Untrust

## VPN

7. VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To\_Tokyo

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 201.22.3.14

(Preshared Key)

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

- > Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level):  
pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(Certificates)

Outgoing Interface: ethernet3

- > Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

8. VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

Name: Paris\_Tokyo

Security Level: Custom

Remote Gateway:

Predefined (select), To\_Tokyo

- > Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible

Bind to Tunnel Interface: (select), tunnel.1

Proxy-ID: (select)

Local IP/Netmask: 172.16.5.0/24

Remote IP/Netmask: 192.168.10.0/24

Service: ANY

## Routes

9. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 203.3.3.1

10. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 192.168.10.0/24

Gateway: (select)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

## Policies

11. Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To Tokyo

Source Address: Trust\_LAN

Destination Address: Tokyo\_office

Service: ANY

Action: Permit

Position at Top: (select)

12. Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Name: From Tokyo

Source Address: Tokyo\_office

Destination Address: Trust\_LAN

Service: ANY

Action: Permit

Position at Top: (select)

## CLI (Tokyo)

### Interfaces – Zones and Tunnel

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 192.168.10.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 201.22.3.14/24
5. set interface tunnel.1 zone untrust
6. set interface tunnel.1 ip unnumbered interface ethernet3

### Addresses

7. set address trust Trust\_LAN 192.168.10.0/24
8. set address untrust paris\_office 172.16.5.0/24

### VPN

#### Preshared Key

- 9a. set ike gateway to\_paris address www.nspar.com main outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
- 9b. set vpn tokyo\_paris gateway to\_paris sec-level compatible
- 9c. set vpn tokyo\_paris bind interface tunnel.1
- 9d. set vpn tokyo\_paris proxy-id local-ip 192.168.10.0/24 remote-ip 172.16.5.0/24 any

## Certificate

- 9a. set ike gateway to\_paris address www.nspar.com main outgoing-interface ethernet3 proposal rsa-g2-3des-sha
- 9b. set ike gateway to\_paris cert peer-ca 1<sup>2</sup>
- 9c. set ike gateway to\_paris cert peer-cert-type x509-sig
- 9d. set vpn tokyo\_paris gateway to\_paris sec-level compatible
- 9e. set vpn tokyo\_paris bind interface tunnel.1
- 9f. set vpn tokyo\_paris proxy-id local-ip 192.168.10.0/24 remote-ip 172.16.5.0/24 any

## Routes

10. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.22.3.20
11. set vrouter trust-vr route 172.16.5.0/24 interface tunnel.1

## Policies

12. set policy top name "To Paris" from trust to untrust Trust\_LAN paris\_office any permit
13. set policy top name "From Paris" from untrust to trust paris\_office Trust\_LAN any permit
14. save

---

2. The number 1 is the CA ID number. To discover the CA's ID number, use the following command: **get pki x509 list ca-cert**.

## CLI (Paris)

### Host Name and Domain Name

1. set hostname www
2. set domain nspar.com

### Interfaces – Zones and Tunnel

3. set interface ethernet1 zone trust
4. set interface ethernet1 ip 172.16.5.1/24
5. set interface ethernet1 nat
6. set interface ethernet3 zone untrust
7. set interface ethernet3 ip dhcp-client enable
8. set interface tunnel.1 zone untrust
9. set interface tunnel.1 ip unnumbered interface ethernet3

### Addresses

10. set address trust Trust\_LAN 172.16.5.0/24
11. set address untrust tokyo\_office 192.168.10.0/24

### VPN

#### Preshared Key

- 12a. set ike gateway to\_tokyo address 201.22.3.14 main outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
- 12b. set vpn paris\_tokyo gateway to\_tokyo sec-level compatible
- 12c. set vpn paris\_tokyo bind interface tunnel.1
- 12d. set vpn paris\_tokyo proxy-id local-ip 172.16.5.0/24 remote-ip 192.168.10.0/24 any

## Certificate

- 12a. set ike gateway to\_tokyo address 201.22.3.14 main outgoing-interface ethernet3 proposal rsa-g2-3des-sha
- 12b. set ike gateway to\_tokyo cert peer-ca 1<sup>2</sup>
- 12c. set ike gateway to\_tokyo cert peer-cert-type x509-sig
- 12d. set vpn paris\_tokyo gateway to\_tokyo sec-level compatible
- 12e. set vpn paris\_tokyo bind interface tunnel.1
- 12f. set vpn paris\_tokyo proxy-id local-ip 172.16.5.0/24 remote-ip 192.168.10.0/24 any

## Routes

- 13. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.3.3.1
- 14. set vrouter trust-vr route 192.168.10.0/24 interface tunnel.1

## Policies

- 15. set policy top name "To Tokyo" from trust to untrust Trust\_LAN tokyo\_office any permit
- 16. set policy top name "From Tokyo" from untrust to trust tokyo\_office Trust\_LAN any permit
- 17. save

## BIDIRECTIONAL POLICIES FOR DIALUP VPN USERS

You can create bidirectional policies for dialup-to-LAN VPNs. This feature provides similar functionality as a dialup-to-LAN dynamic peer VPN configuration. However, in that configuration, the dialup user must configure an internal IP address, so that the admin at the LAN site can use it as the destination address when configuring an outgoing policy. With this new feature, the NetScreen device protecting the LAN uses the predefined address “Dial-Up VPN” as the source address in the incoming policy and the destination in the outgoing policy.

The ability to create bidirectional policies for a dialup-to-LAN VPN tunnel allows traffic to originate from the LAN end of the VPN connection after the connection has been established. Note that unlike a dialup-to-LAN dynamic peer VPN tunnel, this feature requires that the services on the incoming and outgoing policies be identical.

### Example: Bidirectional Dialup-to-LAN VPN Policies

In this example, you configure bidirectional policies for a dialup AutoKey IKE VPN tunnel named *VPN\_dial* for IKE user *dialup-j* with IKE ID *jf@ns.com*. For Phase 1 negotiations, you use the proposal *pre-g2-3des-sha*, with the preshared key *Jf11d7uU*. You select the predefined “Compatible” set of proposals for Phase 2 negotiations.

The IKE user initiates a VPN connection to the NetScreen device from the Untrust zone to reach corporate servers in the Trust zone. After the IKE user establishes the VPN connection, traffic can initiate from either end of the tunnel.

The Trust zone interface is ethernet1, has IP address 10.1.1.1/24, and is in NAT mode. The Untrust zone interface is ethernet3 and has IP address 210.1.1.1/24. The default route points to the external router at 210.1.1.2.

#### WebUI

##### Interfaces – Security Zones

1. Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

2. Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

IP Address/Netmask: 210.1.1.1/24

## Objects

3. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: trust\_net

IP Address/Domain Name:

IP/Netmask: 10.1.1.0/24

Zone: Trust

4. Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: dialup-j

Status: Enable

IKE User: (select)

Simple Identity: (select); jf@ns.com

## VPN

5. VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: dialup1

Security Level: Custom

Remote Gateway Type:

Dialup User: (select); dialup-j

Preshared Key: Jf11d7uU

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level):  
pre-g2-3des-sha

Mode (Initiator): Aggressive

6. VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN\_dial

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (select)

Gateway Name: dialup1

Type:

Dialup User: (select); dialup-j

Preshared Key: Jf11d7uU

Security Level: Compatible

Outgoing Interface: ethernet3

## Route

7. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet1(untrust)

Gateway IP Address: 210.1.1.2

## Policies

8. Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book: (select), Dial-Up VPN

Destination Address:

Address Book: (select), trust\_net

Service: ANY

Action: Tunnel

VPN Tunnel: VPN\_dial

Modify matching VPN policy: (select)

Position at Top: (select)

## CLI

### Interfaces – Security Zones

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet1 nat
4. set interface ethernet3 zone untrust
5. set interface ethernet3 ip 210.1.1.1/24

### Objects

6. set address trust trust\_net 10.1.1.0/24
7. set user dialup-j ike-id u-fqdn jf@ns.com

### VPN

8. set ike gateway dialup1 dialup dialup-j aggressive outgoing-interface ethernet3 preshare Jf11d7uU proposal pre-g2-3des-sha
9. set vpn VPN\_dial gateway dialup1 sec-level compatible

### Route

10. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 210.1.1.2

### Policies

11. set policy top from untrust to trust “Dial-Up VPN” trust\_net any tunnel vpn VPN\_dial
12. set policy top from trust to untrust trust\_net “Dial-Up VPN” any tunnel vpn VPN\_dial
13. save

### *NetScreen-Remote Security Policy Editor*

1. Click **Options > Secure > Specified Connections**.
2. Click **Add a new connection**, and type **Corp** next to the new connection icon that appears.
3. Configure the connection options:
  - Connection Security: Secure
  - Remote Party ID Type: IP Subnet
  - IP Address: 10.1.1.0
  - Mask: 255.255.255.0
  - Connect using Secure Gateway Tunnel: (select)
  - ID Type: IP Address; 210.1.1.1
4. Click the **PLUS** symbol, located to the left of the UNIX icon, to expand the connection policy.
5. Click **My Identity**: Do either of the following:
  - Click **Pre-shared Key > Enter Key**: Type **Jf11d7uU**, and then click **OK**.
  - ID Type: (select **E-mail Address**), and type **jf@ns.com**.
6. Click the **Security Policy** icon, and select **Aggressive Mode**.
7. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.

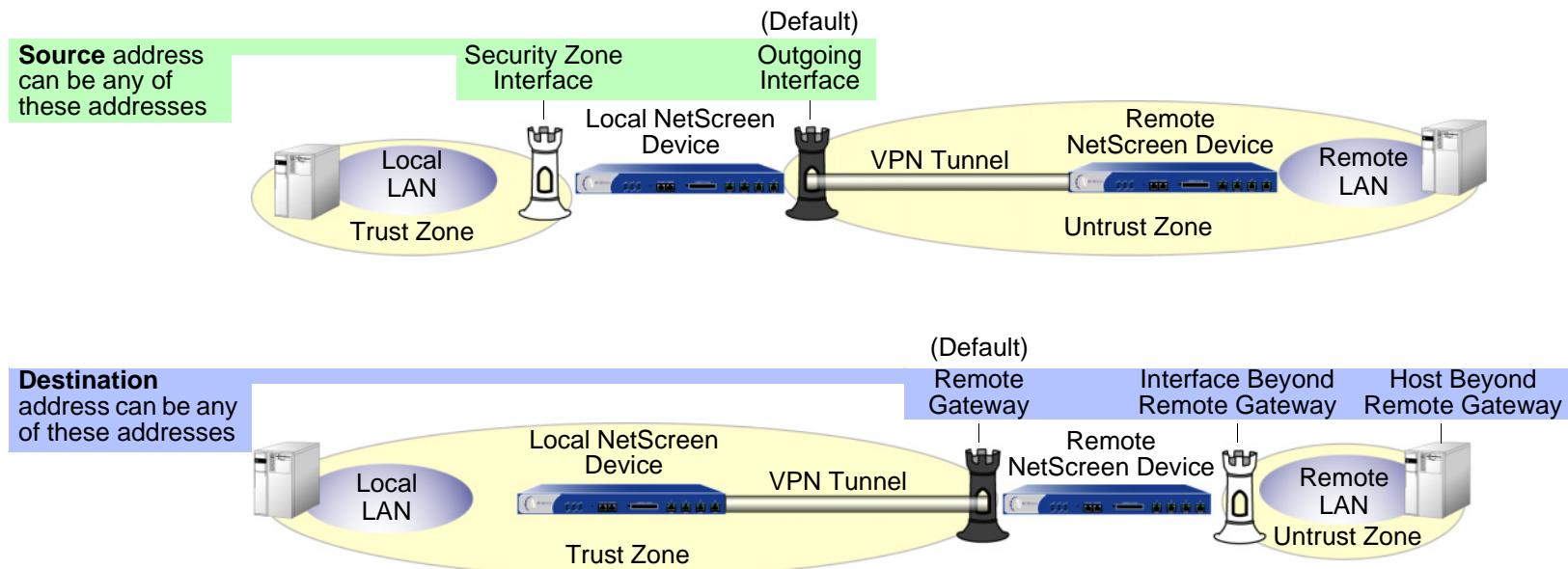
8. Click **Authentication (Phase 1) > Proposal 1**: Select the following Encryption and Data Integrity Algorithms:
  - Encrypt Alg: Triple DES
  - Hash Alg: SHA-1
  - Key Group: Diffie-Hellman Group 2
9. Click **Key Exchange (Phase 2) > Proposal 1**: Select the following IPSec Protocols:
  - Encapsulation Protocol (ESP): (select)
  - Encrypt Alg: Triple DES
  - Hash Alg: SHA-1
  - Encapsulation: Tunnel
10. Click **Key Exchange (Phase 2) > Create New Proposal**: Select the following IPSec Protocols:
  - Encapsulation Protocol (ESP): (select)
  - Encrypt Alg: Triple DES
  - Hash Alg: MD5
  - Encapsulation: Tunnel
11. Click **Key Exchange (Phase 2) > Create New Proposal**: Select the following IPSec Protocols:
  - Encapsulation Protocol (ESP): (select)
  - Encrypt Alg: DES
  - Hash Alg: SHA-1
  - Encapsulation: Tunnel
12. Click **Key Exchange (Phase 2) > Create New Proposal**: Select the following IPSec Protocols:
  - Encapsulation Protocol (ESP): (select)
  - Encrypt Alg: DES
  - Hash Alg: MD5
  - Encapsulation: Tunnel
13. Click **Save**.

## VPN MONITORING

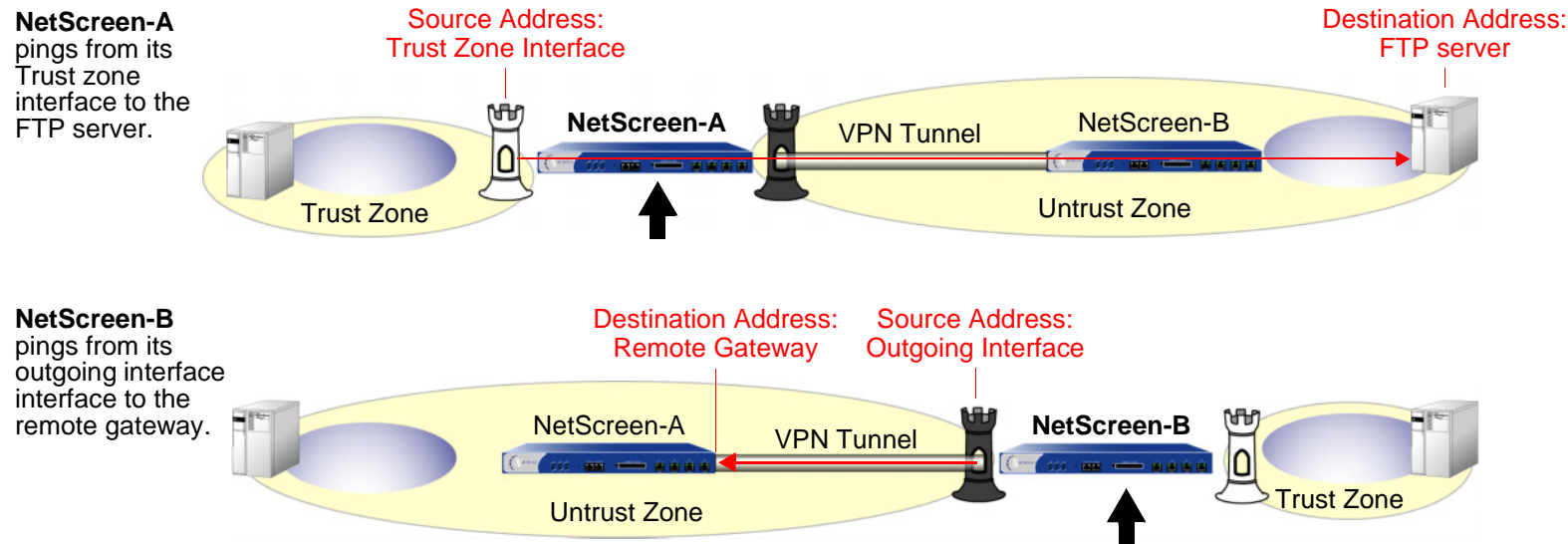
ScreenOS provides the ability to determine the status and condition of active VPNs through the use of SNMP VPN monitoring objects and traps. When you enable the VPN monitoring feature on a Manual Key or AutoKey IKE VPN tunnel, the NetScreen device activates its SNMP VPN monitoring objects.

**Note:** To enable your SNMP manager application to recognize the VPN monitoring MIBs, you must import the NetScreen-specific MIB extension files into the application. You can find the MIB extension files on the NetScreen documentation CD that shipped with your NetScreen device.

When VPN monitoring is enabled, the NetScreen device also sends ICMP echo requests ( or “pings”) through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity through the VPN tunnel. By default, the VPN monitoring feature uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address. ScreenOS 4.0.1 allows increased flexibility in allowing you to specify the use of other source and destination IP addresses for VPN monitoring—mainly to provide support for VPN monitoring when the other end of a VPN tunnel is not a NetScreen device.



The source address configured on the device at one end of the tunnel does not have to be the destination address configured on the device at the other end. For example, on the local device (NetScreen-A) you can specify the Trust zone interface as the source address and the IP address of a server beyond the remote gateway (NetScreen-B) as the destination address. On the remote device (NetScreen-B), you can use the default settings—the source address is the outgoing interface, and the destination address is the remote gateway.



You must create a policy on the sending device to permit pings from the zone containing the source interface to pass through the VPN tunnel to the zone containing the destination address if:

- The source interface is in a different zone from the destination address.
- The source interface is in the same zone as the destination address, and intrazone blocking is enabled.

Likewise, you must create a policy on the receiving device to permit pings from the zone containing the source address to pass through the VPN tunnel to the zone containing the destination address if:

- The destination address is in a different zone from the source address.
- The destination address is in the same zone as the source address, and intrazone blocking is enabled.

## Example: Specifying Source and Destination Addresses for VPN Monitoring

In this example, you configure an AutoKey IKE VPN tunnel between two NetScreen devices (NetScreen-A and NetScreen-B). On device A, you set up VPN monitoring from its Trust zone interface (ethernet1) to the Trust zone interface (10.2.1.1/24) on NetScreen-B. On the NetScreen-B, you set up VPN monitoring from its Trust zone interface (ethernet1) to a corporate intranet server (10.1.1.5) behind NetScreen-A.

NetScreen-A	NetScreen-B
<b>Zones and Interfaces</b> <ul style="list-style-type: none"> <li>ethernet1               <ul style="list-style-type: none"> <li>Zone: Trust</li> <li>IP address: 10.1.1.1/24</li> <li>Interface mode: NAT</li> </ul> </li> <li>ethernet3               <ul style="list-style-type: none"> <li>Zone: Untrust</li> <li>IP address: 210.1.1.1/24</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>ethernet1               <ul style="list-style-type: none"> <li>Zone: Trust</li> <li>IP address: 10.2.1.1/24</li> <li>Interface mode: NAT</li> </ul> </li> <li>ethernet3               <ul style="list-style-type: none"> <li>Zone: Untrust</li> <li>IP address: 202.2.2.2/24</li> </ul> </li> </ul>
<b>Routing-Based AutoKey IKE Tunnel Parameters</b> <ul style="list-style-type: none"> <li>Phase 1               <ul style="list-style-type: none"> <li>Gateway name: gw1</li> <li>Gateway static IP address: 202.2.2.2</li> <li>Security level: Compatible<sup>*</sup></li> <li>Preshared Key: Ti82g4aX</li> <li>Outgoing interface: ethernet3</li> <li>Mode: Main</li> </ul> </li> <li>Phase 2               <ul style="list-style-type: none"> <li>VPN tunnel name: vpn1</li> <li>Security level: Compatible<sup>†</sup></li> <li>VPN Monitoring: src = ethernet1; dst = 10.2.1.1</li> <li>Bound to interface: tunnel.1</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Phase 1               <ul style="list-style-type: none"> <li>Gateway name: gw1</li> <li>Gateway static IP address: 210.1.1.1</li> <li>Proposals: Compatible</li> <li>Preshared Key: Ti82g4aX</li> <li>Outgoing interface: ethernet3</li> <li>Mode: Main</li> </ul> </li> <li>Phase 2               <ul style="list-style-type: none"> <li>VPN tunnel name: vpn1</li> <li>Security level: Compatible</li> <li>VPN Monitoring: src = ethernet1; dst = 10.1.1.5</li> <li>Bound to interface: tunnel.1</li> </ul> </li> </ul>

<sup>\*</sup> A Phase 1 security level of Compatible includes the following proposals: pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, and pre-g2-des-md5.

<sup>†</sup> A Phase 1 security level of Compatible includes the following proposals: nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5.

NetScreen-A	NetScreen-B
Routes	
To 0.0.0.0/0, use ethernet3, gateway 210.1.1.20	To 0.0.0.0/0, use ethernet3, gateway 202.2.2.20
To 10.2.1.0/0, use tunnel.1, no gateway	To 10.1.1.0/0, use tunnel.1, no gateway

Because both devices ping from an interface in their Trust zone to an address in their Untrust zone, the admins at both ends of the VPN tunnel must define policies permitting pings to pass from zone to zone.

**Note:** Because both VPN terminators are NetScreen devices in this example, you can use the default source and destination addresses for VPN monitoring. The use of other options is included purely to illustrate how you can configure a NetScreen device to use them.

## WebUI (NetScreen-A)

### Interfaces – Security Zones and Tunnel

1. Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:
  - Zone Name: Trust
  - IP Address/Netmask: 10.1.1.1/24Enter the following, and then click **OK**:
  - Interface Mode: NAT
2. Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:
  - Zone Name: Untrust
  - IP Address/Netmask: 210.1.1.1/24

3. Network > Interfaces > Tunnel IF New: Enter the following, and then click **OK** :

Tunnel Interface Name: tunnel.1

Zone: Trust

Unnumbered: (select)

Interface: ethernet1(trust-vr)

### Addresses

4. Objects > Addresses > List > New: Enter the following, and then click **OK** :

Address Name: Trust\_LAN

IP Address/Domain Name:

IP/Netmask: 10.1.1.0/24

Zone: Trust

5. Objects > Addresses > List > New: Enter the following, and then click **OK** :

Address Name: Remote\_LAN

IP Address/Domain Name:

IP/Netmask: 10.2.1.0/24

Zone: Untrust

## VPN

6. VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (select)

Gateway Name: gw1

Type:

Static IP Address: (select), Address/Hostname: 202.2.2.2

Preshared Key: Ti82g4aX

Outgoing Interface: ethernet3

Security Level: Compatible

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to Tunnel Interface: (select), tunnel.1

Proxy-ID: (select)

Local IP/Netmask: 10.1.1.0/24

Remote IP/Netmask: 10.2.1.0/24

Service: ANY

VPN Monitor: (select)

Source Interface: ethernet1

Destination IP: 10.2.1.1

Rekey: (clear)

## Routes

7. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:
  - Network Address/Netmask: 0.0.0.0/0
  - Gateway: (select)
  - Interface: ethernet3
  - Gateway IP Address: 210.1.1.20
8. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:
  - Network Address/Netmask: 10.2.1.0/24
  - Gateway: (select)
  - Interface: Tunnel.1
  - Gateway IP Address: 0.0.0.0

## Policies

9. Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:
  - Source Address: Trust\_LAN
  - Destination Address: Remote\_LAN
  - Service: ANY
  - Action: Permit
  - Position at Top: (select)
10. Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:
  - Source Address: Remote\_LAN
  - Destination Address: Trust\_LAN
  - Service: Any
  - Action: Permit
  - Position at Top: (select)

## WebUI (NetScreen-B)

### Interfaces – Security Zones and Tunnel

1. Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **OK**:  
Zone Name: Trust  
IP Address/Netmask: 10.2.1.1/24  
  
Enter the following, and then click **OK**:  
Interface Mode: NAT
2. Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:  
Zone Name: Untrust  
IP Address/Netmask: 202.2.2.2/24
3. Network > Interfaces > Tunnel IF New: Enter the following, and then click **OK**:  
Tunnel Interface Name: tunnel.1  
Zone: Trust  
Unnumbered: (select)  
Interface: ethernet1(Trust)

### Addresses

4. Objects > Addresses > List > New: Enter the following, and then click **OK**:  
Address Name: Trust\_LAN  
IP Address/Domain Name:  
IP/Netmask: 10.2.1.0/24  
Zone: Trust

5. Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Remote\_LAN

IP Address/Domain Name:

IP/Netmask: 10.1.1.0/24

Zone: Untrust

## VPN

6. VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (select)

Gateway Name: gw1

Type:

Static IP Address: (select), Address/Hostname: 210.1.1.1

Preshared Key: Ti82g4aX

Outgoing Interface: ethernet3

Security Level: Compatible

- > Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to Tunnel Interface: (select), tunnel.1

Proxy-ID: (select)

Local IP/Netmask: 10.2.1.0/24

Remote IP/Netmask: 10.1.1.0/24

Service: ANY

VPN Monitor: (select)  
Source Interface: ethernet1  
Destination IP: 10.1.1.5  
Rekey: (clear)

## Routes

7. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:
  - Network Address/Netmask: 0.0.0.0/0
  - Gateway: (select)
  - Interface: ethernet3
  - Gateway IP Address: 202.2.2.20
8. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:
  - Network Address/Netmask: 10.1.1.0/24
  - Gateway: (select)
  - Interface: Tunnel.1
  - Gateway IP Address: 0.0.0.0

## Policies

9. Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:
  - Source Address: Trust\_LAN
  - Destination Address: Remote\_LAN
  - Service: ANY
  - Action: Permit
  - Position at Top: (select)
10. Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:
  - Source Address: Remote\_LAN
  - Destination Address: Trust\_LAN
  - Service: Any
  - Action: Permit
  - Position at Top: (select)

## CLI (NetScreen-A)

### Interfaces – Security Zones and Tunnel

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet1 nat
4. set interface ethernet3 zone untrust
5. set interface ethernet3 ip 210.1.1.1/24
6. set interface tunnel.1 zone trust
7. set interface tunnel.1 ip unnumbered interface ethernet1

### Addresses

8. set address trust Trust\_LAN 10.1.1.0/24
9. set address untrust Remote\_LAN 10.2.1.0/24

### VPN

10. set ike gateway gw1 ip 202.2.2.2 main outgoing-interface ethernet3 preshare Ti82g4aX sec-level compatible
11. set vpn vpn1 gateway gw1 sec-level compatible
12. set vpn vpn1 bind interface tunnel.1
13. set vpn vpn1 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.1.0/24 any
14. set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.2.1.1

### Routes

15. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 210.1.1.20
16. set vrouter trust-vr route 10.2.1.0/24 interface tunnel.1

### Policies

17. set policy top from trust to untrust Trust\_LAN Remote\_LAN any permit
18. set policy top from untrust to trust Remote\_LAN Trust\_LAN any permit
19. save

## CLI (NetScreen-B)

### Interfaces – Security Zones and Tunnel

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.2.1.1/24
3. set interface ethernet1 nat
4. set interface ethernet3 zone untrust
5. set interface ethernet3 ip 202.2.2.2/24
6. set interface tunnel.1 zone trust
7. set interface tunnel.1 ip unnumbered interface ethernet1

### Addresses

8. set address trust Trust\_LAN 10.2.1.0/24
9. set address untrust Remote\_LAN 10.1.1.0/24

### VPN

10. set ike gateway gw1 ip 210.1.1.1 main outgoing-interface ethernet3 preshare Ti82g4aX sec-level compatible
11. set vpn vpn1 gateway gw1 sec-level compatible
12. set vpn vpn1 bind interface tunnel.1
13. set vpn vpn1 proxy-id local-ip 10.2.1.0/24 remote-ip 10.1.1.0/24 any
14. set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.1.1.5

### Routes

15. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 202.2.2.20
16. set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1

### Policies

17. set policy top from trust to untrust Trust\_LAN Remote\_LAN any permit
18. set policy top from untrust to trust Remote\_LAN Trust\_LAN any permit
19. save

## SNMP

The Simple Network Management Protocol (SNMP) agent for the NetScreen device provides network administrators with a way to view statistical data about the network and the devices on it, and to receive notification of system events of interest. NetScreen supports the SNMPv1 protocol, described in RFC-1157, “A Simple Network Management Protocol”.

SNMP administrators are grouped in SNMP communities. NetScreen supports up to three SNMP communities, with up to eight members in each community. In previous releases of ScreenOS, an SNMP community member must be a single host. In ScreenOS 4.0.1, a community member can be either a host or a subnet of hosts, depending on the netmask you use when defining the member. To define an SNMP community member, do either of the following:

### WebUI

Configuration > Report Settings > SNMP > New Community: Enter the following settings, and then click **OK**:

Community Name: *comm\_name*

Permissions: (select options)

Hosts IP Address/Netmask: *ip\_addr/mask*

### CLI

```
set snmp host comm_name ip_addr [ mask ]
```

**Note:** By default, the NetScreen device assigns an SNMP community member a 32-bit netmask (255.255.255.255).

If you define a subnet, any device on that subnet can poll the NetScreen device for SNMP MIB information. However, the NetScreen device cannot send an SNMP trap to a subnet, only to an individual host.

## Example: Defining an SNMP Community

In this example, you create an SNMP community named *Mage*. You assign it read/write privileges and enable it to receive traps. It has the following two members: 10.1.1.1/32 and 10.1.1.0/24

The NetScreen device can only send traps to 10.1.1.1/32 because that is an IP address for a single host. However, that address belongs to the community leader. Upon receiving traps, the leader can then control the distribution of them to the other community members.

You also provide contact information for the local admin of the NetScreen device—name: Howard Thurston; location: hthurston@mage.com—in case an SNMP community member needs to contact him.

### WebUI

1. Configuration > Report Settings > SNMP: Enter the following settings, and then click **Apply**:

System Contact: Howard Thurston

Location: hthurston@mage.com

2. Configuration > Report Settings > SNMP > New Community: Enter the following settings, and then click **OK**:

Community Name: Mage

Permissions:

Write: (select)

Trap: (select)

Including Traffic Alarms: (clear)

Hosts IP Address/Netmask:

10.1.1.1/32

10.1.1.0/24

## CLI

1. set snmp contact Howard Thurston
2. set snmp location hthurston@mage.com
3. set snmp community Mage read-write trap-on
4. set snmp host Mage 10.1.1.1/32
5. set snmp host Mage 10.1.1.0/24
6. save

## VIRTUAL SYSTEM ZONES

You can logically partition a single NetScreen security system<sup>3</sup> into multiple virtual systems to provide multi-tenant services. Each virtual system (vsys) is a unique security domain and can share security zones with the root system and have its own security zones. When a root-level admin creates a vsys object, the following zones are automatically inherited or created:

- All shared zones (inherited from the root system)
- Shared Null zone (inherited from the root system)
- Trust-*vsys\_name* zone
- Untrust-Tun-*vsys\_name* zone
- Self-*vsys\_name* zone
- Global-*vsys\_name* zone

In ScreenOS 4.0.1, each vsys can also support up to four user-defined security zones. You can bind these zones to any shared virtual routers defined at the root level or to the virtual router dedicated to that vsys. To create a security zone for a vsys named vsys1, do either of the following:

### WebUI

1. Vsys > Enter (for vsys1).
2. Network > Zones > New: Enter the following, and then click **OK**:
  - Zone Name: (type a name for the zone)
  - Virtual Router Name: (select a virtual router from the drop-down list)
  - Zone Type: Layer 3

### CLI

1. ns-> enter vsys vsys1
2. ns (vsys1)-> set zone name *name\_str*
3. ns(vsys1)-> set zone vrouter *vrouter*
4. ns(vsys1)-> save

---

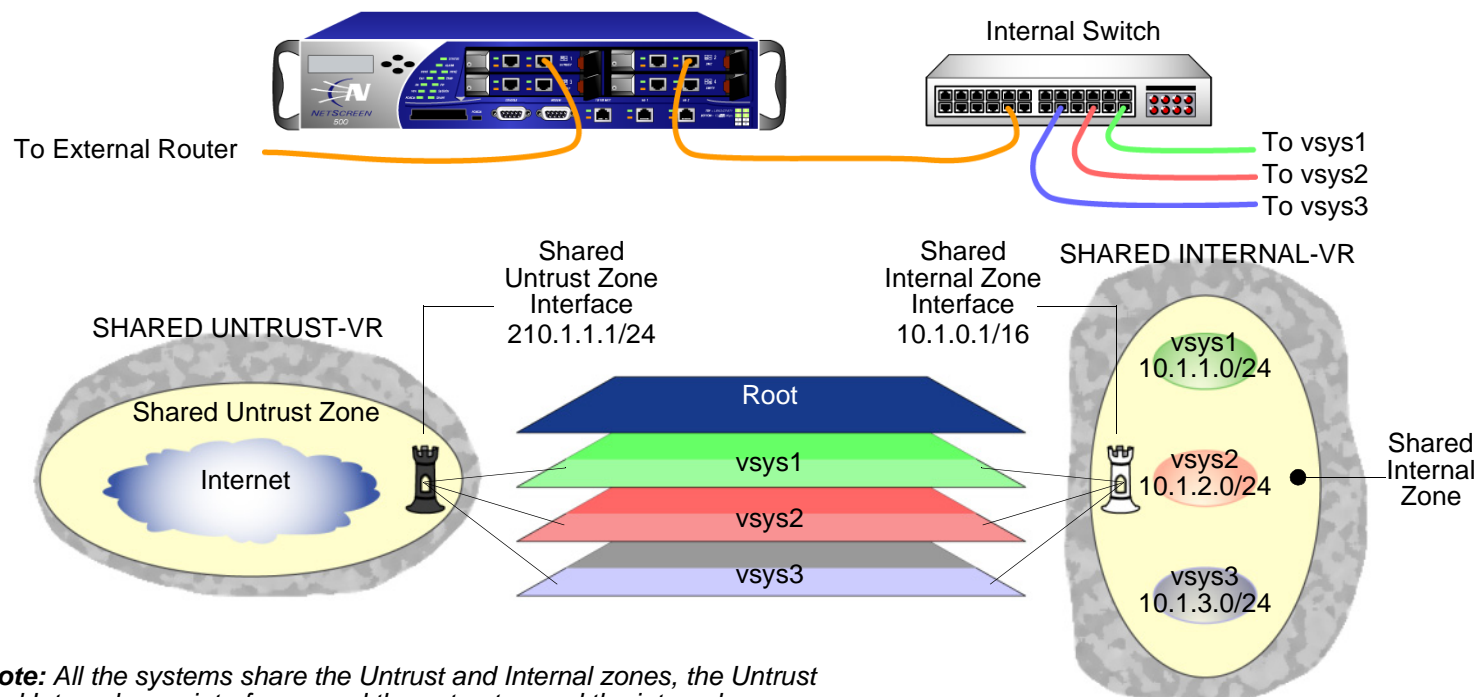
3. NetScreen devices are divided into two general categories: security systems and appliances. Only NetScreen security systems can support virtual systems. Refer to the NetScreen marketing literature to see which platforms support this feature.

## IP CLASSIFICATION FOR VIRTUAL SYSTEM TRAFFIC

NetScreen virtual systems support two kinds of traffic classifications: VLAN-based and IP-based, both of which can function exclusively or concurrently. In ScreenOS 4.0.1, you can now configure IP-based traffic classification for virtual systems through the WebUI.

With IP-based traffic classification, the NetScreen device uses IP addresses to sort traffic, associating a subnet or range of IP addresses with the a particular system—root or vsys. Using IP-based traffic classification exclusively to sort traffic, all systems share the following:

- The untrust-vr and a user-defined internal-vr
- The Untrust zone and up to four user-defined internal zones
- An Untrust zone interface and a user-defined internal zone interface



**Note:** All the systems share the Untrust and Internal zones, the Untrust and Internal zone interfaces, and the untrust-vr and the internal-vr.

## Example: Configuring IP-Based Traffic Classification

In this example, you set up IP-based traffic classification for the following three virtual systems and vsys admins:

- vsys1 – admin: Alice; password: wIEaS1v1
- vsys2 – admin: Bob; password: pjF56Ms2
- vsys3 – admin: Christine; password: 1RhMD553

You create a new zone, name it *Internal*, and bind it to the trust-vr. You then make both the trust-vr and the Internal zone sharable. You bind ethernet3/2 to the shared Internal zone, assign it IP address 10.1.0.1/16, and select NAT mode.

You bind ethernet1/2 to the shared Untrust zone and assign it IP address 210.1.1.1/24. The IP address of the default gateway in the Untrust zone is 210.1.1.250. Both the Internal and Untrust zones are in the shared trust-vr routing domain.

The subnets and their respective vsys associations are as follows:

- 10.1.1.0/24 – vsys1
- 10.1.2.0/24 – vsys2
- 10.1.3.0/24 – vsys3

### WebUI

#### Virtual Systems and Vsys Admins

1. Vsys > New: Enter the following, and then click **OK**:

VSYS Name: vsys1

VSYS Admin Name: Alice

VSYS Admin Password: wIEaS1v1

Confirm Password: wIEaS1v1

2. Vsys > New: Enter the following, and then click **OK**:
  - VSYS Name: vsys2
  - VSYS Admin Name: Bob
  - VSYS Admin Password: pjF56Ms2
  - Confirm Password: pjF56Ms2
3. Vsys > New: Enter the following, and then click **OK**:
  - VSYS Name: vsys3
  - VSYS Admin Name: Christine
  - VSYS Admin Password: 1Rhmd553

### Virtual Routers, Security Zones, and Interfaces

4. Network > Routing > Virtual Routers > Edit (for trust-vr): Select the **Shared and accessible by other vsys** check box, and then click **OK**.
5. Network > Zones > New: Enter the following, and then click **OK**:
  - Zone Name: Internal
  - Virtual Router Name: trust-vr
  - Zone Type: Layer 3
6. Network > Zones > Edit (for Internal): Select the **Shared Zone** check box, and then click **OK**.
7. Network > Interfaces > Edit (for ethernet3/2): Enter the following, and then click **OK**:
  - Zone Name: Internal
  - IP Address/Netmask: 10.1.0.1/16
8. Network > Interfaces > Edit (for ethernet1/2): Enter the following, and then click **OK**:
  - Zone Name: Untrust
  - IP Address/Netmask: 210.1.1.1/24

## Route

9. Network > Routing > Routing Table > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet1/2

Gateway IP Address: 210.1.1.250

## IP Classification of the Trust Zone

10. Network > Zones > Edit (for Internal) > IP Classification: Enter the following, and then click **OK**:

System: vsys1

Address Type:

Subnet: (select); 10.1.1.0/24

11. Network > Zones > Edit (for Internal) > IP Classification: Enter the following, and then click **OK**:

System: vsys2

Address Type:

Subnet: (select); 10.1.2.0/24

12. Network > Zones > Edit (for Internal) > IP Classification: Enter the following, and then click **OK**:

System: vsys3

Address Type:

Subnet: (select); 10.1.3.0/24

13. Network > Zones > Edit (for Internal): Select the **IP Classification** check box, and then click **OK**.

## CLI

### Virtual Systems and Vsys Admins

1. ns-> set vsys vsys1
2. ns(vsys1)-> set admin name Alice
3. ns(vsys1)-> set admin password wIEaS1v1
4. ns(vsys1)-> save<sup>4</sup>
5. ns(vsys1)-> exit
6. ns-> set vsys vsys2
7. ns(vsys2)-> set admin name Bob
8. ns(vsys2)-> set admin password pjF56Ms2
9. ns(vsys2)-> save
10. ns(vsys2)-> exit
11. ns-> set vsys vsys3
12. ns(vsys3)-> set admin name Christine
13. ns(vsys3)-> set admin password 1Rhmd553
14. ns(vsys3)-> save

### Virtual Routers, Security Zones, and Interfaces

15. set vrouter trust-vr shared
16. set zone name Internal
17. set zone Internal shared
18. set interface ethernet3/2 zone Internal
19. set interface ethernet3/2 ip 10.1.0.1/16
20. set interface ethernet3/2 nat

---

4. After issuing any commands, you must issue a **save** command before issuing an **exit** command or the NetScreen device loses your changes

21. set interface ethernet1/2 zone untrust
22. set interface ethernet1/2 ip 210.1.1.1/24

### Route

23. set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/2 gateway 210.1.1.250

### IP Classification of the Trust Zone

24. set zone Internal ip-classification net 10.1.1.0/24 vsys1
25. set zone Internal ip-classification net 10.1.2.0/24 vsys2
26. set zone Internal ip-classification net 10.1.3.0/24 vsys3
27. set zone Internal ip-classification
28. save

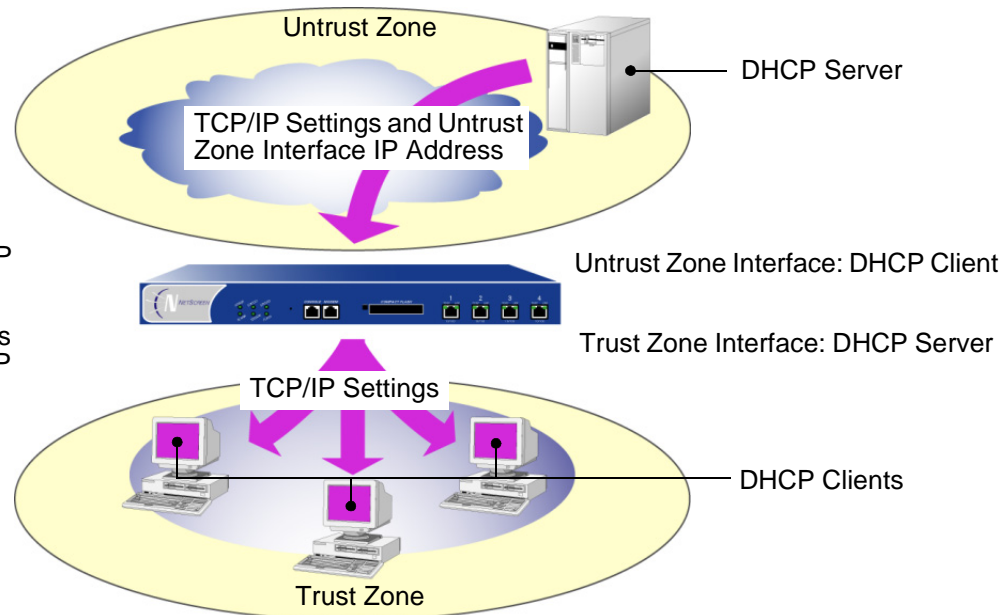
## TCP/IP SETTINGS PROPAGATION

Some NetScreen devices can act as a Dynamic Host Control Protocol (DHCP) client, receiving its TCP/IP settings and the IP address for its Untrust zone interface from an external DHCP server. Some NetScreen devices can act as a DHCP server, providing TCP/IP settings and IP addresses to clients in the Trust zone. When a NetScreen device acts both as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its DHCP server module. TCP/IP settings include the IP address of the default gateway and a subnet mask, and IP addresses for any or all of the following servers:

- DNS (3)
- WINS (2)
- NetInfo (2)
- SMTP (1)
- POP3 (1)
- News (1)

The NetScreen device is both a client of the DHCP server in the Untrust zone and a DHCP server to the clients in the Trust zone.

It takes the TCP/IP settings that it receives as a DHCP client and forwards them as a DHCP server to the clients in the Trust zone.



You can configure the DHCP server module to propagate all TCP/IP settings that it receives from the DHCP client module. You can also override any setting with a different one.

## Example: Forwarding TCP/IP Settings

In this example, you configure the NetScreen device to act both as a DHCP client on the Untrust interface and as a DHCP server on the Trust interface.

As a DHCP client, the NetScreen device receives an IP address for the Untrust interface and its TCP/IP settings from an external DHCP server at 211.3.1.6. You enable the DHCP client module in the NetScreen device to transfer the TCP/IP settings it receives to the DHCP server module.

You configure the NetScreen DHCP server module to do the following with the TCP/IP settings that it receives from the DHCP client module:

- Forward the DNS IP addresses to its DHCP clients in the Trust zone.
- Override the default gateway<sup>5</sup>, netmask, and SMTP server and POP3 server IP addresses with the following:
  - 10.1.1.1 (this is the IP address of the Trust interface)
  - 255.255.255.0 (this is the netmask for the Trust interface)
  - SMTP: 211.1.8.150
  - POP3: 211.1.8.172

You also configure the DHCP server module to deliver the following TCP/IP settings that it does not receive from the DHCP client module:

- Primary WINS server: 10.1.2.42
- Secondary WINS server: 10.1.5.90

Finally, you configure the DHCP server module to assign IP addresses from the following IP Pool to the hosts acting as DHCP clients in the Trust zone: 10.1.1.50 – 10.1.1.200.

---

5. If the DHCP server is already enabled on the Trust interface and has a defined pool of IP addresses (which is default behavior on some NetScreen devices), you must first delete the IP address pool before you can change the default gateway and netmask.

## WebUI

1. Network > Interfaces > Edit (for Untrust): Enter the following, and then click **OK**:
  - Obtain IP using DHCP: (select)<sup>6</sup>
  - Update DHCP Server: (select)
2. Network > Interfaces > Edit (for Trust) > DHCP: Enter the following, and then click **Apply**:
  - DHCP Server: (select)
  - Lease: Unlimited
  - Gateway: 10.1.1.1
  - Netmask: 255.255.255.0
  - WINS#1: 10.1.2.42
  - > Advanced Options: Enter the following, and then click **OK**:
    - WINS#2: 10.1.5.90
    - POP3: 211.1.8.172
    - SMTP: 211.1.8.150
  - > New Address: Enter the following, and then click **OK**:
    - Dynamic: (select)
    - IP Address Start: 10.1.1.50
    - IP Address End: 10.1.1.200

---

6. You can only specify the IP address of the external DHCP server with the CLI command **set interface untrust dhcp-client settings server ip\_addr**.

## CLI

1. set interface untrust dhcp-client settings server 211.3.1.6
2. set interface untrust dhcp-client settings update-dhcpserver
3. set interface untrust dhcp-client settings autoconfig
4. set interface untrust dhcp-client enable
5. set interface trust dhcp server option gateway 10.1.1.1
6. set interface trust dhcp server option netmask 255.255.255.0
7. set interface trust dhcp server option wins1 10.1.2.42
8. set interface trust dhcp server option wins2 10.1.5.90
9. set interface trust dhcp server option pop3 211.1.8.172
10. set interface trust dhcp server option smtp 211.1.8.150
11. set interface trust dhcp server ip 10.1.1.50 to 10.1.1.200
12. set interface trust dhcp server service
13. save

## DNS REFRESH

The NetScreen device incorporates Domain Name System (DNS) support allowing you to use domain names as well as IP addresses for identifying locations. The NetScreen device refreshes all the entries in its DNS table by checking them with a specified DNS server at the following times:

- After you reset the NetScreen device
- After an HA failover occurs
- At a regularly scheduled time of day and at regularly scheduled intervals throughout the day
- When you manually command the device to perform a DNS lookup
  - WebUI: Network > DNS: Click Refresh DNS cache.
  - CLI: `exec dns lookup`

In addition to the existing method of setting a time for a daily automatic refresh of the DNS table, you can also define an interval of time from 4 hours to 24 hours.

**Note:** When you add a fully-qualified domain name (FQDN) such as an address or IKE gateway through the WebUI, the NetScreen device resolves it when you click **Apply** or **OK**. When you type a CLI command that references an FQDN, the NetScreen device attempts to resolve it when you enter it.

### Example: Setting a DNS Refresh Interval

In this example, you configure the NetScreen device to refresh its DNS table every 4 hours beginning at 12:01 AM every day.

#### WebUI

Network > DNS: Enter the following, and then click **Apply** :

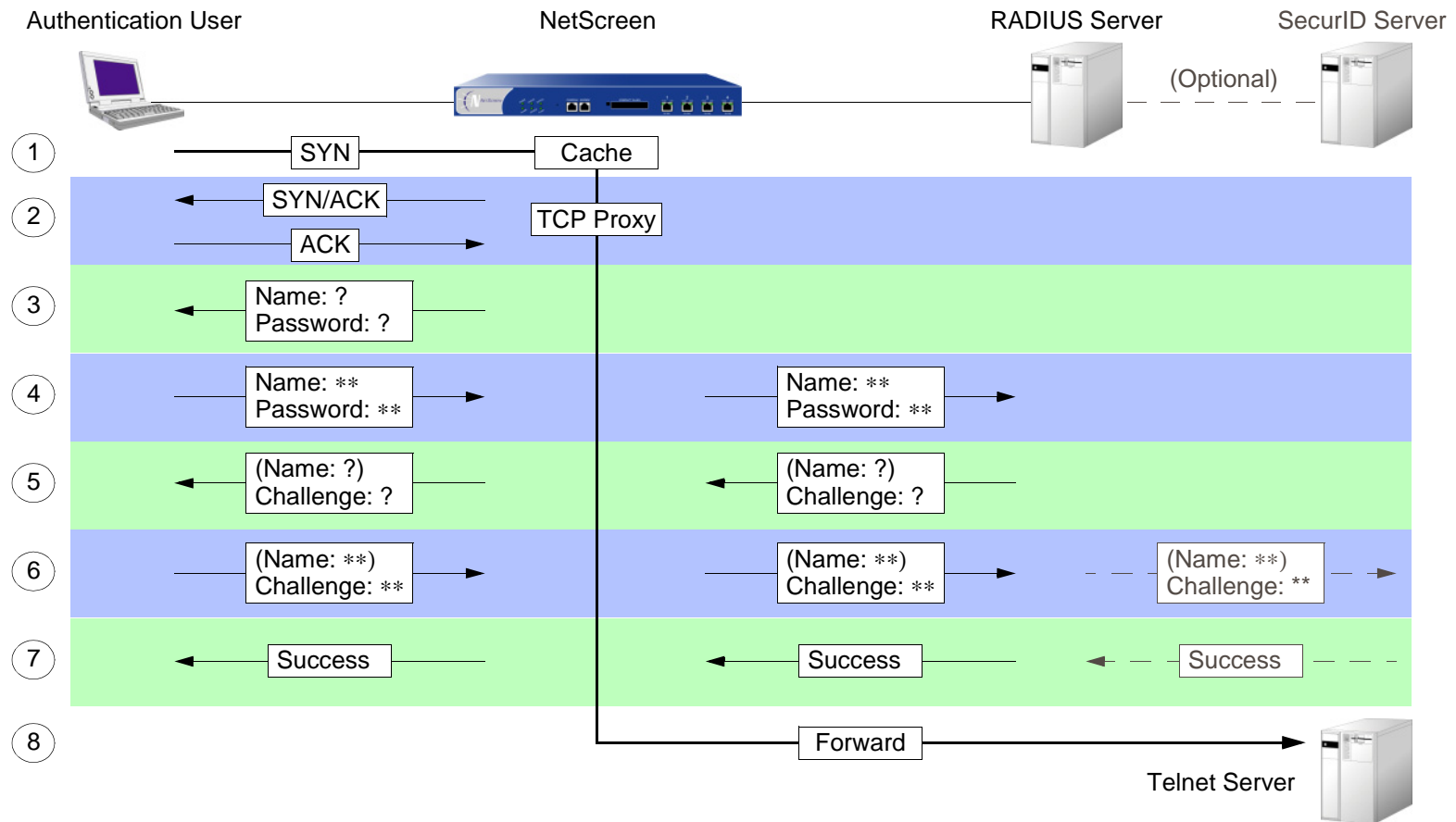
DNS Refresh: (select)  
Every Day at: 12:01  
Interval: 4

#### CLI

1. `set dns host schedule 12:01 interval 4`
2. `save`

## RADIUS ACCESS-CHALLENGE

NetScreen devices can now process access-challenge packets from an external RADIUS server when an authentication user attempts to log on via Telnet. Access-challenge presents an additional condition to the login process after the approval of a user name and password. After an authentication user responds to a login prompt with the correct user name and password, the RADIUS server sends an access-challenge to the NetScreen device, which then forwards it to the user. When the user replies, the NetScreen device sends a new access-request with the user's response to the RADIUS server. If the user's response is correct, the authentication process concludes successfully. Consider the following scenario in which an authentication user wants to telnet to a server:



1. An authentication user sends a SYN packet to initiate a TCP connection for a Telnet session to a Telnet server.
2. A NetScreen device intercepts the packet, checks its policy list, and determines that this session requires user authentication. The NetScreen device caches the SYN packet and proxies the TCP 3-way handshake with the user.
3. The NetScreen device prompts the user to log in with a user name and password.
4. The authentication user enters his or her user name and password and sends it to the NetScreen device. The NetScreen device then sends an access-request with the login information to a RADIUS server.
5. If the information is correct, the RADIUS server sends the NetScreen device an access-challenge with a reply-message attribute that prompts the user to provide a response to a challenge. (The access-challenge can optionally prompt the authentication to provide a user name again. The second user name can be the same as the first or a different one.) The NetScreen device then sends the user another login prompt that contains the content of the reply-message attribute.
6. The authentication user enters his or her challenge response (and optionally a user name) and sends it to the NetScreen device. The NetScreen device then sends a second access-request, with the user's challenge-response, to the RADIUS server.

If the RADIUS server needs to authenticate the challenge-response via another auth server—for example, if a SecurID server must authenticate a token code—the RADIUS server sends the access-request to the other auth server.

7. If the RADIUS server forwarded the challenge-response to another auth server and that server sends an access-accept, or if the RADIUS server itself approves the challenge-response, the RADIUS server sends an access-accept message to the NetScreen device. The NetScreen device then notifies the authentication user that his or her login is successful.
8. The NetScreen device forwards the initial SYN packet to its original destination: the Telnet server.

**Note:** NetScreen does not support access-challenge with L2TP at the time of this release.



## ScreenOS 4.0.2 New Features and Enhancements

---

This chapter presents the new features and feature enhancements introduced in this release. It contains the following sections:

- “Administration” on page 76
  - “Root Admin” on page 76
  - “Admin Users” on page 79
- “Counting Statistics in the WebUI” on page 82
- “SCREENS for MGT Zone” on page 83

The contents of this chapter focus exclusively on new features added in this release and enhancements made to existing features. For more complete information about ScreenOS features, refer to the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

## ADMINISTRATION

NetScreen devices support several levels of administrative users. Each level has its own set of privileges. To restrict administrative access to the NetScreen device, ScreenOS 4.0.2 provides various features that the root admin can set for the root admin and for admin users at all administrative levels. The following sections describe these features and their corresponding CLI commands. (There is no WebUI support for these features.)

**Note:** *In the following sections, it is assumed that you are the root admin.*

### Root Admin

The root admin is the only level that has complete administrative privileges. The enhancements described in this section help prevent unauthorized users from logging in as the root admin and misusing these privileges.

#### Password Minimum Length

In some corporations, one person might initially configure the device as the root admin, but another person later assumes the role of root admin and manages the device. To prevent the subsequent root admin from using short passwords that are potentially easier to decode, the initial root admin can set a minimum length requirement for the root admin's password to any number from 1 to 31.

Note that you can set the minimum password length only if you are the root admin and your own password meets the minimum length requirement you are attempting to set. Otherwise, the NetScreen device displays an error message.

To specify a minimum length for the root admin's password, enter the following command:

```
set admin password restrict length number
```

## Example: Setting the Minimum Length of the Root Admin Password

In this example, you set the minimum length of the root admin's password to 8 characters:

### WebUI

**Note:** You must use the CLI to set the minimum length of the root admin's password.

### CLI

1. set admin password restrict length 8
2. save

## Console Access

You can require the root admin to log in to the NetScreen device through the console only. This restriction requires the root admin to have physical access to the device to log in, thus preventing unauthorized users from logging in remotely as the root admin. After you have set this restriction, the device denies access if anyone tries to log in as the root admin through other means, such as the WebUI, Telnet, or SCS, even if these management options are enabled on the ingress interface.

To restrict the access of the root admin to the console only, enter the following command:

```
set admin root access console
```

## Example: Restricting the Root Admin to Console Access

In this example, you restrict the root admin to log in to the NetScreen device through the console only.

### WebUI

**Note:** You must use the CLI to set this restriction.

### CLI

1. set admin root access console
2. save

## Common Criteria

The root admin can disable all internal commands. This ability is limited to the root admin only. If anyone other than the root admin tries to set this command, the NetScreen device displays an error message.

To disable all internal commands, enter the following command:

```
set common-criteria no-internal-commands
```

## Example: Disabling Internal Commands

In this example, the root admin disables internal commands.

### WebUI

**Note:** You must use the CLI to set this command.

### CLI

1. set common-criteria no-internal-commands
2. save

## Admin Users

This section describes restrictions that the root admin can set for all admin users. These restrictions apply to the root admin as well.

### Limiting Telnet Login Attempts

You can limit the number of unsuccessful login attempts allowed before the NetScreen device terminates a Telnet session. This feature minimizes a malicious user's chances of logging in to a device and protects against certain types of attacks, such as automated dictionary attacks.

You can set the allowed number of unsuccessful login attempts to any number from 1 to 255. The default is three attempts.

To set the number of unsuccessful login attempts allowed before the device closes a Telnet session, enter the following command:

```
set admin access attempts number
```

## Example: Limiting the Number of Login Attempts

In this example, you limit the number of unsuccessful login attempts allowed to 4 attempts.

### WebUI

**Note:** You must use the CLI to set this restriction.

### CLI

1. set admin access attempts 4
2. save

## Telnet Through VPN

To ensure that admin users use a secure connection when they manage the device through Telnet, you can require such users to telnet only through a VPN tunnel. After you have set this restriction, the device denies access if anyone tries to telnet without going through a VPN tunnel. To restrict Telnet access through a VPN, enter the following command:

```
set admin telnet access tunnel
```

## Example: Securing Telnet Connections through VPNs

In this example, you require that admins using Telnet connect through a VPN tunnel. After you configure the VPN tunnel between the remote admin and the NetScreen device, issue the command that sets the restriction on Telnet connections. (For more information on creating a VPN tunnel for administrative traffic originating from or destined to a NetScreen device, refer to *Volume 3: Administration* in the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

### WebUI

**Note:** You must use the CLI to set this restriction .

### CLI

1. set admin telnet access tunnel
2. save

## COUNTING STATISTICS IN THE WEBUI


NetScreen provides traffic logs so you can monitor the traffic that policies permit across the firewall. ScreenOS 4.0.2 provides the ability to count traffic on a per session basis and to log this information. The new *Bytes Transferred* column in the traffic log contains the following additional information for each session:

- The number of bytes transmitted from a source to a destination
- The number of bytes transmitted from a destination to a source

### Example: Viewing Traffic Log Details

In this example, you view the traffic log details of a policy whose ID is 3 and for which you have previously enabled counting:

#### WebUI

Policies: Click the  icon for the policy with ID number 3.

The following information appears:

Date/Time	Source Address/Port	Translated Address/Port	Destination Address/Port	Service	Duration	Bytes Sent	Bytes Received
2003-01-09 21:33:43	1.1.1.1:1046	1.1.1.1:1046	10.1.1.5:80	HTTP	1800 sec.	326452	289207

The *Bytes Sent* column of the table shows that 326452 bytes were sent from 1.1.1.1:1046 to 10.1.1.5:80. The *Bytes Received* column shows that 289207 bytes were sent from 10.1.1.5:80 to 1.1.1.1:1046.

## SCREENS FOR MGT ZONE

NetScreen devices provide a number of SCREEN options to protect a security zone. All SCREEN options, except for the SYN Attack, Block Java/ActiveX/ZIP/EXE Component, and WinNuke Attack are available to protect the MGT zone. By default, no SCREEN options are enabled for the MGT zone. This feature provides defenses against attacks targeting interfaces bound to the MGT zone.

### Example: Enabling SCREEN Options for the MGT Zone

In this example, you enable the following SCREEN options for the MGT Zone:

- Deny Ping of Death attack protection
- Deny Teardrop attack protection
- Deny IP Spoofing attack protection

#### *WebUI*

Network > Zones > Edit (for the MGT zone) > SCREEN: Enter the following settings, and then click **Apply**:

Deny Ping of Death Attack: (select)

Deny Teardrop Attack: (select)

Deny IP Spoofing Attack: (select)

#### *CLI*

1. set zone mgt screen ping-death
2. set zone mgt screen tear-drop
3. set zone mgt screen ip-spoofing
4. save



## ScreenOS 4.0.1 Modified CLI Commands

---

ScreenOS 4.0.1 introduces some enhancements to the following CLI commands:

- [dns](#) on page 86
- [flow](#) on page 87
- [ike](#) on page 89
- [log](#) on page 90
- [snmp](#) on page 91
- [vpn](#) on page 92
- [zone](#) on page 94

All new command elements in the following Syntax sections appear in **red**. For example, in the following command, “**interval number**” is new in this release:

```
set dns host schedule time_str [ interval number ]
```

The following command descriptions focus only on the new elements added in this release. For more information about these commands, refer to the *NetScreen CLI Reference Guide*.

**Description:** Use the **dns** commands to configure Domain Name Services (DNS) or to display DNS configuration information.

## Syntax

### *set*

```
set dns host schedule time_str [ interval number ]
```

### *unset*

```
unset dns host schedule
```

## Keywords and Variables

### *interval*

**interval number** Indicates a 4-, 6-, 8-, or 12-hour interval between DNS table refresh operations. The default interval is 24 hours; that is, once a day at the scheduled DNS lookup time. Use this option to refresh the DNS table more frequently.

**Example:** To set the DNS refresh operation at 6-hour intervals beginning at 12:10 AM:

```
set dns host schedule 12:10 interval 6
```

## flow

**Description:** Use the **flow** commands to adjust how the NetScreen device processes sessions, or to display the session processing parameters.

### Syntax

#### *set*

```
set flow aging
{
  early-ageout number |
  high-watermark number |
  low-watermark number
}
```

#### *unset*

```
unset flow aging
{
  early-ageout |
  high-watermark |
  low-watermark
}
```

## Keywords and Variables

### *aging*

<b>aging</b>	Directs the NetScreen device to begin aggressively aging out sessions when the number of entries in the session table exceeds the high-watermark setting, and then stop when the number of sessions falls below the low-watermark setting. When the session table is in any other state, the normal session timeout value is applied—for TCP, session timeout is 30 minutes; for HTTP, it is 5 minutes; and for UDP, it is 1 minute. During the time when the aggressive aging out process is in effect, the NetScreen device ages out sessions—beginning with the oldest sessions first—at the rate you specify.
<b>early-ageout</b> <i>number</i>	Defines the the ageout value before the NetScreen device aggressively ages out a session from its session table. The value you enter can be from 2 to 10 units, each unit representing a 10-second interval. The default early-ageout value is 2, or 20 seconds.
<b>high-watermark</b> <i>number</i>	Sets the point at which the aggressive aging out process begins. The number you enter can be from 1 to 100 and indicates a percent of the session table capacity in 1% units. The default is 100, or 100%.
<b>low-watermark</b> <i>number</i>	Sets the point at which the aggressive aging out process ends. The number you enter can be from 1 to 10 and indicates a percent of the session table capacity in 10% units. The default is 10, or 100%.

**Example:** To activate the aggressive aging-out process when the session table reaches 70% capacity and deactivate the process when it drops below 60%, and to set the aggressive ageout value at 30 seconds:

```
set flow aging low-watermark 60
set flow aging high-watermark 70
set flow aging early-ageout 3
```

**Description:** Use the **ike** commands to define the Phase 1 and Phase 2 proposals and the gateway for an AutoKey IKE (Internet Key Exchange) VPN tunnel, and to specify and display other IKE parameters.

## Syntax

### *set*

```
set ike gateway name address { ip_addr | hostname[.dom_name] } ...
```

## Keywords and Variables

### *address*

**address** Defines the remote IKE gateway address either as an IP address or as a hostname or fully-qualified domain name (FQDN), which is a hostname + domain name. Note: If you specify a hostname or FQDN that the NetScreen device cannot resolve to an IP address, the IKE gateway is classified as disabled.

**Example:** To use www.netscreen.com as the address of a remote IKE gateway named ns1, define the preshared key as 7a850wq, and specify the Phase 1 security level as compatible<sup>1</sup>:

```
set ike gateway ns1 address www.netscreen.com preshare 7a850wq sec-level compatible
```

---

1. The *compatible* security level for Phase 1 negotiations includes the following four proposals: pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, and pre-g2-des-md5.

**Description:** Use the **log** commands to display log messages, specify their destinations, and display log status.

## Syntax

*get*

```
get log
  { ... | self | traffic }
  [ ... | dst-port { port_num1-port_num2 | port_num3 } | ... ]
```

## Keywords and Variables

*dst-port*

**dst-port** Filters the output of the get log command by a range of destination port numbers or by a specific destination port number.

**Example:** To filter the get traffic log output to display only traffic destined for port 80 (that is, HTTP traffic):

```
get log traffic dst-port 80
```

## snmp

**Description:** Use the **snmp** commands to configure the NetScreen device for monitoring and management via the Simple Network Management Protocol (SNMP), and to view SNMP configuration settings.

### Syntax

#### *set*

```
set snmp host comm_name ip_addr[/mask ]
```

### Keywords and Variables

#### *mask*

*mask* Defines a SNMP community member as a subnet. Note: When you define an SNMP community member as a subnet, that member can poll the NetScreen device but it cannot receive SNMP traps. To receive SNMP traps, the community member must be a single host.

**Example:** To define the subnet 10.5.1.0/24 as a member of the SNMP community named olympia:

```
set snmp host olympia 10.5.1.0/24
```

**Description:** Use the **vpn** commands to create or remove a Virtual Private Network (VPN) tunnel, or to display current VPN tunnel parameters.

NetScreen devices support two key methods for VPNs—AutoKey IKE and Manual Key. AutoKey IKE (Internet Key Exchange) is a standard protocol that automatically regenerates encryption keys at user-defined intervals. Manual Key VPNs use predefined keys that remain unchanged until the participants change them explicitly.

## Syntax

*set*

```
set vpn name monitor [ source-interface interface [ destination-ip ip_addr ] ]  
rekey
```

## Keywords and Variables

*destination-ip*

**destination-ip** Specifies the destination IP address for the VPN monitoring feature to ping.

**Example:** To use ethernet3 as the source interface and 10.1.1.5 as the destination IP address for VPN monitoring through a VPN tunnel named tun1:

```
set vpn tun1 monitor source-interface ethernet3 destination-ip 10.1.1.5
```

## *rekey*

### **rekey**

When the key lifetime for a Phase 1 or Phase 2 security association (SA) is about to expire, the rekey option keeps the SA active even if there is no other VPN traffic except the ICMP echo requests (pings) sent by the VPN monitoring module.

**Example:** To enable the VPN monitoring feature to keep Phase 1 and Phase 2 SAs active by rekeying when the current key is about to expire for a VPN tunnel named corp:

```
set vpn corp monitor rekey
```

**Description:** Use the **zone** commands to create, remove, configure, or display a security zone.

## Syntax

### *set*

```
set zone name reassembly-for-alg
set zone name screen alarm-without-drop
set zone name screen block-component [activex | java | zip | exe ]
set zone name screen limit-session
[
  destination-ip-based [ number ] |
  source-ip-based [ number ]
]
```

## Keywords and Variables

### *reassembly-for-alg*

#### **reassembly-for-alg**

Reassembles all fragmented IP packets and TCP segments for HTTP and FTP traffic that arrives at any interface bound to the zone on which you enable this option. With this option enabled, the NetScreen device can better detect malicious URLs that an attacker has deliberately broken into packet or segment fragments. Packet and segment reassembly also improves application layer gateway (ALG) filtering by allowing the NetScreen device to examine the complete text within payloads.

**Example:** To enable IP packet and TCP segment reassembly on all interfaces bound to the Untrust zone:

```
set zone untrust reassembly-for-alg
```

### *alarm-without-drop*

#### **alarm-without-drop**

Generates an alarm when detecting an attack, but does not block the attack. This option is useful if you allow the attack to enter a segment of your network that you have previously prepared to receive it—such as a honeynet, which is essentially a decoy network with extensive monitoring capabilities.

**Example:** To enable the attack monitoring feature on the Untrust zone:

```
set zone untrust alarm-without-drop
```

### *block-component*

#### **block-component [ activex | java | zip | exe ]**

Selectively blocks HTTP traffic containing any of the following components:

- ActiveX controls
- Java applets
- .exe files
- zip files

An attacker can use any of these components to load an application on a protected host, then use the application to gain control of the host. If you enable the blocking of HTTP components without specifying which components, the NetScreen device blocks them all. Alternatively, you can configure the NetScreen device to block only specified components.

Note: If you enable ActiveX-blocking, the NetScreen device also blocks packets containing Java applets, .exe files, and .zip files because they might be contained within an ActiveX control.

**Examples:** To block ActiveX and Java applets in HTTP traffic received on interfaces bound to the Untrust zone:

```
set zone untrust block-component activex  
set zone untrust block-component java
```

To block all HTTP components in traffic received on interfaces bound to the Untrust zone:

```
set zone untrust block-component
```

## *limit-session*

### **limit-session**

Enables the limiting of sessions per second initiated from a single source IP address or directed to a single destination IP address. By default, this option limits the number of sessions per second from or to a single IP address to 128. You can define a source- or destination-based session-limit threshold between 1 and 49,999 sessions per second.

**destination-ip-based** [ *number* ] Limits the number of sessions destined for any single IP address to the value specified.

**Example:** To limit the number of sessions from any host in the Trust and Untrust zones to any single IP address to 80 sessions per second:

```
set zone trust screen limit-session destination-ip-based 80
set zone trust screen limit-session
set zone untrust screen limit-session destination-ip-based 80
set zone untrust screen limit-session
```

## ScreenOS 4.0.2 Modified CLI Commands

---

ScreenOS 4.0.2 introduces some enhancements to the following CLI command:

- [admin](#) on page 98
- [common-criteria](#) on page 103

All new command elements in the following Syntax sections appear in **red**. For example, in the following command, "**access attempts number**" is new in this release:

```
set admin
{
  access attempts number |
  auth
```

The following command descriptions focus only on the new elements added in this release. For more information about the command, refer to the *NetScreen CLI Reference Guide*.

**Description:** Use the **admin** commands to configure or display administrative parameters for the NetScreen device.

## Syntax

### *clear*

```
clear [ cluster ] admin user { cache | login }
```

### *get*

```
get admin  
  [  
    auth [ banner | settings ] |  
    current-user |  
    manager-ip |  
    scs all |  
    user [ cache | login ]  
  ]
```

### *set*

```
set admin  
  {  
    access attempts number |  
    auth  
      {  
        banner { console | telnet } login string |  
        server name_str |  
        timeout number |  
      } |  
  }
```

```
device-reset |
format { dos | unix } |
hw-reset |
mail
  {
  alert |
  mail-addr1 ip_addr | mail-addr2 ip_addr |
  server-name { ip_addr | name_str } |
  traffic-log
  } |
manager-ip ip_addr [ mask ] |
name name_str |
password pswd_str |
password restrict length number |
port port_num |
privilege { get-external | read-write } |
root access console |
scs
  {
  password { disable | enable } username name_str |
  port port_num
  } |
telnet
  {
  port port_num
  access tunnel
  } |
user name_str password pswd_str [ privilege { all | read-only } ]
}
```

## *unset*

```
unset admin
{
  access attempts |
  auth
  {
    banner { console | telnet } login |
    server |
    timeout |
  } |
  device-reset |
  format |
  hw-reset |
  mail
  { alert | mail-addr1 | mail-addr2 | server-name | traffic-log } |
  manager-ip { ip_addr | all } |
  name |
  password [ restrict length ] |
  port |
  root access console
  scs [ port ] |
  telnet { port | access tunnel } |
  user name_str
}
```

## Keywords and Variables

### *access attempts*

```
set admin access attempts number  
unset admin access attempts
```

**access attempts** Specifies the number (1 - 255) of unsuccessful login attempts allowed before the device closes the Telnet connection. The default is 3.

**Example:** The following command sets the number of allowed unsuccessful login attempts to 5:

```
set admin access attempts 5
```

### *access tunnel*

```
set admin telnet access tunnel  
unset admin telnet access tunnel
```

**access tunnel** Requires a VPN tunnel for admins who log in through a Telnet connection.

### *restrict length*

```
set admin password restrict length number  
unset admin password restrict length
```

**restrict length** Sets the minimum password length of the root admin. The password length can be any number from 1 to 255.

**Example:** The following command sets the minimum password length of the root admin to 8:

```
set admin password restrict length 8
```

### *root access console*

```
set admin root access console  
unset admin root access console
```

**root access console** Restricts the root admin to logging in to the device through the console only.

## Defaults

The default for access attempts is 3.

## common-criteria

**Description:** Use the **common-criteria** command to disable all internal commands. Only the root admin can set this command. If someone other than the root admin tries to set this command, the NetScreen device displays an error message.

### Syntax

*set*

```
set common-criteria
{
no-internal-commands
}
```

*unset*

```
unset common-criteria no-internal-commands
```

### Keywords and Variables

*no-internal-commands*

```
set common-criteria no-internal-commands
unset common-criteria no-internal-commands
```

**no internal commands**     Disables all internal commands.



# ScreenOS 4.0.1 New and Modified Messages

---

This chapter introduces all the new NetScreen messages for this release. Each message is presented, its meaning explained, and—where appropriate—an administrative action recommended. The messages are grouped by message type, and then within that type by severity level, from the most severe to the least.

- “Authentication” on page 106
- “DNS” on page 107
- “Firewall” on page 108
- “IKE” on page 111
- “Sessions” on page 113
- “VPN” on page 114
- “Zones” on page 115

For a complete list of NetScreen messages, refer to the *NetScreen Messages Reference Guide*.

## AUTHENTICATION

The following messages relate to user authentication.

### Information (00544)

<b>Message</b>	User <name> [ of group <grp_name> ] at <ip_addr> has been challenged by the RADIUS server at <ip_addr>.
<b>Meaning</b>	The named external RADIUS authentication server has proposed a challenge to the authentication user at the specified IP address. If the user is a member of a user group, the group name is also included in the message.
<b>Action</b>	No recommended action

## DNS

The following messages concern Domain Name System (DNS) settings.

### Notification (00004)

- Message** DNS lookup time has been changed to start at <hour>:<minute> with an interval of <number> hours.
- Meaning** An administrator has set the daily start time and subsequent time interval for automatically refreshing the DNS table in the NetScreen device.
- Action** No recommended action

## FIREWALL

The following messages concern firewall settings and reports of attacks.

**Note:** The message text for all firewall alarms detecting an attack has been modified in ScreenOS 4.0.1 to the following:

<attack\_name> has been detected! From <ip\_addr1>:<port\_num1> to <ip\_addr2>:<port\_num2>, using protocol { TCP | UDP | <number> }, and arriving at interface <interface> in zone <zone>. [ The attack occurred <number> { time | times }. ]

### Critical (00033)

- Message** { Source | Destination } threshold has been exceeded! From <ip\_addr1>:<port\_num1> to <ip\_addr2>:<port\_num2>, using protocol { TCP | UDP | <number> }, and arriving at interface <interface> in zone <zone>. [ The attack occurred <number> { time | times }. ]
- Meaning** The NetScreen device has detected and blocked an attempt to initiate a session in excess of the defined session limit from the same IP address or to the same IP address. The packet originated from and was destined for the specified IP addresses and port numbers. The packet used the specified protocol and arrived at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets in excess of the session threshold.
- Action** No recommended action

---

### Critical (00400)

- Message** { ActiveX control | JAVA applet | EXE file | ZIP file } has been detected! From <ip\_addr1>:<port\_num1> to <ip\_addr2>:<port\_num2>, using protocol { TCP | UDP | <number> }, and arriving at interface <interface> in zone <zone>. [ The attack occurred <number> { time | times }. ]
- Meaning** The NetScreen device has detected and blocked HTTP traffic containing the specified component (ActiveX control or Java applet) or file type (.exe or .zip files) sent from the specified source IP address and port number and destined to the specified destination IP address and port number. The packet arrived at the named interface
- Action** No recommended action

---

### Notification (00005)

- Message** A { destination-based | source-based } session-limit threshold has been set at <number> in zone <zone\_name>.
- Meaning** An administrator has set a limit to the the number of sessions per second from the same IP address or to the same IP address that the NetScreen device accepts on any interface bound to the specified security zone. When the session limiting SCREEN option is enabled and the number of sessions per second from a single IP address reaches the defined threshold, the NetScreen device drops further sessions from that source for the remainder of that second. Similarly, when the session limiting SCREEN option is enabled and the number of sessions per second to a single IP address reaches the defined threshold, the NetScreen device drops further sessions to that destination for the remainder of that second.
- Action** No recommended action

- Message** { Destination-based | Source-based } session limiting has been { enabled | disabled } in zone <zone\_name>.
- Meaning** An administrator has enabled or disabled source-based or destination-based session limiting in the specified security zone.
- Action** No recommended action
- 
- Message** HTTP component blocking of { ActiveX controls | Java applets | .exe files | .zip files } has been { enabled | disabled } in zone <zone\_name>.
- Meaning** An administrator has enabled or disabled the blocking of packets containing the specified component (ActiveX or Java) or file type (.exe or .zip files) in HTTP traffic arriving at any interface bound to the specified security zone.
- Action** No recommended action
- 
- Message** Alarm-without-drop screen option has been { enabled | disabled } for zone <zone\_name>.
- Meaning** An administrator has enabled or disabled the alarm-without-drop SCREEN option, which instructs the NetScreen device to notify an admin of a detected attack but does not take action to block it.
- Action** If this SCREEN option has been enabled, ensure that it is the device behavior you want. NetScreen recommends extreme caution regarding this option and recommends its use only in conjunction with intrusion detection products such as the NetScreen-IDP 100, and network monitoring devices such as sniffers, honeypots, and honeynets.

## IKE

The following messages relate to the Internet Key Exchange (IKE) protocol, one of the three main components of IPSec—the other two are the Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols. IKE provides a secure means for the distribution and maintenance of cryptographic keys and the negotiation of the parameters constituting a secure communications channel.

### Information (00536)

- |                |   |
|----------------|---|
| <b>Message</b> | IKE gateway <name> has been enabled. The peer address <hostname[.dom_name]> has been resolved to <ip_addr>.   |
| <b>Meaning</b> | When an administrator configured the named IKE gateway with a host name or a fully-qualified domain name (FQDN = host name + domain name), the NetScreen device was unable to resolve the name to an IP address. As a result, the NetScreen device has temporarily disabled that IKE gateway.   |
| <b>Action</b>  | Check that the host name or FQDN is correct. Ensure that the NetScreen device is properly configured for DNS service. Also check if the NetScreen device can connect to the DNS server and that the DNS server is responsive to DNS queries.  |
| <b>Message</b> | IKE gateway< name> has been disabled because the peer IP address <ip_addr> is already in use by another IKE gateway on interface <interface>.   |
| <b>Meaning</b> | When an administrator configured the named IKE gateway with a host name or a fully-qualified domain name (FQDN = host name + domain name), the NetScreen device successfully resolved the name to an IP address but then discovered that another IKE gateway configuration has already used the same IP address. As a result, the NetScreen device has temporarily disabled that IKE gateway. |
| <b>Action</b>  | Check that the host name or FQDN is correct. Check the IKE gateway configurations.  |

- Message** IKE gateway <name> has been disabled. The peer address< hostname[.dom\_name]> cannot be resolved to an IP address.
- Meaning** When an administrator configured the named IKE gateway with a host name or a fully-qualified domain name (FQDN = host name + domain name), the NetScreen device was unable to resolve the name to an IP address. As a result, the NetScreen device has temporarily disabled that IKE gateway.
- Action** Check that the host name or FQDN is correct. Ensure that the NetScreen device is properly configured for DNS service. Also check if the NetScreen device can connect to the DNS server and that the DNS server is responsive to DNS queries.

## SESSIONS

The following messages pertain to sessions, and in particular to the aggressive aging out of sessions during periods of high-volume traffic.

### Notification (00040)

- Message** { High | Low } watermark for early aging has been changed { to the default (100) | from <number1> to <number2> }.
- Meaning** An administrator has returned the high or low watermark setting to its default, which is 100 percent of the session table capacity, or from one setting to another. The NetScreen device begins aggressively aging out sessions when the number of entries in the session table exceeds the high-watermark setting, and then stops when the number of sessions falls below the low-watermark setting.
- Action** No recommended action
- 
- Message** Ageout value for early aging has been changed { to default (2) | from <number1> to <number2> }.
- Meaning** An administrator has returned the aggressive ageout value to its default, which is 2 units (or 20 seconds), or from one setting to another. The aggressive ageout value indicates how much time to subtract from the normal session ageout period when the aggressive aging mechanism is in effect.
- Action** No recommended action

## VPN

The following messages relate to IPSec virtual private network (VPN) tunnels, and VPN-related technologies.

### Notification (00017)

<b>Message</b>	VPN monitoring for VPN <vpn_name> has been enabled. Src IF <interface_name>, dst IP <ip_addr>, with rekeying { enabled   disabled }.
<b>Meaning</b>	An administrator has enabled VPN monitoring on the named VPN tunnel and instructed the NetScreen device to send ICMP echo requests from the indicated source interface to the specified destination IP address. If the rekey option is enabled and a key lifetime for a Phase 1 or Phase 2 security association (SA) is about to expire, the VPN monitoring activity keeps the SA active even if there is no other VPN traffic. If the rekey option is not enabled, an expiring key is renewed only if user-generated traffic is active in the VPN tunnel.
<b>Action</b>	No recommended action

---

### Information (00536)

<b>Message</b>	VPN monitoring for VPN <vpn_name> has deactivated the SA with ID <number>.
<b>Meaning</b>	The VPN monitoring feature has deactivated the specified security association (SA) for the named VPN tunnel. When the VPN monitoring option determines that a VPN tunnel link is down and the rekey option is enabled, the NetScreen device clears any active SAs associated with that tunnel.
<b>Action</b>	Investigate the network status and check the VPN tunnel configuration.

## ZONES

The following messages relate to security zones.

### Notification (00037)

<b>Message</b>	IP/TCP reassembly for ALG was { enabled   disabled } on zone <zone_name>.
<b>Meaning</b>	An administrator has enabled or disabled the IP packet reassembly and TCP stream reassembly for FTP and HTTP traffic arriving on any interface bound to the specified zone. Reassembling IP packets and TCP segments improves application layer gateway (ALG) filtering by allowing the NetScreen device to examine the complete text within payloads.
<b>Action</b>	No recommended action



## ScreenOS 4.0.2 New and Modified Messages

---

This chapter introduces all the new NetScreen messages for this release. Each message is presented, its meaning explained, and—where appropriate—an administrative action recommended. The messages are grouped by message type, and then within that type by severity level, from the most severe to the least.

- [“Admin” on page 118](#)

For a complete list of NetScreen messages, refer to the *NetScreen Messages Reference Guide*.

## ADMIN

The following messages relate to the administration of the NetScreen device.

### Notification (00002)

**Message** Root admin password restriction of minimum 8 characters has been { enabled | disabled } by admin <name> { from host <ipaddr> | from Console }

**Meaning** The named root admin has either enabled or disabled the feature that sets the root admin minimum password length to 8 characters.

**Action** Set the root admin password to no less than 8 characters.

**Message** Failed login attempts from Telnet before administrative session disconnects has been changed from <number> to <number> by admin <name> { from host <ipaddr> | from Console }

**Meaning** The named admin changed the number of unsuccessful login attempts allowed before the NetScreen device closes the Telnet connection.

**Action** No recommended action

**Message** Root admin access restriction through console only has been { enabled | disabled } by admin <name> { from host <ipaddr> | from Console }

**Meaning** The named root admin has either enabled or disabled the feature that restricts the root admin to logging in to the device through the console only.

**Action** No recommended action

**Message** Admin access restriction of telnet administration through tunnel only has been { enabled| disabled } by admin <name> { from host <ipaddr> | from Console }

**Meaning** The named admin has either enabled or disabled the feature that restricts telnet access through a VPN tunnel.

**Action** No recommended action

