Network Configuration Example

Deploying the SRX Series for Enterprise Security

Release
NCE0139

Modified: 2018-02-26

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Deploying the SRX Series for Enterprise Security
NCE0139

Table of Contents

Chapter 1 Deploying the SRX Series for Enterprise Security 5

About This Network Configuration Example 5
Introduction to the SRX Series 5
Security Threats and What the SRX Series Offers 5
Next-Generation Security Features 7
Example: Configuring a Next-Generation Firewall on SRX Series Devices 9

CHAPTER 1

Deploying the SRX Series for Enterprise Security

- About This Network Configuration Example on page 5
- Introduction to the SRX Series on page 5
- Security Threats and What the SRX Series Offers on page 5
- Next-Generation Security Features on page 7
- Example: Configuring a Next-Generation Firewall on SRX Series Devices on page 9

About This Network Configuration Example

This document provides a step-by-step example for configuring next-generation security features on an SRX Series device in an enterprise network. This document is intended for security and IT engineers, as well as network architects.

Introduction to the SRX Series

Juniper Networks® SRX Series Services Gateways are high-performance network security solutions for enterprises and service providers that deliver security, routing, and networking capabilities. Specifically for security, the SRX Series offers a next-generation firewall, application visibility and control, IPS, as well as other security services. SRX Series devices provide a complete security solution to protect and control your business assets.

Related Documentation

- Security Threats and What the SRX Series Offers on page 5
- Next-Generation Security Features on page 7
- Example: Configuring a Next-Generation Firewall on SRX Series Devices on page 9

Security Threats and What the SRX Series Offers

The network security landscape has changed dramatically as networks become more complex and dynamic. New challenges are emerging from web-based and social networking applications, sophisticated cyber attacks leveraging technology and social engineering, increased use of Web applications, internal attacks, and ubiquitous Internet access. The following list examines some of these issues:

- Denial-of-service (DoS) attacks—Any attacks aimed at hampering a service can fall into this category. This sort of attacker tries to exploit a known weakness in software, networking practices, and operating systems to crash a system or subsystem.
- Improper use of bandwidth—Random access to noncritical applications such as entertainment, chatting, video, and gaming consume a large quantity of bandwidth and results in poor quality of work, waste of network resources, and inefficiency and poor performance of critical applications.
- Unauthorized user access—Unauthorized users could gain access to the server, to a resource, and to sensitive information and misuse the asset or steal proprietary information.
- Internal attacks—This type of attack originates from inside the local network. Unlike external attacks, the intruder is someone who has been entrusted with authorized access to the network. It is easier for legitimate network users to steal, modify, or destroy data or to plant malicious code on the network.
- Session hijacking—IP session hijacking is an attack whereby a user's session is taken over, being in the control of the attacker.
- Inadvertent downloads of viruses, malware, or trojans—Activities such as surfing the Web, video or file-sharing websites, playing games, or using social media websites might result in inadvertent download of malware and virus threats.
- Sophisticated viruses—Threats are evolving with increasing volume and sophistication. The most prevalent threat types include spyware, phishing, instant messaging, peer-to-peer file sharing, streaming media, social media, and blended network attacks.
- Malware driven by downloads—This pertains to downloads that install an unknown or counterfeit executable program, often a computer virus, spyware, malware, or crimeware, while visiting a website or viewing an e-mail message.

Juniper Networks SRX Series devices provide a security solution with a complete set of tools to achieve end-to-end security to protect critical network resources that reside on the network. Security solutions include stateful firewall, intrusion prevention system (IPS), complete set of integrated unified threat management (UTM) security features, AppSecure, and security intelligence.

The remainder of this document describes how to configure the security features on SRX Series devices.

Related Documentation

- Introduction to the SRX Series on page 5
- Next-Generation Security Features on page 7
- Example: Configuring a Next-Generation Firewall on SRX Series Devices on page 9

Next-Generation Security Features

SRX Series Services Gateways support next-generation firewall protection with application-aware security services, intrusion detection and prevention (IDP), a role-based user firewall, and unified threat management (UTM) to achieve end-to-end security.

Table 1 on page 7 describes the security features and their intended uses.

Table 1: Next-Generation Security Features

Security Feature	Intended Use
Firewall User Authentication	Firewall user authentication provides another layer of protection in the network by restricting or permitting users individually or in groups. Firewall user authentication protects the network by controlling who and what can access to the network. It minimizes policy management complexity with user-based and role-based firewall controls. For details, see the Junos OS User Authentication Guide for Security Devices.
Intrusion Prevention	Intrusion detection and prevention (IDP) features enable you to selectively enforce various attack detection and prevention techniques on network traffic passing through an IDP-enabled device. IDP provides protection against network-based exploit attacks aimed at application vulnerabilities. For details, see the Junos OS Intrusion Detection and Prevention (IDP) Feature Guide for Security Devices.

Table 1: Next-Generation Security Features *(continued)*

Security Feature	Intended Use
AppSecure	AppSecure is a suite of application security capabilities that identifies applications for greater visibility. It utilizes advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network. AppSecure detects application behaviors and weaknesses that prevent application-borne security threats that are difficult to detect and stop. The following AppSecure service modules can be configured to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the application ID of the traffic: • AppID–Provides application visibility and control over each application that is allowed to communicate on the network. • AppTrack–Simplifies application visibility and control. • AppFW–Stops users from visiting inappropriate web sites or inadvertently downloading spyware and other malicious applications from known sites. • AppQoS–Prioritizes traffic based on application type and limits the amount of bandwidth an application can consume. • SSL Proxy- SSL proxies provide encryption and decryption by residing between the server and the client. With the implementation of SSL proxy, AppID can identify applications encrypted in SSL. SSL proxy can be enabled as an application service in a regular firewall policy rule. IDP, application firewall, and application tracking services can use the decrypted content from SSL proxy. For details, see the Junos OS AppSecure Services Feature Guide for Security Devices.
UTM	UTM enables a business to protect itself from spam, viruses, worms, spyware, trojans, and malware. With UTM, you can implement a comprehensive set of security features that include: • Antispam–This protects against malware at the desktop, gateway, and server levels. • Web filtering–Web filtering stop users from visiting inappropriate websites or inadvertently downloading spyware and other malicious applications from known sites and ensures productivity and policy compliance. • Antivirus–This prevents spam messages and malicious content. • Content filtering–Content filtering provides basic data loss prevention functionality. For details, see the Junos OS UTM Feature Guide for Security Devices.

Related Documentation

- Introduction to the SRX Series on page 5
- Security Threats and What the SRX Series Offers on page 5
- Example: Configuring a Next-Generation Firewall on SRX Series Devices on page 9

Example: Configuring a Next-Generation Firewall on SRX Series Devices

This example provides step-by-step procedures required for configuring a next-generation firewall for a medium-size enterprise campus.

- Hardware and Software Requirements on page 9
- Overview and Topology on page 9
- Configuring Address Objects, Security Zones, and Security Policies on page 12
- Configuring AppSecure Modules on page 16
- Configuring IDP on page 23
- Configuring Unified Threat Management on page 26
- Configuring Screens on page 31
- Configuring Firewall User Authentication on page 33
- Configuring SSL Proxy on page 35
- Verification on page 37

Hardware and Software Requirements

The following SRX Series devices running Junos® OS Release 12.1X47 or later are used in this example:

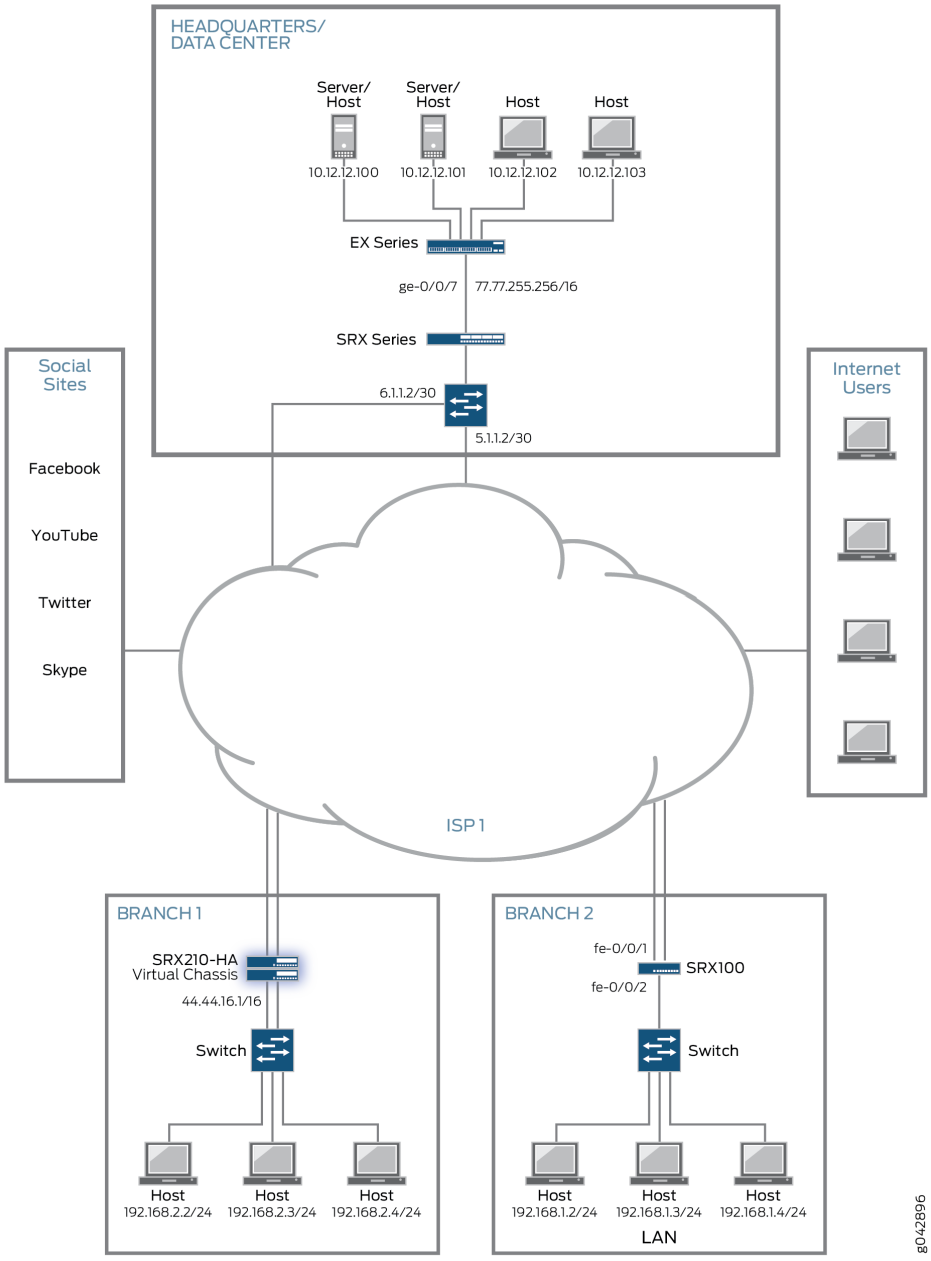
- Branch-1: One Juniper Networks SRX Series Services Gateway (SRX210) operating in Layer 2 transparent mode
- Branch-2: One Juniper Networks SRX Series Services Gateway (SRX210) operating in chassis cluster mode
- Data Center and Headquarters: Juniper Networks SRX Series Services Gateways (SRX240 and SRX550)

Before you begin, complete the basic configuration for your SRX Series device. See the Getting Started Guide for Branch SRX Series.

Overview and Topology

Figure 1 on page 10 shows the basic topology used in the midsize enterprise campus solution. This topology was chosen to provide a general and flexible example that can be modified to apply to different enterprise vertical markets and physical facilities.

Figure 1: Enterprise Campus Solution Topology



In this topology, the following three physical locations are defined:

- Branch-1: Low to medium-density location that is geographically separate from the location of the headquarters (HQ) and the other branch.
  - The SRX Series device is placed between the internal core switch and the Internet edge router.

    - Each user will be authenticated by Firewall User Authentication (integrated user firewall authentication).

- Branch-2: Low to medium-density location that is geographically separate from HQ and the other branch.
    - The external edge router is in chassis cluster mode with integrated firewall configured.
    - Users from each division will be authenticated by Unified Access Controller (UAC) with specific roles to secure the network and to ensure that only authenticated users can access the protected host in the data center.
- Headquarters/Data Center: High-density location that serves as the campus network core.
    - The data center is provided with chassis redundancy along with ISP. Two-gigabit interfaces are used as aggregated interfaces for configuring the RETH interface.
    - The data center hosts some real-time servers such as FTP, HTTP, MySQL, Syslog Server/STRM, and so on in the DMZ zone.
    - Users need to access data center servers through dynamic VPN, and some other users need to be authenticated by UAC (contacting IC series devices over SSL). For more information on IC Series, see IC Series.

To illustrate a common configuration scenario, the following design assumptions are made for all three locations (Branch-1, Branch-2, and data center):

- Site-to-site IPsec tunnel is configured between the branches and DC/HQ.
- All three locations have dual links to two different ISPs to provide redundancy.

The SRX Series device is responsible for identifying and taking accurate action for the traffic flowing between:

- Individual branches to the Internet
- Individual branches to a HQ/data center
- Between the branches (Branch-1 and Branch-2)

To configure the next-generation firewall:

NOTE: This example shows a minimal configuration involving only a few users and selected features, and applications.

1. Configure address objects.

   An address book is a collection of addresses and address sets. Address books are referenced in security policies. Address book entries include addresses of hosts and subnets whose traffic is either allowed, blocked, encrypted, or user-authenticated.

2. Configure security policies to enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall.

   A security policy controls the traffic flow from one zone to another zone by defining the kinds of traffic permitted from specified IP sources to specified IP destinations.

   Each user has following security policies created for the following requirements:

   - For accessing the servers in the data center (e-mail servers, FTP servers, and HTTP servers)
   - For accessing the Internet (multiple social sites, P2P applications, and other standard applications)

3. Identify the traffic at different network layers using AppID.

   Once the application is determined, apply AppSecure service modules to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the application ID of the traffic.

4. Enable IDP services and activate the predefined Recommended policy as the active policy.

5. Configure UTM to provide security features on the device to protect against multiple threat types.

6. Configure Screen to protect from DDOS attack.

   Configure Screen options to protect against internal and external attacks.

7. Configure the integrated user firewall authentication on devices for domain and non-domain users to provide access to the Internet through an SRX Series device.

8. Configure SSL proxy for secure transmission of data by using the encryption technology.

Configuring Address Objects, Security Zones, and Security Policies

A security policy controls the traffic flow from one zone to another zone by defining the kinds of traffic permitted from specified IP sources to specified IP destinations.

As a first step, set up a new zone and add three servers to that zone. Then provide communication between a host (PC) in the trust zone (in the branch office) to the servers

in the newly created zone (HQ). Then create an interzone security policy to allow traffic between the two zones.

Table 2 on page 13 provides specific configuration parameters used in creating address objects.

Table 2: Address Book Configuration Parameters

Host	IP Address	Address Book	Zones
Branch-1			
branch-1-user-1	192.168.2.2/24	address-book-branch-1-users	Branch1-Zone
branch-1-user-2	192.168.2.3/24		
branch-1-user-3	192.168.2.4/24		
Branch-2			
branch-2-user-1	192.168.1.2/24	address-book-branch-2-users	Branch2-Zone
branch-2-user-2	192.168.1.3/24		
branch-2-user-3	192.168.1.4/24		

Table 3 on page 13 provides specific configuration parameters used in creating security policies.

Table 3: Security Policy Configuration Parameters

Location	Purpose	Policy Name	From Zone	To Zone
Branch-1	Access the servers in the HQ (e-mail servers, FTP servers and HTTP servers, and so on).	Branch1-policy	Branch1-Zone	HQ-Zone
	Access the Internet.	permit-traffic-branch-1-to-internet	Branch1-Zone	untrust
Branch-2	Access the servers in the HQ (e-mail servers, FTP servers and HTTP servers, and so on).	Branch2-policy	Branch2-Zone	HQ-Zone
	Access the Internet.	permit-traffic-branch-2-to-internet	Branch2-Zone	untrust

For more information, see the Security Building Blocks Feature Guide.

- Configuring Security Zone for Headquarters on page 14
- Configuring Security Zones, Address Objects, and Security Policies on Branch-1 on page 14
- Configuring Security Zones, Address Objects, and Security Policies on Branch-2 on page 15

Configuring Security Zone for Headquarters

Step-by-Step Procedure

To configure security zones for Headquarters:

1. Configure a security zone **HQ-Zone** and configure it to support inbound traffic for all system services.

```
[edit]
user@host-1# set security zones security-zone HQ-Zone host-inbound-traffic
  system-services all
user@host-1# set security zones security-zone HQ-Zone host-inbound-traffic
  protocols all
user@host-1# set security zones security-zone HQ-Zone interfaces ge-0/0/2.0
```

2. Enable AppTrack for the security zone.

```
[edit]
user@host-1# set security zones security-zone HQ-Zone application-tracking
```

Configuring Security Zones, Address Objects, and Security Policies on Branch-1

Step-by-Step Procedure

To configure security zones and policies for Branch-1 users:

1. Configure a security zone **Branch1-Zone** and configure it to support inbound traffic for all system services.

```
[edit]
user@host-1# set security zones security-zone Branch1-Zone host-inbound-traffic
  system-services all
user@host-1# set security zones security-zone Branch1-Zone host-inbound-traffic
  protocols all
user@host-1# set security zones security-zone Branch1-Zone interfaces ge-0/0/1.0
user@host-1# set security zones security-zone Branch1-Zone application-tracking
```

2. Create an address book, define addresses in it, and attach it to a security zone.

```
[edit]
user@host-1# set security address-book address-book-branch-1-users address
  user-1 192.168.2.2
user@host-1# set security address-book address-book-branch-1-users address
  user-2 192.168.2.3
user@host-1# set security address-book address-book-branch-1-users address
  user-3 192.168.2.4
user@host-1# set security address-book address-book-branch-1-users attach zone
  Branch1-Zone
```

3. Configure a specific security policy to allow traffic from a host in the **Branch1-Zone** zone to a server in the **HQ-Zone** zone.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match source-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match application any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy then log session-init
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy then log session-close
```

Configuring Security Zones, Address Objects, and Security Policies on Branch-2

Step-by-Step Procedure

To configure security zones and policies for Branch-2 users:

1. Configure a security zone **Branch2-Zone** and configure it to support inbound traffic for all system services.

```
[edit]
user@host-2# set security zones security-zone Branch2-Zone host-inbound-traffic
  system-services all
user@host-2# set security zones security-zone Branch2-Zone host-inbound-traffic
  protocols all
user@host-2# set security zones security-zone Branch2-Zone interfaces ge-0/0/1.0
user@host-2# set security zones security-zone Branch2-Zone application-tracking
```

2. Create an address book, define addresses in it, and attach it to a security zone.

```
[edit]
user@host-2# set security address-book address-book-branch-2-users address
  user-1 192.168.1.2
user@host-2# set security address-book address-book-branch-2-users address
  user-2 192.168.2.3
user@host-2# set security address-book address-book-branch-2-users address
  user-3 192.168.3.2
user@host-2# set security address-book address-book-branch-2-users attach zone
  Branch2-Zone
```

3. Configure a specific security policy to allow traffic from a host in the **Branch2-Zone** zone to a server in the **HQ-Zone** zone.

```
[edit]
user@host-2# set security policies from-zone Branch2-Zone to-zone HQ-Zone policy
  Branch2-policy match source-address any
user@host-2# set security policies from-zone Branch2-Zone to-zone HQ-Zone policy
  Branch2-policy match destination-address any
user@host-2# set security policies from-zone Branch2-Zone to-zone HQ-Zone policy
  Branch2-policy match application any
user@host-2# set security policies from-zone Branch2-Zone to-zone HQ-Zone policy
  Branch2-policy then log session-init
```

```
user@host-2# set security policies from-zone Branch2-Zone to-zone HQ-Zone policy
    Branch2-policy then log session-close
```

Configuring AppSecure Modules

Configure application identification to recognize traffic at different network layers using characteristics other than port number. Once the application is determined, configure application tracking, application firewall, and application quality of service to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the application ID of the traffic.

For more information, see the AppSecure Services Feature Guide for Security Devices.

In this procedure, you perform the following tasks:

- Download, install, and enable application identification.
- Configure Apptrack and enable it in the zone “Branch1-Zone”. The first log message is to be generated when the session starts, and update messages should be sent every 4 minutes after that. A final message should be sent at session end.
- Add the remote syslog device configuration to receive AppTrack log messages in sd-syslog format.
- Define application firewall rulesets. Permit or deny selected traffic from the untrust zone to the trust zone, based on the application firewall rule sets defined with the rules matching the dynamic applications. Here, you are defining the rules to perform following tasks:
  - Allow access to FTP, HTTP, POP3, IMAP, and SMTP.
  - Block certain application traffic such as Yahoo and Facebook and other social networking sites.
- Implement AppQoS to classify the incoming packets based on the various protocols and further prioritize and rate limit the packets.

NOTE: **The procedure to configure AppSecure modules is same for both branches. The following examples show configuration steps on Branch-1 only.**

The following procedures show how to configure AppSecure modules on Branch-1. You can use the same procedure for other branches.

- Installing the Application Identification License on page 17
- Installing the Application Signature Package on page 17
- Configuring AppTrack for Application Visibility and Control on page 19
- Configuring Application Firewall Rule Sets for Application Enforcement on page 20
- Configuring AppQoS to Prioritize Marking and Rate Limiting of Application Traffic on page 21

Installing the Application Identification License

Step-by-Step Procedure

You can install the license on the SRX Series device using either the automatic method or manual method as follows:

1. Install your license on the device.

   To install or update your license automatically, your device must be connected to the Internet.

   - Update the license automatically on the device.

     [edit]
     user@host-1> **request system license update**

     ```
     Trying to update license keys from https://ae1.juniper.net, use 'show
     system license' to check status.
     ```

   - Install the license manually on the device.

     user@host-1> **request system license add terminal**

     ```
     [Type ^D at a new line to end input,
      enter blank line between each license key]
     ```

     Paste the license key and press Enter to continue.

2. Verify that the license is installed on your device.

   Use the **show system license** command to view license usage, as shown in the following example:

   ```
   License usage:
                                  Licenses     Licenses    Licenses    Expiry

     Feature name                       used    installed      needed
     idp-sig                               0            1           0
   2015-12-31 16:00:00 PST
     appid-sig                             0            1           0
   2015-12-31 16:00:00 PST
     full-cp-key                           1            1           0
   permanent
     logical-system                        1           76           0
   permanent

   Licenses installed:
   ```

   The output sample is truncated to display only license usage details.

Installing the Application Signature Package

Step-by-Step Procedure

To install the application signature package:

1. Download the application package.

   user@host-1> **request services application-identification download**

```
Please use command "request services application-identification download
status" to check status
```

The download retrieves the application package from the Juniper Networks security website https://signatures.juniper.net/cgi-bin/index.cgi.

You can download and install application signatures through intrusion detection and prevention (IDP) security packages using the **request security idp security-package download** command.

2. Check the download status.

   user@host-1> **request services application-identification download status**

```
Application package 2345 is downloaded successfully
```

NOTE: You can also use the system log to view the result of the download.

3. Install the application package.

   user@host-1> **request services application-identification install**

```
Please use command "request services application-identification install
status" to check status and use command "request services
application-identification proto-bundle-status" to check protocol bundle
status
```

The application package is installed in the application signature database on the device.

4. Check the installation status of the application package.

   user@host-1> **request services application-identification install status**

```
Install application package 2345 succeed
```

5. After successful download and installation of the application package, use the following commands to view the predefined application signature package content:

   - View the current version of the application package:

     user@host-1> **show services application-identification version**

```
Application package version: 2345
```

   - View the current status of the application package:

     user@host-1> **show services application-identification status**

```
pic: 0/0
```

```
Application Identification
 Status                            Enabled
 Sessions under app detection      0
 Engine Version                    4.18.2-24.006 (build date Mar  3 2015)

 Max TCP session packet memory     30000
 Force packet plugin               Disabled
 Force stream plugin               Disabled
 Statistics collection interval    1 (in minutes)

Application System Cache
 Status                            Enabled
 Negative cache status             Disabled
 Max Number of entries in cache    131072
 Cache timeout                     3600 (in seconds)

Protocol Bundle
 Download Server
https://devdb.secteam.juniper.net/xmlexport.cgi
 AutoUpdate                        Disabled
Slot 1:
 Application package version       433
 Status                            Active
 Version                          1.150.0-26.005 (build date Mar 30 2015)

 Sessions                          0
Slot 2
 Status                            Not Applicable
```

Configuring AppTrack for Application Visibility and Control

Step-by-Step Procedure

To configure AppTrack:

1. Add the remote syslog device configuration to receive Apptrack messages in sd-syslog format.

   ```
   [edit]
   user@host-1# set security log mode stream
   user@host-1# set security log format sd-syslog
   user@host-1# set security log source-address 5.0.0.254
   user@host-1# set security log stream app-track-logs host 5.0.0.1
   ```

2. Enable AppTrack for the security zone Branch1-Zone.

   ```
   [edit]
   user@host-1# set security zones security-zone Branch1-Zone application-tracking
   ```

3. (Optional) Generate update messages every 4 minutes.

   ```
   [edit]
   user@host-1# set security application-tracking session-update-interval 4
   ```

4. (Optional) Generate the first message when the session starts.

   ```
   [edit]
   ```

```
user@host-1# set security application-tracking first-update
```

Once the first message has been generated, an update message is generated each time the session update interval is reached.

Configuring Application Firewall Rule Sets for Application Enforcement

Step-by-Step Procedure

To configure the security policy with application firewall rule sets that permit or deny traffic from different dynamic applications:

1. Create a white list to permit certain applications.

```
[edit]
user@host-1# set security application-firewall rule-sets phase1 rule 1 match
  dynamic-application junos:HTTP
user@host-1# set security application-firewall rule-sets phase1 rule 1 then permit
user@host-1# set security application-firewall rule-sets phase1 rule 2 match
  dynamic-application SNI
user@host-1# set security application-firewall rule-sets phase1 rule 2 then permit
user@host-1# set security application-firewall rule-sets phase1 rule 3 match
  dynamic-application junos:TELNET
user@host-1# set security application-firewall rule-sets phase1 rule 3 then permit
user@host-1# set security application-firewall rule-sets phase1 rule 4 match
  dynamic-application junos:IMAP
user@host-1# set security application-firewall rule-sets phase1 rule 4 then permit
user@host-1# set security application-firewall rule-sets phase1 rule 5 match
  dynamic-application junos:POP3
user@host-1# set security application-firewall rule-sets phase1 rule 5 then permit
user@host-1# set security application-firewall rule-sets phase1 rule 6 match
  dynamic-application junos:FTP
user@host-1# set security application-firewall rule-sets phase1 rule 6 then permit
user@host-1# set security application-firewall rule-sets phase1 rule 7 match
  dynamic-application junos:SMTP
user@host-1# set security application-firewall rule-sets phase1 rule 7 then permit
```

2. Create a black list to deny certain applications.

```
[edit]
user@host-1# set security application-firewall rule-sets phase1 rule 8 match
  dynamic-application junos:YAHOO-MAIL
user@host-1# set security application-firewall rule-sets phase1 rule 8 then deny
user@host-1# set security application-firewall rule-sets phase1 rule 9 match
  dynamic-application junos:FACEBOOK-ACCESS
user@host-1# set security application-firewall rule-sets phase1 rule 9 then deny
user@host-1# set security application-firewall rule-sets phase1 rule 10 match
  dynamic-application-group junos:social-networking
user@host-1# set security application-firewall rule-sets phase1 rule 10 match
  dynamic-application-group junos:web:p2p
user@host-1# set security application-firewall rule-sets phase1 rule 10 match
  dynamic-application-group junos:p2p
user@host-1# set security application-firewall rule-sets phase1 rule 10 then deny
```

3. Create a default rule to permit all application traffic that does not match one of the rules.

```
[edit]
user@host-1# set security application-firewall rule-sets phase1 default-rule permit
```

4. Configure a security policy to apply the application firewall rule set.

   In this example, policy Branch1-policy applies the rule set phase1 to all traffic from the Branch1-Zone zone to the HQ-Zone zone.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match source-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match application any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy then permit application-services application-firewall rule-set
  phase1
```

Configuring AppQoS to Prioritize Marking and Rate Limiting of Application Traffic

Step-by-Step Procedure

To configure an AppQoS implementation:

1. Define one or more forwarding classes dedicated to AppQoS marking.

   In this example, a single forwarding class, my-app-fc, is defined and assigned to queue 0.

```
[edit]
user@host-1# set class-of-service forwarding-classes queue 0 my-app-fc
```

2. Define rate limiters.

   In this example, two rate limiters are defined:

   - test-r1 with a bandwidth of 100 Kbps and a burst limit of 13,000 bytes
   - test-r2 with a bandwidth of 200 Kbps and a burst limit of 26,000 bytes

```
[edit]
user@host-1# set class-of-service application-traffic-control rate-limiters test-rl
  bandwidth-limit 100
user@host-1# set class-of-service application-traffic-control rate-limiters test-rl
  burst-size-limit 13000
user@host-1# set class-of-service application-traffic-control rate-limiters test-r2
  bandwidth-limit 200
user@host-1# set class-of-service application-traffic-control rate-limiters test-r2
  burst-size-limit 26000
```

3. Define AppQos rules and application match criteria.

For this example, rule 0 in rule set ftp-test1 is applied to junos:FTP packets.

```
[edit]
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 match application junos:FTP
```

4. Define the action for rule 0 when it encounters a junos:FTP packet.

   In this example, when a match is made, the packet is marked with the forwarding class my-app-fc, the DSCP value of af22, and a loss priority of low.

```
[edit]
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then forwarding-class my-app-fc
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then dscp-code-point af22
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then loss-priority low
```

5. Assign rate limiters for rule 0 to traffic in each direction.

   In this case, the rate limiter test-r1 is set in both directions.

NOTE: Rate limiter test-r1 can be assigned to one or both traffic directions in rule 0. It could also be assigned in other rules within rule set ftp-test1. However, once test-r1 is assigned to rule set ftp-test1, it cannot be assigned in any other rule set.

```
[edit]
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then rate-limit client-to-server test-r1
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then rate-limit server-to-client test-r1
```

6. Log the AppQoS event whenever this action as defined in rule 0 is triggered:

```
[edit]
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then log
```

7. Define other rules to handle application packets that did not match the previous rule.

   In this example, following rule (rule 1) applies to all remaining applications:

```
[edit]
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 match application-any
```

8. Assign rate limiters for the second rule.

In this example, any traffic that is not from FTP is assigned rate limiter test-r2 in both directions.

```
[edit]
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 then rate-limit client-to-server test-r2
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 then rate-limit server-to-client test-r2
user@host-1# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 then log
```

9. Add the AppQoS implementation to a policy.

   In this example, policy Branch1-policy applies the rule set ftp-test1 to all traffic from the Branch1-Zone zone to the HQ-Zone zone.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match source-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match application any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy then permit application-services application-traffic-control rule-set
  ftp-test1
```

Configuring IDP

Configure the Intrusion detection and prevention (IDP) feature to selectively enforce various attack detection and prevention techniques on network traffic passing through an IDP-enabled device.

As a first step, download and install the signature database from the Juniper Networks website. Next, download and install the predefined IDP policy templates and activate the predefined policy “Client-And-Server-Protection” as the active policy. Next, enable the security policy for IDP inspection.

For more information, see the Intrusion Detection and Prevention Guide for Security Devices.

Enabling IDP in a Security Policy

Step-by-Step Procedure

The following procedure shows how to configure IDP on Branch-1. You can use the same procedure for other branches.

To configure IDP on Branch-1:

1. Download the security package.

```
user@host-1> request security idp security-package download

Will be processed in async mode. Check the status using the status checking
 CLI
```

NOTE: Downloading the database might take some time depending on the database size and the speed of your Internet connection.

2. Check the security package download status.

```
user@host-1> request security idp security-package download status

Done;Successfully downloaded
from(https://services.juniper.net/cgi-bin/index.cgi).
Version info:2457(Wed Jan  7 19:16:21 2015 UTC, Detector=12.6.160140822)
```

3. Install the security package.

```
user@host-1> request security idp security-package install

Will be processed in async mode. Check the status using the status checking
 CLI
```

NOTE: Installing the attack database might take some time depending on the security package size.

4. Check the attack database install status.

   The command output displays information about the downloaded and installed versions of the attack database.

```
user@host-1> request security idp security-package install status

Done;Attack DB update : successful - [UpdateNumber=2230,ExportDate=Mon Feb
 4 19:40:13 2013 GMT-8,Detector=12.6.160121210]
Updating control-plane with new detector : successful
Updating data-plane with new attack or detector : successful
```

5. Confirm your IDP security package version.

```
user@host-1> show security idp security-package-version

Attack database version:2230(Mon Feb  4 19:40:13 2013 GMT-8)
  Detector version :12.6.160121210
  Policy template version :2230
```

6. Download the predefined IDP policy templates.

```
user@host-1> request security idp security-package download policy-templates

Will be processed in async mode. Check the status using the status checking
 CLI
```

7. Check the security package download status.

```
user@host-1> request security idp security-package download status
```

```
Done;Successfully downloaded
from(https://services.juniper.net/cgi-bin/index.cgi).
Version info:2248
```

8. Install the IDP policy templates.

```
user@host-1> request security idp security-package install policy-templates
```

```
Will be processed in async mode. Check the status using the status checking
 CLI
```

9. Verify the installation status update.

```
user@host-1> request security idp security-package install status
```

```
Done;policy-templates has been successfully updated into internal repository
(=>/var/db/scripts/commit/templates.xsl)!
```

10. Enable the **templates.xsl** scripts file.

    On commit, the Junos OS management process (mgd) looks in **templates.xsl** and installs the required policy.

```
[edit]
user@host-1# set system scripts commit file templates.xsl
```

11. Commit the configuration.

    The downloaded templates are saved to the Junos OS configuration database, and they are available in the CLI at the **[edit security idp idp-policy]** hierarchy level.

```
[edit]
user@host-1# commit
```

12. Display the list of downloaded templates.

```
[edit]
user@host-1# set security idp active-policy ?
```

```
Possible completions:
  (active-policy)      Set active policy
Client-And-Server-Protection
Client-And-Server-Protection-1G
Client-Protection
Client-Protection-1G
DMZ_Services
DNS_Service
File_Server
Getting_Started
IDP_Default
Recommended
Server-Protection
Server-Protection-1G
Web_Server
```

    For more information about predefined IDP policy templates, see Understanding Predefined IDP Policy Templates.

13. Activate the predefined **Client-And-Server-Protection** policy as the active policy.

```
[edit]
user@host-1# set security idp active-policy Client-And-Server-Protection
```

14. Confirm the active policy enabled on your device.

```
[edit]
user@host-1# run show security idp active-policy

active-policy Client-And-Server-Protection;
```

15. Enable the security policy for IDP inspection.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match source-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match application any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy then permit application-services idp
```

Configuring Unified Threat Management

Configure UTM to protect your device against multiple threat types.

In this procedure, you define custom objects, configure feature profiles for UTM components (antispam, antivirus, and Web filtering), configure a UTM policy and attach feature profiles, and apply the UTM policy to the security policy as an application service.

For more information, see the Junos OS UTM Library for Security Devices.

NOTE: You must confirm UTM licenses on your device before you start configuring the UTM feature.

Table 4 on page 27 provides the list of configuration parameters used to configure antispam, antivirus, and Web filtering in this example.

Table 4: UTM Components Configuration Parameters

Parameter	Value
Custom objects	URL pattern: • blacklists • whitelists • urllistblack
	MIME pattern: • block-mime-list
	Filename extension: • block-extension-list
	Custom URL category: • blacklist
	Protocol command: • permit-command-list • block-command-list
Antivirus feature profile	fav_profile
Antivirus type	kaspersky-lab-engine
Antispam sbl profile	as_smtp
Web filtering- surf control integrated profile	wf_cpa SHS-Policy-1
Web filtering-websense redirect profile	wf_ws
Content filter profile	CF
UTM policy	utm_p1
Security policy	utm_p1

Configuring UTM Components

Step-by-Step Procedure

The following procedure shows how to configure UTM on Branch-1. You can use the same procedure for other branches.

To configure antispam, antivirus, content filtering, and Web filtering:

1. Configure the antivirus feature profile.

   [edit]

```
user@host-1# set security utm feature-profile anti-virus type kaspersky-lab-engine
user@host-1# set security utm feature-profile anti-virus kaspersky-lab-engine
  pattern-update interval 1500
user@host-1# set security utm feature-profile anti-virus kaspersky-lab-engine profile
  fav_profile scan-options scan-mode all
```

2. Configure custom objects for the antispam feature profile.

```
user@host-1# set security utm custom-objects url-pattern blacklists value
  http://*.gamble.com
user@host-1# set security utm custom-objects url-pattern blacklists value
  http://*.flashgames.com
user@host-1# set security utm custom-objects url-pattern whitelists value
  http://*.work.com
user@host-1# set security utm custom-objects url-pattern whitelists value
  http://*.taxes.com
user@host-1# set security utm custom-objects url-pattern whitelists value
  http://*.networking.com
```

3. Configure the antispam feature profile.

```
[edit]
user@host-1# set security utm feature-profile anti-spam address-whitelist whitelists
user@host-1# set security utm feature-profile anti-spam address-blacklist blacklists
user@host-1# set security utm feature-profile anti-spam sbl profile as_smtp
  sbl-default-server
user@host-1# set security utm feature-profile anti-spam sbl profile as_smtp
  spam-action block
```

4. Configure custom objects for the Web filtering feature profile.

```
user@host-1# set security utm custom-objects url-pattern urllistblack value
  http://www.untrusted.com
user@host-1# set security utm custom-objects custom-url-category blacklist value
  urllistblack
```

5. Configure the integrated Web filtering feature profile.

```
[edit]
user@host-1# set security utm feature-profile web-filtering url-blacklist blacklist
user@host-1# set security utm feature-profile web-filtering type
  surf-control-integrated
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  cache timeout 60
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  cache size 4k
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  server host cpa.surfcpa.com
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  server port 9020
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile wf_cpa category Sports action block
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile wf_cpa default log-and-permit
```

```
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile wf_cpa custom-block-message Juniper_is_blocking_you
```

6. Select an action (permit, log and permit, block) for this profile for requests that experience errors.

```
[edit]
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 category Computing_Internet action permit
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 category Education action permit
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 category Finance_Investment action permit
```

7. Select a default action (block) for this profile for requests that experience errors, and configure a custom message to be sent when HTTP requests are blocked.

```
[edit]
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 default block
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 custom-block-message "This site is blocked by Juniper
  Webfiltering.You can check the category of this site by clicking
  http://mtas.surfcontrol.com/mtas/JuniperTest-a-Site"
```

8. Select fallback settings (block or log and permit) for this profile.

```
[edit]
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 fallback-settings default block
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 fallback-settings server-connectivity block
user@host-1# set security utm feature-profile web-filtering surf-control-integrated
  profile SHS-Policy-1 fallback-settings too-many-requests block
```

9. Configure the Web filtering feature profile (redirect).

```
[edit]
user@host-1# set security utm feature-profile web-filtering websense-redirect
  profile wf_ws server host 10.155.206.13
user@host-1# set security utm feature-profile web-filtering websense-redirect
  profile wf_ws server port 15868
user@host-1# set security utm feature-profile web-filtering websense-redirect
  profile wf_ws fallback-settings default log-and-permit
user@host-1# set security utm feature-profile web-filtering websense-redirect
  profile wf_ws fallback-settings server-connectivity log-and-permit
user@host-1# set security utm feature-profile web-filtering websense-redirect
  profile wf_ws fallback-settings too-many-requests block
user@host-1# set security utm feature-profile web-filtering websense-redirect
  profile wf_ws sockets 8
user@host-1# set security utm feature-profile web-filtering websense-redirect
  profile wf_ws account netscreen
```

10. Configure custom objects for the content filtering profile.

```
user@host-1# set security utm custom-objects protocol-command
  permit-command-list value get
user@host-1# set security utm custom-objects protocol-command
  block-command-list value user
user@host-1# set security utm custom-objects protocol-command
  block-command-list value pass
user@host-1# set security utm custom-objects protocol-command
  block-command-list value port
user@host-1# set security utm custom-objects protocol-command
  block-command-list value type
user@host-1# set security utm custom-objects filename-extension
  block-extension-list value [zip js vbs]
user@host-1# set security utm custom-objects mime-pattern block-mime-list value
  [video/quicktime image/x-portable-anymap x-world/x-vrml]
```

11. Configure the content filtering feature profile.

```
[edit]
user@host-1# set security utm feature-profile content-filtering profile CF
  permit-command permit-command-list
user@host-1# set security utm feature-profile content-filtering profile CF
  block-command block-command-list
user@host-1# set security utm feature-profile content-filtering profile CF
  block-extension block-extension-list
user@host-1# set security utm feature-profile content-filtering profile CF block-mime
  list block-mime-list
user@host-1# set security utm feature-profile content-filtering profile CF
  notification-options custom-message **********AccessDenied**********
```

12. Create a UTM policy and apply the antivirus profile to the UTM policy.

```
[edit]
user@host-1# set security utm utm-policy utm_p1 anti-virus http-profile fav_profile
user@host-1# set security utm utm-policy utm_p1 anti-virus ftp upload-profile
  fav_profile
user@host-1# set security utm utm-policy utm_p1 anti-virus ftp download-profile
  fav_profile
user@host-1# set security utm utm-policy utm_p1 anti-virus smtp-profile fav_profile
user@host-1# set security utm utm-policy utm_p1 anti-virus pop3-profile fav_profile
user@host-1#set security utm utm-policy utm_p1 anti-virus imap-profile fav_profile
```

13. Apply the antispam profile to the UTM policy.

```
[edit]
user@host-1# set security utm utm-policy utm_p1 anti-spam smtp-profile as_smtp
```

14. Apply the content filtering profile to the UTM policy.

```
[edit]
user@host-1# set security utm utm-policy utm_p1 content-filtering http-profile CF
user@host-1# set security utm utm-policy utm_p1 content-filtering ftp upload-profile
  CF
user@host-1# set security utm utm-policy utm_p1 content-filtering ftp
  download-profile CF
user@host-1# set security utm utm-policy utm_p1 content-filtering smtp-profile CF
```



```
user@host-1# set security utm utm-policy utm_p1 content-filtering pop3-profile CF
user@host-1# set security utm utm-policy utm_p1 content-filtering imap-profile CF
```

15. Apply the Web filtering profile to the UTM policy.

```
[edit]
user@host-1# set security utm utm-policy utm_p1 web-filtering http-profile wf_cpa
```

16. Configure traffic options for the UTM policy.

```
[edit]
user@host-1# set security utm utm-policy utm_p1 traffic-options sessions-per-client
  limit 2000
user@host-1# set security utm utm-policy utm_p1 traffic-options sessions-per-client
  over-limit block
```

17. Attach the UTM policy to the security policy Branch1-Zone (policy from the Branch1-Zone zone to HQ-Zone untrust zone), and set the application services to be allowed.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match source-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy match application any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-policy then permit application-services utm-policy utm_p1
```

Configuring Screens

Configure the following screen options to secure the zone by inspecting and then allowing or denying all the inter-zone traffic that would be inspected by the screen feature:

- Reconnaissance attacks (IP spoofing, IP source route option)
- Denial-of-service attacks (ICMP flood, UDP flood, syn flood, ping of death, tear drop, land)
- Suspicious packet attributes (bad IP options, unknown protocols)

After configuring screen options, you must enable screens in the zone.

For more information, see the Junos OS Attack Detection and Prevention Library for Security Devices.

Configuring Multiple Screening Options

Step-by-Step Procedure

The following procedure shows how to configure screen options on Branch-1. You can use the same procedure for other branches.

To configure screen options:

1. Configure protection against an ICMP flood attack.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust icmp flood threshold 10000
   ```

2. Configure protection against the ping of death, an OS-targeted attack.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust icmp ping-death
   ```

3. Configure the IP bad option screen to block large ICMP packets.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust ip bad-option
   ```

4. Configure to detect packets with timestamp options.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust ip timestamp-option
   ```

5. Configure to block IP spoof attacks.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust ip spoofing
   ```

6. Configure to block packets with the source route option set.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust ip source-route-option
   ```

7. Configure the unknown protocol screen to block packets with an unknown protocol.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust ip unknown-protocol
   ```

8. Configure protection against a teardrop attack.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust ip tear-drop
   ```

9. Configure the zone-syn-flood protection screen option, and set the timeout value to 20.

   ```
   [edit]
   user@host-1# set security screen ids-option UTrust tcp syn-flood alarm-threshold
     1024
   ```

```
user@host-1# set security screen ids-option UTrust tcp syn-flood attack-threshold
  200
user@host-1# set security screen ids-option UTrust tcp syn-flood
  destination-threshold 2048
user@host-1# set security screen ids-option UTrust tcp syn-flood timeout 20
```

10. Enable protection against a land attack.

```
[edit]
user@host-1# set security screen ids-option UTrust tcp land
```

11. Enable UDP flood protection.

```
[edit]
user@host-1# set security screen ids-option UTrust udp flood
```

12. Enable the screen in the security zone.

```
[edit]
user@host-1# set security zones security-zone Branch1-Zone screen UTrust
```

Configuring Firewall User Authentication

The integrated user firewall feature introduces an authentication source through integration with Microsoft Active Directory technology. This feature enforces user-based and group-based policy control over traffic.

Configure the integrated user firewall feature by configuring a Windows Active Directory domain, an LDAP base, unauthenticated users to be directed to a captive portal, and a security policy based on a source identity.

For more information, see the Authentication and Integrated User Firewalls Feature Guide for Security Devices.

Table 5 on page 33 provides the domain and domain controller parameters used in establishing a Windows Active Directory domain.

Table 5: Domain and Domain Controllers Parameters

Parameter	Value	Description
Configure Active Directory Access domain name	example.net	Specify domain name to which the query is to be added.
LDAP base distinguished name (DN)	dc=example,dc=net.	Base DN is the starting point where the system starts searching for the user.
Domain controller name and IP address	DC-1 192.0.2.15	The IP address of the domain controller (server).
User name	admin	The user ID used to access the domain controller.

Table 5: Domain and Domain Controllers Parameters *(continued)*

Parameter	Value	Description
Password	welcome	Enter the password for the account used to access the DC.

Table 6 on page 34 provides the domain and domain controller parameters used in configuring a captive portal.

Table 6: Captive Portal Configuration Parameters

Parameter	Value	Description
Base distinguished name	DC=acme,DC=nonexample,DC=net	Base DN is the starting point where the searching for the user starts.
Search filter	cn=	Search filter is used to fine search the user groups. The Filter used for group search will be cn=. cn is the default, and is used by most LDAP servers.
Server IP address	192.0.2.3	LDAP server's IP address.
LDAP administrator name	administrator	LDAP administrator's distinguished name.
LDAP administrator password	password123	LDAP administrator's password.

Configuring Integrated User Firewall Authentication

Step-by-Step Procedure

The following procedure shows how to configure user authentication on Branch-1. You can use the same procedure for other branches.

To integrate user firewall authentication:

1. Configure the LDAP base distinguished name.

```
[edit]
user@host-1# set services user-identification active-directory-access domain
  example.net user-group-mapping ldap base DC=example,DC=net
user@host-1# set services user-identification active-directory-access domain
  example.net user administrator password xxxxx
user@host-1# set services user-identification active-directory-access domain
  example.net domain-controller ad1 address 192.0.2.15
```

2. Create the access profile profile1 for the users, configure a domain name, the username and password of the domain, and the name and IP address of the domain controller in the domain.

```
[edit]
user@host-1# set access profile profile1 authentication-order ldap
user@host-1# set access profile profile1 authentication-order password
user@host-1# set access profile profile1 ldap-options base-distinguished-name
  DC=acme,DC=net
user@host-1# set access profile profile1 ldap-options search search-filter cn=
user@host-1# set access profile profile1 ldap-options search admin-search
  distinguished-name admin
user@host-1# set access profile profile1 ldap-options search admin-search password
  "$9$8HqL-wJGikmfGU0BEhrl"
user@host-1# set access profile profile1 ldap-server 192.0.2.3
```

3. Configure a policy for the source-identity, unauthenticated user, and enable the firewall authentication captive portal.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet match source-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internety match application any
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet match source-identity unauthenticated-user
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet then permit firewall-authentication
  user-firewall access-profile profile1
```

4. Configure a second policy to enable a specific user.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet match source-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet match application any
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet match source-identity
  “example.net\galenrikka”
user@host-1# set security policies from-zone Branch1-Zone to-zone untrust policy
  permit-traffic-branch-1-to-internet then permit
```

Configuring SSL Proxy

In this procedure, you must generate and update the root CA certificate. Next, you will configure an SSL proxy profile and apply the root CA certificate and CA profile groups to the SSL proxy profile. Finally, you will configure the SSL proxy on a security policy.

You can configure additional services such as AppFW or IPS to provide granular inspection.

For more information, see Configuring SSL Proxy.

Configuring SSL Proxy

Step-by-Step Procedure

The following procedure shows how to configure an SSL proxy on Branch-1. You can use the same procedure for other branches.

To generate a root CA certificate using the Junos OS CLI, follow these steps on an SRX Series device:

1. From operational mode, generate a PKI public/private key pair for a local digital certificate.

   ```
   user@host-1> request security pki generate-key-pair certificate-id SELF-SIGNED
     size 2048 type rsa

   Generated key pair SELF-SIGNED, key size 2048 bits
   ```

2. From operational mode, define a self-signed certificate.

   ```
   user@host-1> request security pki local-certificate generate-self-signed certificate-id
     SELF-SIGNED subject CN=abc domain-name juniper.net email user@juniper.net

   Self-signed certificate generated and loaded successfully
   ```

3. From configuration mode, apply the loaded certificate as root-ca in the SSL proxy profile.

   ```
   [edit]
   user@host-1# set services ssl proxy profile SSL-PROXY-SAMPLE root-ca
     SELF-SIGNED
   ```

4. Specify to ignore server authentication.

   Junos OS provides the following options for trusted CA certificates:

   - Loading the default trusted CA list
   - Importing the trusted CA list manually
   - Ignoring server authentication

   For more information, see Configuring SSL Proxy.

   This example uses the Ignoring server authentication method.

   In this method, any errors encountered during server certificate verification at the time of the SSL handshake are ignored. We do not recommend using this option for authentication because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause of dropped SSL sessions.

   ```
   [edit]
   user@host-1# set services ssl proxy profile SSL-PROXY-SAMPLE
     ignore-server-auth-failure
   ```

5. Configure an option to receive the logs.

SSL proxy logs contain the logical system name, SSL proxy whitelists, policy information, SSL proxy information, and other information that helps you troubleshoot when there is an error.

```
[edit]
user@host-1# set services ssl proxy profile SSL-PROXY-SAMPLE log all
```

6. Create a security policy and specify the match criteria for the policy.

   For match criteria, specify the traffic for which you want to enable the SSL proxy.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-ssl-proxy-policy match source-address 192.168.1.0/24
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-ssl-proxy-policy match destination-address any
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-ssl-proxy-policy match application any
```

7. Apply the SSL proxy profile to the security policy.

```
[edit]
user@host-1# set security policies from-zone Branch1-Zone to-zone HQ-Zone policy
  Branch1-ssl-proxy-policy then permit application-services ssl-proxy profile-name
  SSL-PROXY-SAMPLE
```

Verification

Confirm that the configuration is working properly.

- Verifying the Security Policy Configuration on page 37
- Verifying the Security Policy for User Authentication on page 38
- Verifying the IDS Profile for Screening Options on page 39
- Verifying Application Statistics on page 39
- Verifying AppQoS Session Statistics on page 40
- Verifying AppTrack Counter Values on page 40
- Verifying the Antivirus Protection Configuration on page 41
- Verifying the Antispam Protection Configuration on page 42
- Verifying the Content Filtering Protection Configuration on page 42
- Verifying the Web Filtering Protection Configuration on page 42
- Verifying the SSL Proxy Configuration on page 43

Verifying the Security Policy Configuration

Purpose Verify that the security policy is configured correctly on the branch office.

Action From operational mode, enter the **show security policies** command to display details about the policy configured on the device.

```
user@host> show security policies from-zone Branch1-Zone to-zone HQ-Zone detail
Policy: Branch1-policy, action-type: permit, State: enabled, Index: 4, Scope
Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: Branch1-Zone, To zone: HQ-Zone
  Source addresses:
    any-ipv4(address-book-branch-1-users): 0.0.0.0/0
    any-ipv6(address-book-branch-1-users): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
  Intrusion Detection and Prevention: enabled
  Unified Access Control: disabled
  Unified Threat Management: enabled
  Application firewall:phase1
  Application traffic control: ftp-test1
Session log: at-create, at-close
```

Meaning The output displays information about the Branch1-policy policy configured on the system. Verify the following information:

- From and To zones
- Intrusion Detection and Prevention
- Unified Threat Management
- Application firewall
- Application traffic control

Verifying the Security Policy for User Authentication

Purpose Verify that integrated user firewall authentication is configured correctly on the branch office.

Action From operational mode, enter the **show security policies** command to display details about the policy configured on the device.

```
user@host> show security policies from-zone Branch1-Zone to-zone untrust detail
Policy: permit-traffic-branch-1-to-internet, action-type: permit, State: enabled, Index:
 5, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: Branch1-Zone, To zone: untrust
  Source addresses:
```



```
  any-ipv4(address-book-branch-1-users): 0.0.0.0/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
    Source port range: [0-0]
    Destination port range: [0-0]
Source identities:  unauthenticated-user  example.net\galenrikka
Per policy TCP Options: SYN check: No, SEQ check: No
Authentication: no auth, Access profile: profile1
```

Meaning The output displays information about the policy permit-traffic-branch-1-to-internet configured on the system. Verify the following information:

- From and To zones
- Source identities

Verifying the IDS Profile for Screening Options

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

Action From operational mode, enter the **show security screen ids-option** command to display details about the configured screen options on the device.

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

Name                                    Value
  ICMP flood threshold                  10000
  UDP flood threshold                   1000
  IP tear drop                          enabled
  TCP SYN flood attack threshold        200
  TCP SYN flood alarm threshold         1024
  TCP SYN flood source threshold        4000
  TCP SYN flood destination threshold   2048
  TCP SYN flood timeout                 20
  IP spoofing                           enabled
  ICMP ping of death                    enabled
  IP source route option                enabled
  TCP land attack                       enabled
  IP unknown protocol                   enabled
  IP timestamp option                   enabled
```

Meaning The output displays information about the screen options details configured on the system.

Verifying Application Statistics

Purpose View the application usage statistics.

Action From operational mode, enter the **show services application-identification statistics applications** command.

```
user@host> show services application-identification statistics applications

Last Reset: 2014-11-06 01:49:17 PST
            Application           Sessions              Bytes    Encrypted
            BITTORRENT                   9            1178014           No
      FACEBOOK-ACCESS                    3              24012          Yes
               GOOGLE                    1               8004          Yes
                 HTTP                    4           18295042           No
                 HTTP                    1               7964          Yes
                  SSL                    5              39980          Yes
```

Meaning The output displays information about the cumulative session and byte statistics per application.

Verifying AppQoS Session Statistics

Purpose Verify that AppQoS session statistics are being accumulated at each egress node.

Action From operational mode, enter the **show class-of-service application-traffic-control counter** command.

```
user@host> show class-of-service application-traffic-control counter

pic: 1/0
  Counter type                                                  Value
 Sessions processed                                             1
 Sessions marked                                                1
 Sessions honored                                               0
 Sessions rate limited                                          1
 Client-to-server flows rate limited                            0
 Server-to-client flows rate limited                            1
```

Meaning The output displays information about the AppQoS DSCP marking and honoring statistics based on layer-7 application classifiers.

Verifying AppTrack Counter Values

Purpose View the AppTrack counters periodically to monitor logging activity.

Action From operational mode, enter the **show security application-tracking counters** command.

```
user@host> show security application-tracking counters

AVT counters:                Value
 Session create messages           1
 Session close messages            1
```

```
Session volume updates              2
Failed messages                     0
```

Meaning The output displays information about the status of AppTrack counters.

NOTE: The following output shows a sample syslog message of the AppTrack log:

```
Nov  6 02:06:45 5.0.0.254 RT_FLOW: APPTRACK_SESSION_CREATE: AppTrack
session created 4.0.0.1/36694->5.0.0.1/80 junos-http HTTP FACEBOOK-APP
 4.0.0.1/36694->5.0.0.1/80 None None 6 1 untrust trust 120014281 N/A
N/A No

Nov  6 02:09:10 5.0.0.254 RT_FLOW: APPTRACK_SESSION_CLOSE: AppTrack
session closed TCP FIN: 4.0.0.1/36694->5.0.0.1/80 junos-http HTTP
FACEBOOK-APP 4.0.0.1/36694->5.0.0.1/80 None None 6 1 untrust trust
120014281 1847(96181) 6911(10359653) 145 N/A N/A No

Nov  6 02:07:45 5.0.0.254 RT_FLOW: APPTRACK_SESSION_VOL_UPDATE: AppTrack
 volume update: 4.0.0.1/36694->5.0.0.1/80 junos-http HTTP FACEBOOK-APP
 4.0.0.1/36694->5.0.0.1/80 None None 6 1 untrust trust 120014281
790(41217) 2934(4395945) 60 N/A N/A No
Nov  6 02:08:45 5.0.0.254 RT_FLOW: APPTRACK_SESSION_VOL_UPDATE: AppTrack
 volume update: 4.0.0.1/36694->5.0.0.1/80 junos-http HTTP FACEBOOK-APP
 4.0.0.1/36694->5.0.0.1/80 None None 6 1 untrust trust 120014281
1559(81205) 5831(8741445) 120 N/A N/A No
```

Verifying the Antivirus Protection Configuration

Purpose Verify that the antivirus protection configuration is working properly.

Action From operational mode, enter the **show security utm anti-virus status** command.

```
user@host> show security utm anti-virus status

UTM anti-virus status:

Anti-virus key expire date: 2010-12-31 00:00:00
Update server: http://update.juniper-updates.net/AV/SRX210
Interval: 120 minutes
Pattern update status: next update in 54 minutes
Last result: already have latest database
Anti-virus signature version: 09/03/2009 07:01 GMT-8, virus records: 467973
Anti-virus signature compiler version: N/A
Scan engine type: kaspersky-lab-engine
Scan engine information: last action result: No error(0x00000000)
```

Meaning The output displays information about antivirus status for connections including clean and infected files and scan engine status.

Verifying the Antispam Protection Configuration

Purpose Verify that the antispam protection configuration is working properly.

Action From operational mode, enter the **show security utm anti-spam status** and **show security utm anti-spam statistics** commands.

```
user@host> show security utm anti-spam status

SBL Whitelist Server:
SBL Blacklist Server:
    msgsecurity.juniper.net

DNS Server:
    Primary  :     192.168.5.68, Src Interface: lo0
    Secondary:   192.168.60.131, Src Interface: ge-0/0/0
    Ternary  :    172.17.28.100
```

Meaning The output displays information about antispam status for connections including whitelist and blacklist server information

Verifying the Content Filtering Protection Configuration

Purpose Verify that the content filtering configuration is working properly.

Action From operational mode, enter the **show security utm content-filtering statistics** and **show security utm anti-spam statistics** commands.

```
user@host>  show security utm content-filtering statistics

 Content-filtering-statistic:         Blocked
     Base on command list:                  1
     Base on mime list:                     0
     Base on extension list:                3
     ActiveX plugin:                        0
     Java applet:                           0
     EXE files:                             0
     ZIP files:                             0
     HTTP cookie:                           0
```

Meaning The output displays content-filtering statistics for connections including lists of blocked files and the reasons for blocking.

Verifying the Web Filtering Protection Configuration

Purpose Verify that the Web filtering configuration is working properly.

Action From operational mode, enter the **show security utm web-filtering status** and **show security utm web-filtering statistics** commands.

user@host> show security utm web-filtering status

```
 UTM web-filtering status:
Server status: Websense redirect URL filtering
```

user@host> show security utm web-filtering statistics

```
 UTM web-filtering statistics:
    Total requests:                 0
    white list hit:                 0
    Black list hit:                 0
    Server reply permit:            0
    Server reply block:             0
    Web-filtering sessions in total: 4000
    Web-filtering sessions in use:   1
    Fall back:                      log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              0
Too-many-requests                                0              0
```

Meaning The output of **show security utm web-filtering status** displays whether the Web filtering server connection is up or not.

The output of **show security utm web-filtering statistics** displays Web filtering statistics for connections including whitelist and blacklist hits and custom category hits.

Verifying the SSL Proxy Configuration

Purpose View the SSL proxy statistics.

Action From operational mode, enter the **show services ssl proxy statistics** command.

user@host> show services ssl proxy statistics

```
PIC:fwdd0 fpc[0] pic[0] ------
        sessions matched                    30647
        sessions whitelisted                    0
        sessions bypassed:non-ssl               0
        sessions bypassed:mem overflow          0
        sessions created                    25665
        sessions ignored                        6
        sessions active                         0
        sessions dropped                        0
```

Meaning The output displays information about the number of proxy sessions that are matched, whitelisted, bypassed, created, dropped, active, and ignored.

Related Documentation

- Introduction to the SRX Series on page 5
- Security Threats and What the SRX Series Offers on page 5
- Next-Generation Security Features on page 7