JUNIPER NETWORKS

Engineering. Simplicity.

DAY ONE: SRX SERIES UP AND RUNNING WITH ADVANCED SECURITY SERVICES

Set up the SRX Series as a next-generation firewall and take advantage of its advanced security features, including machine-learning malware prevention capabilities.

By Alexandre S. Cezar

DAY ONE: SRX SERIES UP AND RUNNING WITH ADVANCED SECURITY SERVICES

From a security perspective, the SRX Series goes beyond traditional stateful firewalls, providing Unified Threat Management (UTM), Advanced Anti-Malware detection and blocking (Sky ATP), reputation blocking (Security Intelligence), and a complete set of next-generation firewall services (NGFW): Application Firewall, Application QOS, Application Routing, SSL Proxy Inspection, and Intrusion Prevention System (IPS). But there isn't an all-in-one document that explains how you can easily configure all this. Until now.

Day One: SRX Series Up and Running with Advanced Security Services walks you through the SRX Series setup using advanced security measures to protect and defend your network. Learn how to spend more time analyzing security traffic than fixing common configuration issues with your new SRX Series – chapter by chapter this book shows you how.

> "The Juniper Networks SRX Series Security platforms provide exceptional security for networks needing to secure their infrastructure and Alexandre Cezar has written a thorough guide on setting up, configuring, and operating these advanced services on the SRX platform. This *Day One* book is easy to use as Cezar demystifies network security engineering along the way."
>
> *Harry Cornwell, JDI Technical Marketing Engineer-L7 Services, Juniper Networks*

> "*This book is an invaluable guide for SRX administrators, both new and old, looking to better acquaint themselves with the latest features and functionality available on the platform.*"
>
> *Craig Dods, Chief Architect, Security, Juniper Networks*

IT'S DAY ONE AND YOU HAVE A JOB TO DO, SO LEARN HOW TO:

- Set up a SRX Series device using the graphical user interface in a matter of minutes.
- Understand how the SRX works and the best practices for security zones and policies.
- Implement IPsec site-to-site VPN tunnels and SSL remote client VPN.
- Configure the SRX as a next-generation firewall (NGFW).
- Configure Unified Threat Management (UTM).
- Configure the automated 'infected host-blocking' capability
- Enable advanced security features, such as Sky ATP and Spotlight Secure.
- Monitor the SRX, security events, and generate reports.
- Perform basic and advanced troubleshooting.

ISBN 978-1-941441-65-7
52500
9 781941 441657

Juniper Networks Books are singularly focused on network productivity and efficiency. Peruse the complete library at www.juniper.net/books.

JUNIPER
NETWORKS

Day One: SRX Series Up and Running with Advanced Security Services

by Alexandre S. Cezar

JUNIPer
NETWORKS

Published by Juniper Networks Books
Author: Alexandre S. Cezar
Technical Reviewers: Craig Dods, Laurent Paumelle, Pavel Zhivov, and Riadh Trabelsi
Editor in Chief: Patrick Ames
Copyeditor: Nancy Koerbel

ISBN: 978-1-941441-65-7 (print)
Printed in the USA by Vervante Corporation.

ISBN: 978-1-941441-68-8 (ebook)

Version History: v1, March 2018
2 3 4 5 6 7 8 9 10

http://www.juniper.net/dayone

About the Author

Alexandre Cezar (CISSP, Comptia Security+, JNCIP-Security, JNCDS-Security, JNCDS-Datacenter, JNCIS-Cloud) holds a BS of Mathematics from the Santo André Foundation and a MBA in Information Security from the Federal University for Technological Education of Rio de Janeiro (CEFET-RJ). He is a Consulting Engineer at Juniper Networks, specializing in Security Products and Cloud/SDN Solutions. Before joining Juniper, Alexandre occupied Senior Systems Engineering and Product Management positions at different organizations, such as Netwitness, RSA, Cloudshield Technologies, Alcatel-Lucent, and Alienvault, among others, in addition to spending several years designing and implementing multi-vendor networks for customers around the globe.

Author's Acknowledgments

The author would like to take this opportunity to thank his wife, Rosemary, for all the support (and late night coffees), Patrick Ames for helping to guide this book's progress, and Craig Dods, Laurent Paumelle, Pavel Zhivov, and Riadh Trabelsi for the technical support that helped make this book a reality.

Feedback? Comments? Error reports? Email them to dayone@juniper.net.

Welcome to Day One

This book is part of the *Day One* library, produced and published by Juniper Networks Books.

Day One books were conceived to help you get just the information that you need on day one. The series covers Junos OS and Juniper Networks networking essentials with straightforward explanations, step-by-step instructions, and practical examples that are easy to follow.

You can obtain publications from either series in multiple formats:

- Download a free PDF edition at http://www.juniper.net/dayone.
- Get the ebook edition for iPhones and iPads from the iBooks Store. Search for *Juniper Networks Books* or the title of this book.
- Get the ebook edition for any device that runs the Kindle app (Android, Kindle, iPad, PC, or Mac) by opening your device's Kindle app and going to the Amazon Kindle Store. Search for *Juniper Networks Books* or the title of this book.
- Purchase the paper edition at Vervante Corporation (www.vervante.com) for between $15-$40, depending on page length.
- Note that most mobile devices can also view PDF files.

SRX Series Documentation

The official and in-depth documentation on all aspects of SRX Series deployment starts here: https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/srx-series/product/index.html.

What You Need to Know Before Reading This Book

Before reading this book, you should have a basic understanding of the Junos OS. Specifically, you should be able to change configurations and to navigate through the command line or graphical user interface hierarchy. You should reference other Day One books and online training to help you acquire this background.

Other knowledge that will be helpful to you as you read through this book is:

- Understanding of TCP/IP.
- Knowing the difference between stateless and stateful firewall technologies.
- Understanding of Deep Packet Inspection (DPI).
- Basic knowledge of how anti-virus, anti-spam, and web filtering technologies work.
- Understanding of malware concepts.
- Basic knowledge of cloud-based services.
- Familiarity with interface naming in devices running the Junos OS.

Although not mandatory to get the most from reading this book, access to SRX devices can help you practice configuring the various scenarios covered here, increasing the speed with which you implement SRX devices in your network.

NOTE The SRX family comes in several different platforms designed for a variety of networking uses. There are branch SRX Series Services Gateways, High-End SRX Series Services Gateways, and virtual vSRX Series Gateways. This book simplifies the terminology by using the generic term *SRX*, or *the SRX*.

What You Will Learn by Reading This Book

- Set up a SRX Series Device using the graphical user interface in a matter of minutes.
- Understand how the SRX works and the best practices on setting up security zones and policies.
- Implement IPsec site-to-site VPN tunnels and SSL remote client VPN.
- Configure the SRX as a next-generation firewall (NGFW).
- Configure unified threat management (UTM).
- Enable advanced security features, such as Sky Advanced Threat Protection (ATP) and Spotlight Secure.

- Configure the infected host-blocking capability
- Monitor the SRX, analyze security events, and generate reports.
- Perform basic and advanced troubleshooting.

MORE? Some features of the SRX are configured differently on different platforms, and at the time this book was written not all features were available on all platforms. This book attempts to point that out for you, however, always check the Juniper Networks SRX landing page for the most recent feature availability for your SRX platform of choice: https://www.juniper.net/us/en/products-services/security/srx-series/.

SRX Hardening Checklist

It's always good to look for ways to improve the security posture of your network. Although this book covers some hardening configurations that apply to anyone, it's important to check for other tasks that can apply to your specific environment.

Great sources of information are located on:

Team CYRU Security templates:
http://www.cymru.com/gillsr/documents/junos-template.pdf

This Week: Hardening Junos Devices, 2nd Edition, by John Weidley:
https://www.juniper.net/us/en/training/jnbooks/day-one/fundamentals-series/hardening-junos-devices-checklist/

Chapter 1

Understanding How the SRX Series Works

You'll find the SRX is a very flexible security platform. From a security perspective, the SRX goes beyond traditional stateful firewalls, providing unified threat management services (UTM), Advanced Anti-Malware detection and blocking (Sky ATP), reputation blocking (Security Intelligence), and a complete set of next-generation firewall services (Application Firewall, Application QOS, Application Routing, SSL Proxy Inspection, and intrusion prevention system (IPS). It also offers advanced switching and routing capabilities, including support for protocols, such as 802.1x, OSPF, BGP, MPLS, IS-IS, and even advanced capabilities such as SD-WAN.

This *Day One* book focuses on configuration and management via the J-Web interface (on-box).

MORE? Juniper also offers a multi-dimensional and centralized approach to manage the SRXs via Junos Space Security Director. For more information about this approach, start here: https://www.juniper.net/us/en/products-services/security/security-director/.

Before starting your deployment and configuration tasks, it's important for you to understand some basic concepts. This chapter focuses on explaining key SRX concepts and references a basic topology you can use in your lab or in your own deployments.

Interfaces and Security Zones

From a security perspective, interfaces are the logical properties of a network interface. Logical properties include:

- Protocol families running on the interface (including any protocol-specific MTUs).
- IP address or addresses associated with the interface. A logical interface can be configured with an IPv6 address, IPv4 address, or both.
- The IP specification requires a unique address on every interface of each system attached to an IP network, so that traffic can be correctly routed.
- VLAN configurations.

The first thing that administrators realize after configuring an IP address in an interface is that they cannot even ping it. This is because SRX devices are hardened devices, and no traffic is allowed in and out of the box without explicitly permitting it. Makes sense.

To permit traffic in and out of an interface, you need to configure more elements. Besides the IP address settings, an interface needs to be associated with a security zone, and the security zone in turn needs to be bound by association with a routing instance. This relationship is illustrated in Figure 1.1.

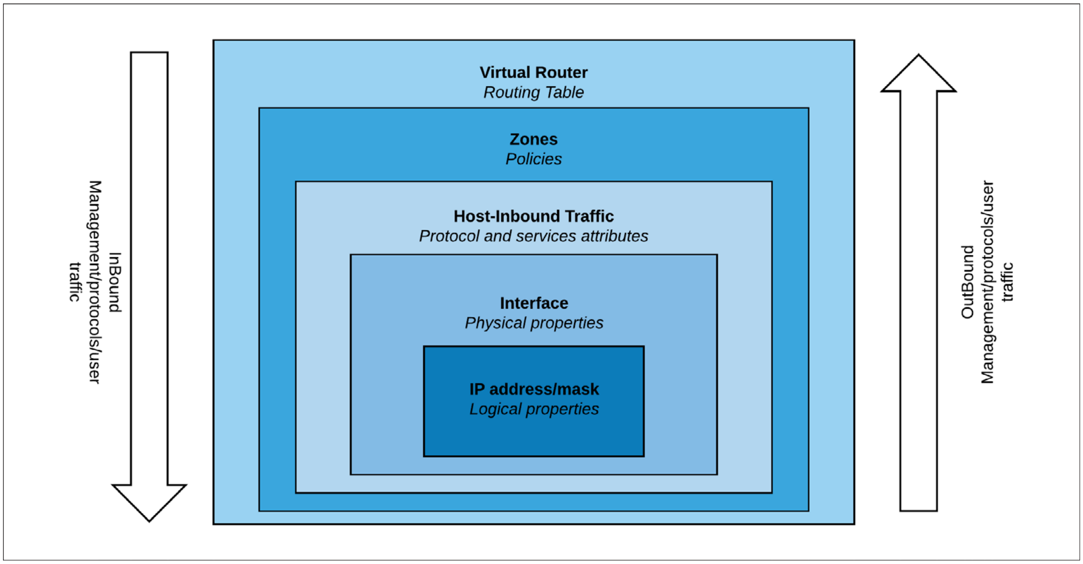


Figure 1.1 SRX Traffic Flow

In Figure 1.1 you can see that traffic destined for an interface can be one of three different types:

- Management (or system-services), for example HTTPS and SSH;
- Protocol-related such as OSPF and DHCP (or referred to simply as protocol);
- Or user originated traffic, such as packets corresponding to the communication from a client to a server.

Notice that if traffic is destined to an interface for the purpose of managing the device, then that is where host-inbound traffic comes into play. Host-inbound traffic is a feature that allows an administrator to enable certain services in a given interface for management and other control plane-related activities. It can be configured at two different levels. If configured at the zone level, then it will affect all the interfaces bound to that zone, but when configured at the interface level, host-inbound traffic will affect only that specific interface. In the event that host-inbound traffic is configured at both the interface and zone levels, then the interface settings will override the zone level one. In other words, services are not added.

Let's try another example. If you configure *ping system services* at the zone level, and try to ping an interface belonging to that zone, it will respond properly. If you later decide to enable SSH in the same interface by configuring system services at the interface level, then ping will stop responding. This is because interface settings take precedence. To fix this and be able to get responses again, you need to also enable *ping system services* at the interface level.

TIP Remember that host-inbound traffic settings have no effect over outbound traffic.

Before moving past the interface level, there are two important points you should note:

- First, configuring system services host-inbound traffic is not sufficient to manage a device via an interface. While the interface can accept those types of traffic, for some services like Telnet, SSH, FTP, and J-Web access, you must also enable the corresponding services at the global system level.
- Second, host-inbound traffic settings do not affect fxp0 interfaces, and they cannot be configured for those interfaces, as fxp0 interfaces are exclusively for out-of-band management purposes. So as long as you configure an IP address, and turn on the services, then you can connect remotely. While this book manages the SRX using transit interfaces (in-band management), it's important that you understand the different type of management options that are available.

A closer examination of Figure 1.1 also reveals the presence of policies; it indicates that traffic from any zone, destined to any other zone (even if it's the same as the source), requires a security policy to be permitted to pass through. Be aware that traffic moving from one zone to any other zone, implies that this is user data or transit traffic (referred to many times as *transient traffic*).

The absence of security policies will result in dropped traffic. This specific behavior is what it makes the SRX so secure by nature – you decide what specific traffic is permitted from one zone to another or even for interfaces that belong to the same security zone.

Since management traffic is not traversing the firewall but is actually terminating at the firewall, then this does not explicitly require examination by any security policies, although best practice recommends that administrators apply security policies to restrict management traffic.

Finally, the outer layer of Figure 1 (the router), makes reference to the routing table instance. By default, all predefined zones or newly created zones are bound to the default-routing instance (IPv4 routing table), unless specified otherwise. Put differently, configuring an IP address in an interface, and binding it to a zone, creates a host routing entry table in inet.0.

You can extend the virtual router (VR) concept to as many VRs as needed to fit your routing requirements. You can have a peering VR running BGP, a "core" VR running OSPF, and a default VR receiving only the necessary routes from these custom VRs.

Zone Types

It's also critical that you understand what zones are, and what zone types are available in the Junos OS for the SRX.

Zones are logical constructs in Junos OS that aggregate interfaces, objects, and security policies to define a security boundary.

There are two types of zones that can be configured: *functional zones* and *security zones*.

A functional zone is a logical construct that is applied to the interface so it can have a management function. Interfaces that are a member of a functional zone cannot be used in a security zone. On the SRX, the only functional zone available is the management zone. Adding an interface into this zone allows the interface to be used for out-of-band management.

A security zone is a logical construct that is applied to interfaces, which allows it to pass or deny traffic if certain conditions (policies) are met. A logical interface cannot be part of more than one security zone.

Traffic that enters and exits a security zone is processed according to the features you configure, such as packet filters, security policies, UTM, application control, and screens (anti-DoS). For example, the SRX can determine:

- whether the packet is allowed into the device;
- which screens to apply to the packet;
- the route the packet takes to reach its destination;
- which CoS to apply to the packet, if any;
- whether to apply NAT to translate the packet's IP address; and
- whether the packet requires an Application Layer Gateway (ALG).

Packets that enter and exit a device undergo both packet-based and flow-based processing:

- Flow-based packet processing treats related packets, or a stream of packets, in the same way. Packet treatment depends on characteristics that were established for the first packet of the packet stream, which is referred to as a flow. Packet sequencing is maintained for the sampled packets.
- Packet-based, or stateless, packet processing treats packets discretely. Each packet is assessed individually for treatment.

The rest of this book focuses on flow-based processing.

Understanding Flow-Based Processing

A packet undergoes flow-based processing after packet-based filters and some screens have been applied to it. Figure 1.2 is a conceptual view of flow-based traffic processing on the SRX.

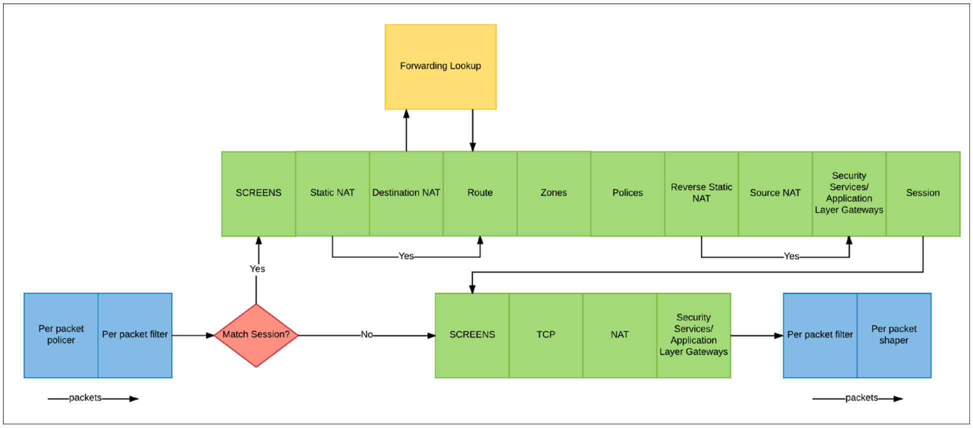


Figure 1.2 Traffic Flow for Flow-Based Processing

A flow is a stream of related packets that meet the same matching criteria and share the same characteristics. Junos OS treats packets belonging to the same flow in the same manner.

After the SRX determines if the packet belongs to a new flow or an existing flow, it actually completes many more complex analyses before it determines what to do with the session or packet, and a lot depends on whether the SRX has already seen the flow (session).

When there is no match for the session, the SRX subjects the packet to first path processing. If the packet matches an installed session, the SRX enables fast path processing.

To determine if a flow exists for a packet, the SRX attempts to match the packet's information to that of an existing session based on the following match criteria:

- Source address
- Destination address
- Source port
- Destination port
- Protocol
- Unique session token number for a given zone and virtual router

If the packet is from a new flow, the following steps happen:

- SCREENS check.
- Static or Destination NAT lookup (in case one the them is found).
- Route lookup to determine the next hop.
- Destination interface and zone lookup.
- Firewall policy lookup.
- Reverse or Source NAT lookup (in case one them is found).
- Define the ALG that needs to be used.
- Apply intrusion detection and prevention system (IDP), VPN, or other advanced security services.
- Install the new session in the SRX flow session table.

If the packet matches an existing session, then fast-path flow processing is used. On fast-flow processing, many of the first-path lookups are not necessary (already done). Fast-path processing executes the following:

- SCREENS check.
- TCP header and flag checks.
- Route lookup and NAT translation.
- Apply ALG services.
- Apply advanced security services.

It's important to note that even if the flow session is established and the fast path is used, the security checks still take place, so the SRX can block and drop denial of service and other malicious attacks during the lifespan of a session.

One other important process that requires further explanation is the Services/ALG.

An Application Layer Gateway (ALG) is a software component that is designed to manage specific protocols such as Session Initiation Protocol (SIP), FTP, and other protocols that need the device to create pinholes to allow returning traffic. The ALG plugin is responsible for Application-Layer aware packet processing.

Services are the advanced security features the SRX uses to protect networks, such as UTM, AppSecure, Sky ATP, SSL-Proxy, Security Intelligence, and IDP. Advanced security services and ALGs are evaluated and inspected in the Services module shown in Figure 1.3.

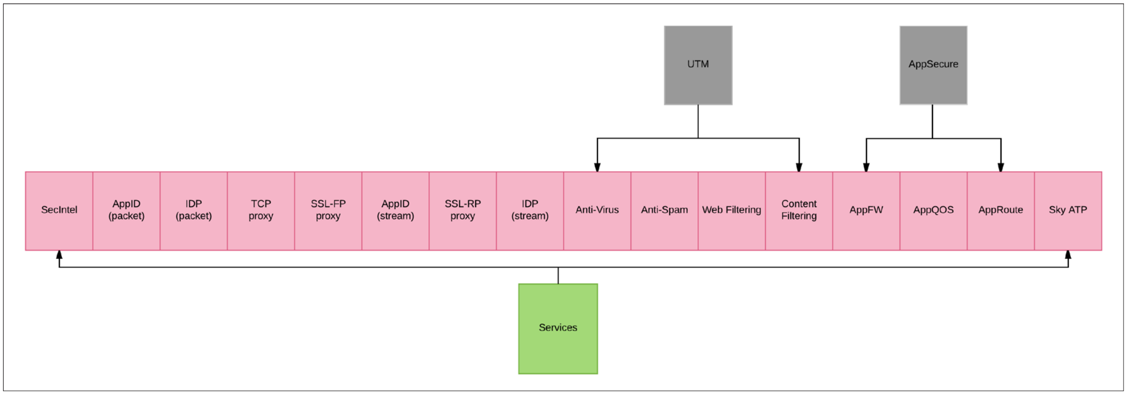


Figure 1.3 Detailed View of the Services/ALG Details

MORE? You can find a detailed explanation about how SRX flow processing works on the *Flow Based and Packet Based Processing Feature Guide for Security Devices* paper, located in the Juniper TechLibrary: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/security/security-processing-overview.pdf.

This Book's Reference Topology

The topology shown in Figure 1.4 will be used for the configuration and deployments in this book. The main objective is to mimic a sample enterprise network comprised of four different zones:

- Trust (user endpoints, printers, etc.) – Device management will also be achieved from this zone.
- Server (Non-Internet exposed servers, such as Active Directory, File Server, etc.).
- DMZ (Internet facing services, such as a web server).
- Untrust (Internet).

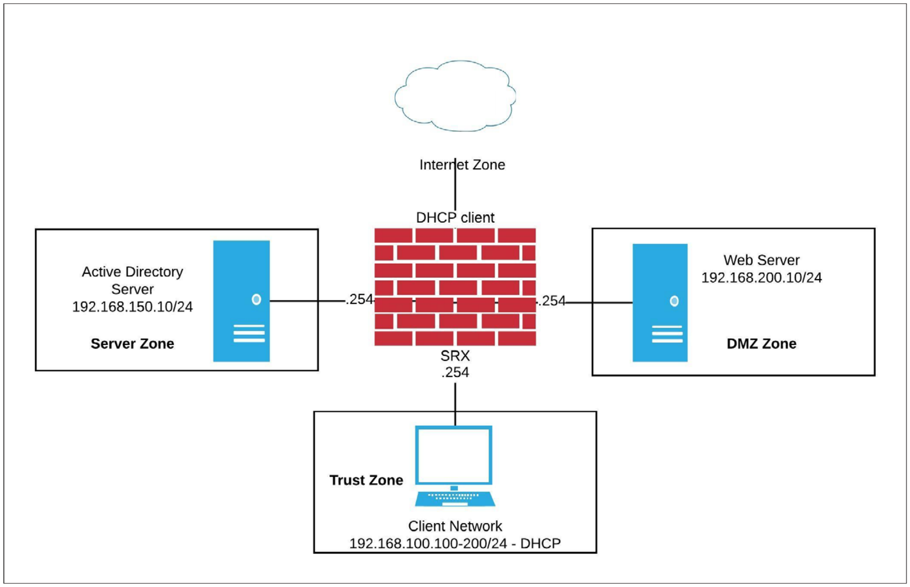


Figure 1.4 This Book's Reference Topology

With this topology, endpoints are connected in the Trust zone and advanced services such as User Firewall, Application Firewall, Anti-Virus, Web filtering, Anti-Malware (Sky ATP), and Threat Feeds are enabled. This allows the administrator to provide greater security for the connected endpoints and to obtain visibility into the network.

The Server Zone protects the internal server farm and offers security isolation from the endpoints. This allows an administrator to enable only the necessary ports, exposing the necessary services only to users who need them, and reducing the likelihood of an attack. It also enables the administrator to enable IPS for specific servers or services, saving system resources.

The DMZ Zone is where all Internet-facing services are allocated. The DMZ Zone will only allow access to the necessary ports and applications, blocking all other traffic. The IPS is a must have in this zone, as attacks against the exposed services are very likely to happen and an IPS can mitigate many attacks upfront. An Application Firewall can also be leveraged to control which applications can be opened, not just the TCP/UDP ports.

These are the basic SRX Series concepts that you need to know. As you get your own SRX up and running, revisit this chapter at any time during this book's tutorials to reacquaint yourself with the fundamentals.

Chapter 2

Managing the SRX

Because you can connect to the SRX Series in multiple ways, it's a very flexible security platform for performing configuration and management tasks. And because it is a Junos OS device, you have the option to manage a SRX via the console port, the CLI, the on-box web interface (known as *J-Web*), the centralized management platforms (Junos Space Security Director or Contrail Services Orchestrator), via the cloud using the Sky Enterprise Management Platform, or through even more sophisticated mechanisms like Automation/DevOps platforms, and scripts written in Python or Ruby.

Some of these connection methods first require an initial configuration. Additionally, since every single configuration and management method is not available via all interfaces, it's important to understand what is possible with each method, then you can decide what is best for your environment.

As mentioned before, this *Day One* book focuses on configuration and management via the J-Web interface, but it highlights capabilities of the other methods, when appropriate.

Connecting Via Console Port

Every physical SRX model, from the smallest to the largest, has a RJ45 console connection that is properly identified. So when connecting via the console, all that is required is a rollover serial connection directly from your computer, or via a console server.

This connection method does not require any prior configuration on the SRX and the actual management interface is the CLI.

There are really no limitations on what you can do via this connection method, and for this reason it's considered perhaps one of the most powerful ways to manage the device and it should always be leveraged as a management method (as an always-on backup connection to the device, for example).

To connect via the console, you need: the supplied console cable, a computer with a serial port (or a USB to Serial adapter), and a terminal emulation application running on the connected computer.

Connecting Via the CLI

This method refers to a connection via a different port than the console, even though the actual interface is the same CLI. It's different than the previous method because you use an Ethernet port, and it requires some upfront configuration, the most significant being the network address configuration (IP and subnet) in the selected port.

You can use any port for CLI management, that really depends on your requirements, but in a nutshell, any port, or all ports, can be configured to accept management connections. Since you are now dealing with an IP connection, you can directly attach using a standard Ethernet patch cable, or you can also be thousands of miles away (provided, of course, that you can reach the configured IP address).

Typically, after doing an initial configuration via the console, most administrators configure the necessary elements to allow remote access to the device via protocols like SSH. There are several steps to enable remote access management via the CLI, and these are shown in subsequent chapters of this book.

Since the interface is the same as when you connect via the console, when managing the device, you can enjoy the same unlimited power with some added benefits, the most important being the ability to accept multiple, concurrent administration connections, via the same ports.

NOTE SRX models also have a dedicated management port that is different than the console. This port is exclusive for management purposes. Also known as *fxp0s*, these interfaces exist in the control plane of the SRX and cannot be used for user data traffic (which helps to guarantee that the dedicated management channel remains open in the event that there is a disruption of the data plane).

Check the specific documentation for your SRX to identify what port (if any) is the dedicated management port.

Connecting Via the GUI J-Web

J-Web is a renewed version of the legacy web-based management interface that ran on older SRX models. The new J-Web allows you to manage the SRX via a graphical interface on a web browser and perform almost all of the management tasks. This capability is available on all SRX platforms, big or small, physical or virtual.

Connecting via J-Web has similar requirements to connecting via CLI. Some initial configuration needs to be done, such as setting an IP address and a subnet mask, as well as turning on this particular management service. As long as you can reach the IP address configured on any of the interfaces, and the corresponding services are turned on, then you can launch the graphical interface.

Centralized Management: Junos Space Security Director

Junos Space Security Director is a Juniper Networks management platform designed to manage multiple SRX firewalls in a centralized way.

No matter how many SRX devices you have, but certainly if their number is in the hundreds or thousands, you must consider Security Director to simplify provisioning and monitoring tasks. With just a few clicks, you can push changes to the entire network, making what could be considered a complex task something easy to do.

Deployment, configuration, and operation of Junos Space Security Director easily requires another *Day One* book, but there is plenty of documentation and technical training available to teach you what you need to know about this option at the Juniper TechLibrary (https://www.juniper.net/documentation/en_US/release-independent/junos-space-apps/junos-space-security-director.html). Instead, this book simply introduces you to the technology and explains a few basic concepts of the platform.

If you already have Security Director and want to manage your first SRX, you'll need to first configure an IP address and management services into the SRX so that Security Director can discover and manage your firewall, and provided that this IP can be reached from the Junos Space Security Director, you can then import and manage the firewalls.

In terms of limitations, Security Director is not suitable for tasks like debugging (this is an on-box task), but on the other hand, it is a good solution for centralizing security events, viewing logs, analyzing security policies for inconsistencies, monitoring the devices, creating custom IPS and Application signatures, generating reports, pushing configurations to your SRXs, and keeping your network in optimal condition. Be sure to check it out.

Cloud-based Management: Juniper Sky Enterprise

For customers looking for a simple way to deploy and manage Juniper devices, Juniper offers a cloud-based management solution called Sky Enterprise.

As a cloud-based service, Juniper Sky Enterprise eases network administration and costs by eliminating software maintenance cycles and dedicated network management infrastructure. The solution offers a centralized and user-friendly portal that supports features such as Zero Touch Provisioning (ZTP), device configuration, and monitoring.

MORE? For more information about Sky Enterprise see https://juniper.net/us/en/products-services/network-management/sky-enterprise/.

SD-WAN, Security, and NFV Management: Contrail Service Orchestration

Contrail Service Orchestration is a platform designed to manage SRX and NFX devices on networks that demand a high level of adaptiveness for services like SD-WAN and Network Function Virtualization (NFV).

It supports Zero Touch Provisioning, SD-WAN and security services management, and the configuration and deployment of NFV service chaining.

MORE? Get more information about Contrail Service Orchestration at: https://www.juniper.net/us/en/products-services/sdn/contrail/contrail-service-orchestration/.

Connecting to the SRX for the First Time

After unpacking the SRX and physically installing it, you can perform the initial configuration tasks. You can do this using different methods (console port, ZTP, Wizard). This book focuses on using the J-Web Setup Wizard, but provides the initial configuration via CLI so you can connect via the console port.

To Connect to Your SRX Via J-Web

To connect to your SRX via the graphical user interface (J-Web) and perform the setup wizard:

- Connect an Ethernet cable to your computer, and at the other end, to the management port of the SRX;
- Set your interface IP address to 192.168.1.2 and mask to 255.255.255.0;
- Open your web browser (Firefox is recommended);
- Enter the address *https://192.168.1.1*.

NOTE Check your SRX model documentation to find out which port you need to connect in order to access the setup wizard, but it's usually one of the ports between interfaces 0 and 5.

MORE? Specific product information can be found at https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/srx-series/product/index.html and the list of features available per platform is available at https://pathfinder.juniper.net/home/.

If you want to perform the initial configuration using the GUI, you can go straight to Chapter 3, but if you want to use the console port instead, continue on here.

IMPORTANT Note that while this book uses port ge-0/0/0 for the internal network, ge-0/0/1 for the internal servers' network, ge-0.0/2 for DMZ, and ge-0/0/3 for the Internet, depending on your SRX, you may need to use a different combination, as some models use ge-0/0/0 for WAN. Please check your device-specific documentation before proceeding.

To Connect to Your SRX Via Console Port

Connect the provided console cable to your computer, and at the other end, to the port of the SRX. Open your terminal emulation program, such as HyperTerminal in Windows.

In the application, set the port settings (the COM port that identifies the serial connection) with the following information:

- Bits per second: *9600;* Data bits: *8;* Parity: *None*; Stop bits: *1*.
- Flow control: *None*.
- Click Open or Connect (the wording is application dependent).

For MacOS devices, you'll need to get a USB serial adapter, install the proper drivers, and then connect to the SRX with a console cable.

You can use the Terminal application to find the Mac OSX USB port number. See the example below as a reference:

```
macOSX:user$ cd /dev
macOSX:user$ ls -ltr /dev/*usb*
crw-rw-rw- 1 root wheel 10, 66 Jan 2 23:46 tty. USA19H142P1.1
```

After finding the port number, connect to the USB port with the following command, followed by the router USB port speed:

```
macOSX:user$ screen /dev/tty. USA19H142P1.1 9600
```

Assuming that this is a brand new or factory-restored device, you should now have a login prompt.

To Set Up the Initial Information

1. Log in as the *root* user. There is no password.

2. Start the CLI, by typing *cli* at the command prompt.

3. Enter configuration mode.

4. Set the root authentication password by entering a clear text password, an encrypted password, or an SSH public key string (DSA or RSA). The command is (enter the password twice as requested):

```
set system root-authentication plain-text-password
```

5. Commit your configuration.

6. Configure the SRX hostname:

```
set system host-name (name of the device)
```

7. Configure the transit network interfaces:

```
set interfaces interface name unit 0 family inet address (IP address/prefix-length)
```

8. Configure the default route:

```
set routing-options static route 0.0.0.0/0 next-hop (gateway IP)
```

9. Configure basic security zones and bind them to traffic interfaces:

```
set security zones security-zone Trust interfaces ge-0/0/0
set security zones security-zone Internet interfaces ge-0/0/3
```

10. Allow services in the Trust interface:

```
set security zones security-zone Trust interfaces ge-0/0/0.0 host-inbound-traffic system-services all
```

11. Configure basic security policies:

```
set security policies from-zone Trust to-zone Internet policy (policy-name) match source-address any
destination-address any application any
set security policies from-zone Trust to-zone Internet policy (policy-name) then permit
```

12. Create a NAT rule for source translation of all Internet-bound traffic:

```
set security nat source rule-set (ruleset-name) from zone Trust
set security nat source rule-set (ruleset-name) to zone Internet
set security nat source rule-set (ruleset-name) rule (rule-name) match source-address 0.0.0.0/0
destination-address 0.0.0.0/0
set security nat source rule-set (ruleset-name rule (rule-name) then source-nat interface
```

13. Commit the configuration.

Chapter 3

Initial Configuration

As mentioned in Chapter 2, the SRX offers different management methods, and one of the great improvements it achieved is the new J-Web Wizard.

It makes it a lot easier for inexperienced (and even experienced) SRX administrators to quickly set up a new device. It also offers the opportunity for an experienced administrator to set up more complex configurations, right from the start.

This chapter walks you through the setup wizard and how to secure management access of the SRX.

Using the Setup Wizard

The setup wizard configures the services gateway so it can securely pass traffic. The wizard:

- Provides recommended settings based on your previous selections. For example, the wizard recommends security policies based on the security topology you have defined.
- Determines which configuration tasks to present to you based on your selections.
- Flags any missing required configuration when you attempt to leave a page.
- Indicates which configuration elements or tasks are unavailable to you based on your previous selections by graying them out.

You can choose one of the following setup modes to configure the services gateway:

- *Default Setup mode:* This mode allows you to quickly set up a services gateway in a default security configuration. In this mode, you can configure basic system settings, such as the administrator password, and download purchased licenses. Any additional configuration can be carried out after completing the Setup Wizard.
- *Guided Setup mode:* This mode allows you to set up a services gateway in a custom security configuration.

The following screen will appear:

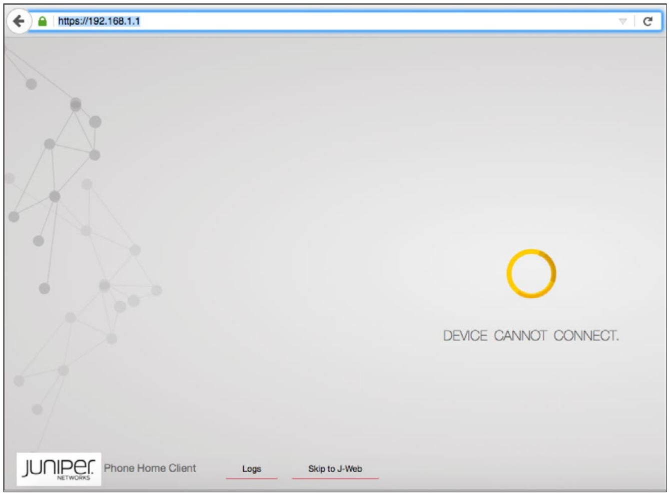


Figure 3.1 *Phone Home Client Initial Wizard*

The screen displays the message *Device Cannot Connect*. This is because the SRX is trying to reach the Phone Home Server (part of the ZTP setup process). As we are not using ZTP as a setup method on this book, just click on *Skip to J-Web*.

Now, just define the root password to continue:

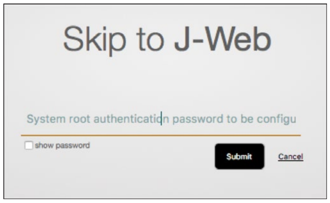
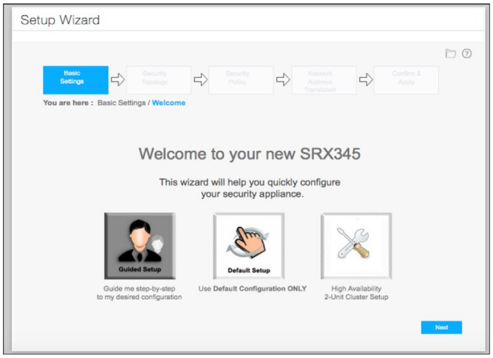


Figure 3.2 *Root Password Configuration*

After a few seconds, reload the browser. You will be prompted with the J-Web login screen. Type your username and password (user: *root* password: *defined in the previous step*). After logging in, you will be presented with the setup wizard screen in Figure 3.3.

Basic Settings



Setup Wizard

You are here : Basic Settings / Welcome

Welcome to your new SRX345

This wizard will help you quickly configure your security appliance.

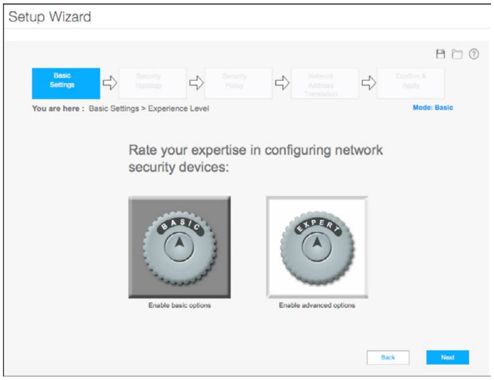
Guide me step-by-step to my desired configuration

Use Default Configuration ONLY

High Availability 2-Unit Cluster Setup

Figure 3.3 *Setup Wizard Initial Screen*

Click on *Guided Setup* and then, click on Next. The wizard will ask for your experience level as shown in Figure 3.4. For now, let's start with the Basic Options. Select and then click on Next:



Setup Wizard

You are here : Basic Settings > Experience Level

Mode: Basic

Rate your expertise in configuring network security devices:

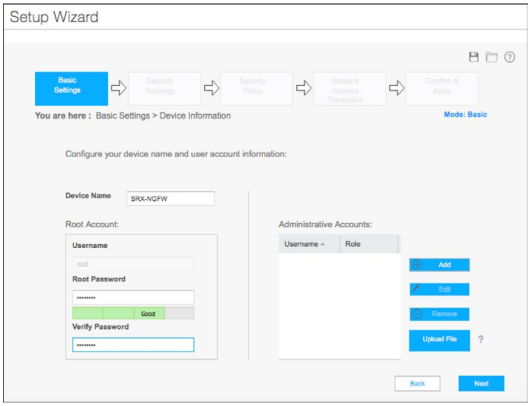
Enable basic options

Enable advanced options

Figure 3.4 *Setup Modes*

NOTE Expert Mode allows the administrator to define additional zones and offers more advanced configurations during the setup. It allows the configuration of more complex scenarios, but it's recommended only for advanced administrators. Try it out in the lab.

Next, let's define the SRX hostname, the root password, and other administrative accounts, as needed, as shown in Figure 3.5:



You are here : Basic Settings > Device Information

Mode: Basic

Configure your device name and user account information:

Device Name: SRX-NGFW

Root Account:

Username: root

Root Password: ••••••••• Good

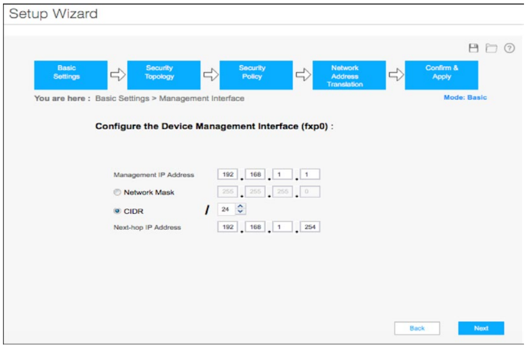
Verify Password: •••••••••

Administrative Accounts:

Username	Role

Figure 3.5 *User Settings*

Configure the out-of-band management interface (fxp0), IP address, and subnet, and click on Next:



You are here : Basic Settings > Management Interface

Mode: Basic

Configure the Device Management Interface (fxp0) :

Management IP Address 192 . 168 . 1 . 1

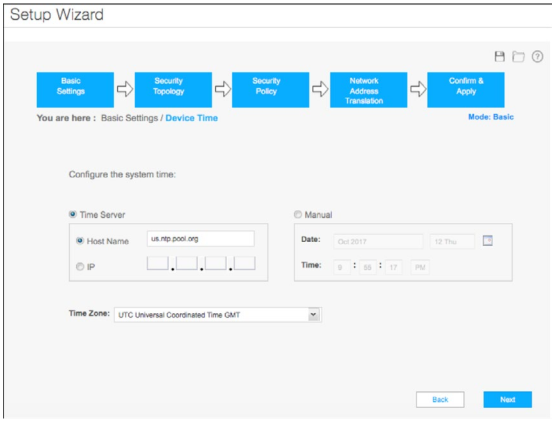
○ Network Mask 255 . 255 . 255 . 0

● CIDR / 24

Next-hop IP Address 192 . 168 . 1 . 254

Figure 3.6 *Management Interface (fxp0) Settings*

Next, configure the NTP Server and time zone:



You are here : Basic Settings / Device Time

Configure the system time:

● Time Server

● Host Name us.ntp.pool.org

○ IP . . .

○ Manual

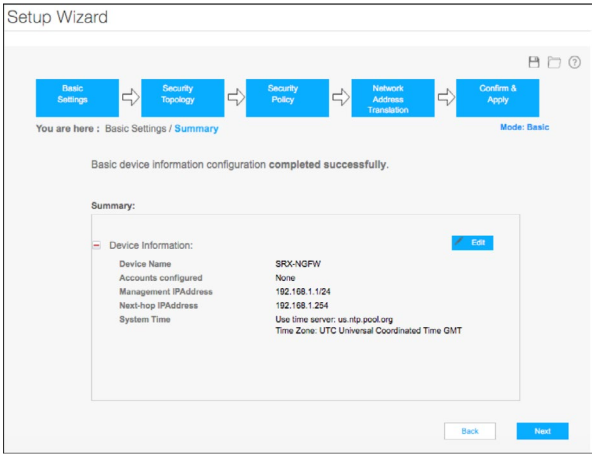
Date: Oct 2017 12 Thu

Time: 9 : 55 : 17 PM

Time Zone: UTC Universal Coordinated Time GMT

Figure 3.7 *Time/Date Settings*

The setup wizard will summarize this part of the configuration. If all is correct, click Next:



You are here : Basic Settings / Summary

Basic device information configuration **completed successfully.**

Summary:

Device Information:

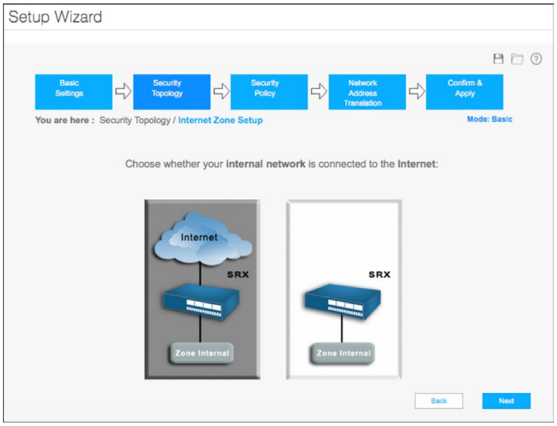
Device Name	SRX-NGFW
Accounts configured	None
Management IPAddress	192.168.1.1/24
Next-hop IPAddress	192.168.1.254
System Time	Use time server: us.ntp.pool.org Time Zone: UTC Universal Coordinated Time GMT

Figure 3.8 *Basic Device Settings Review*

Security Topology

The next part of the configuration is about defining the security topology.

In Figure 3.9, select the Zone Internal and Internet setup and click Next:

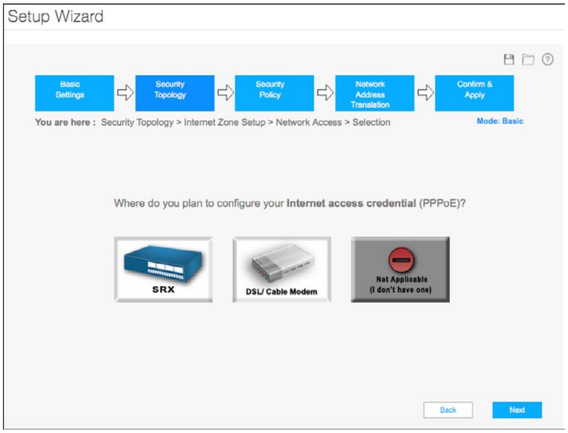


You are here : Security Topology / Internet Zone Setup

Choose whether your internal network is connected to the Internet:

Figure 3.9 *Security Topology Definition*

If you use PPoE in your lab or in your Internet connection, you can define it here. If you don't use it, just select the Not Applicable option as shown here. And then Next:



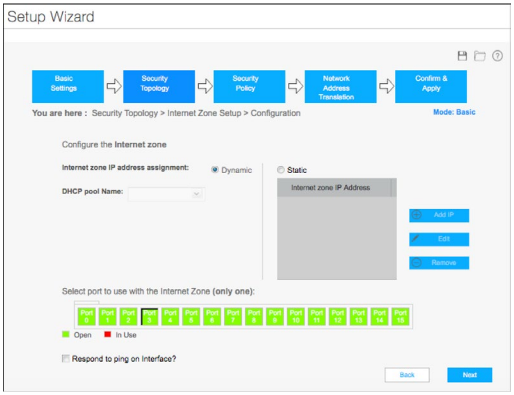
You are here : Security Topology > Internet Zone Setup > Network Access > Selection

Where do you plan to configure your Internet access credential (PPPoE)?

Figure 3.10 *Internet Credentials Configuration*

Let's define the Internet interface properties. Select one interface and configure the interface properties.

Here, the book is using interface 3 and defining it as a DHCP client interface. If your Internet interface uses a static IP, remember to reflect this in your configuration. When complete click Next:



Setup Wizard

You are here : Security Topology > Internet Zone Setup > Configuration

Mode: Basic

Configure the **Internet zone**

Internet zone IP address assignment: ● Dynamic ○ Static

DHCP pool Name:

Internet zone IP Address

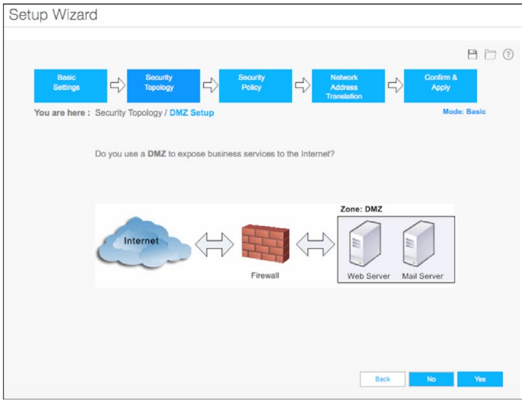
Select port to use with the Internet Zone **(only one)**:

🟩 Open 🟥 In Use

□ Respond to ping on Interface?

Figure 3.11 *Internet Zone Definition*

In the next step, the setup wizard asks if the administrator wants to define a DMZ. If you're following this book's reference topology, click Yes. If you're configuring a two-zone set up (Trust/Internet), just click No and skip the DMZ steps:



Setup Wizard

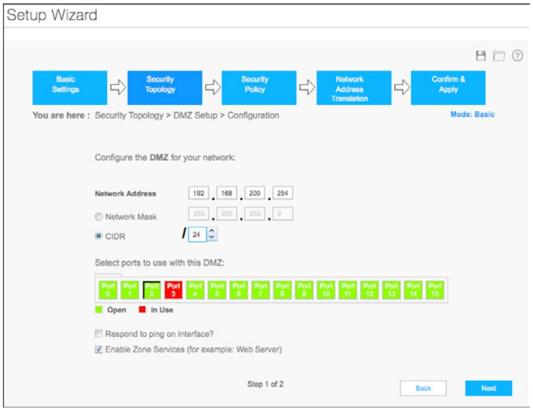
You are here : Security Topology / **DMZ Setup**

Mode: Basic

Do you use a **DMZ** to expose business services to the Internet?

Figure 3.12 *DMZ Zone Definition*

Let's define the DMZ interface properties. In Figure 3.13 select the interface you want to use for the DMZ zone. Here, we're using interface 2:



You are here : Security Topology > DMZ Setup > Configuration

Mode: Basic

Configure the **DMZ** for your network:

Network Address 192 . 168 . 200 . 254

○ Network Mask 255 . 255 . 255 . 0

● CIDR / 24

Select ports to use with this DMZ:

Port 0 · Port 1 · Port 2 · Port 3 · Port 4 · Port 5 · Port 6 · Port 7 · Port 8 · Port 9 · Port 10 · Port 11 · Port 12 · Port 13 · Port 14 · Port 15

🟩 Open 🟥 In Use

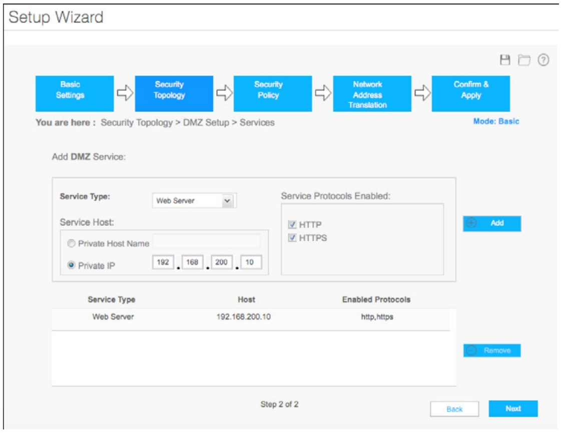
□ Respond to ping on Interface?

☑ Enable Zone Services (for example: Web Server)

Step 1 of 2

Figure 3.13 DMZ Zone Interface Configuration

The next step is to set up the services available in the DMZ zone. The setup wizard offers a couple of predefined templates, so let's use the web service template. After inserting the private server IP address and the services available, click on Add, and then Next:



You are here : Security Topology > DMZ Setup > Services

Mode: Basic

Add **DMZ** Service:

Service Type: Web Server

Service Host:

○ Private Host Name

● Private IP 192 . 168 . 200 . 10

Service Protocols Enabled:

☑ HTTP

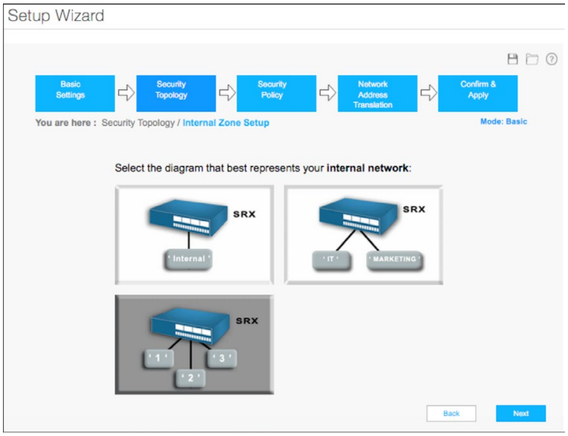
☑ HTTPS

Service Type	Host	Enabled Protocols
Web Server	192.168.200.10	http,https

Step 2 of 2

Figure 3.14 DMZ Services Definition

Next the setup wizard asks for the internal network topology. Select the 3x zone setup and click Next as shown in Figure 3.15:



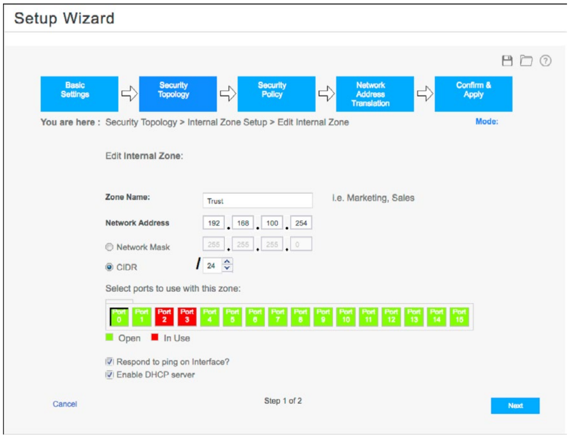
You are here : Security Topology / Internal Zone Setup

Mode: Basic

Select the diagram that best represents your **internal network**:

Figure 3.15 Internal Zone Setup

It’s time to define the Trust interface. Select Interface 0 for the Trust Zone and configure the interface properties:



You are here : Security Topology > Internal Zone Setup > Edit Internal Zone

Mode:

Edit **Internal Zone**:

Zone Name: Trust   I.e. Marketing, Sales

Network Address 192 . 168 . 100 . 254

○ Network Mask 255 . 255 . 255 . 0

● CIDR / 24

Select ports to use with this zone:

🟩 Open 🟥 In Use

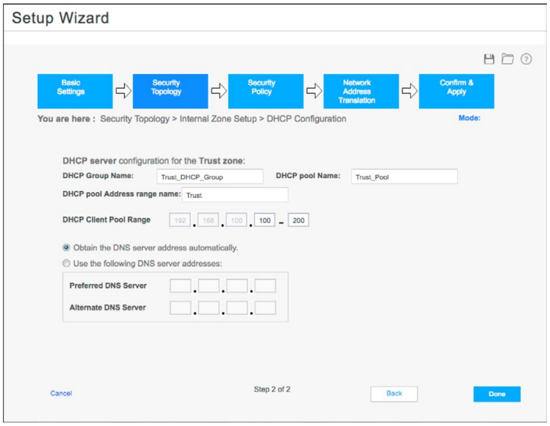
☑ Respond to ping on Interface?

☑ Enable DHCP server

Step 1 of 2

Figure 3.16 Internal Zone (Trust) Configuration

Next configure the DHCP Server properties and insert the values that fit for your own lab or network environment. If you're not using DHCP server in the SRX, just skip this step:


Setup Wizard

You are here : Security Topology > Internal Zone Setup > DHCP Configuration

Mode:

DHCP server configuration for the Trust zone:

DHCP Group Name: Trust_DHCP_Group

DHCP pool Name: Trust_Pool

DHCP pool Address range name: Trust

DHCP Client Pool Range 192 . 168 . 100 . 100 - 200

● Obtain the DNS server address automatically.

○ Use the following DNS server addresses:

Preferred DNS Server . . .

Alternate DNS Server . . .

Figure 3.17 *DHCP Server Configuration*

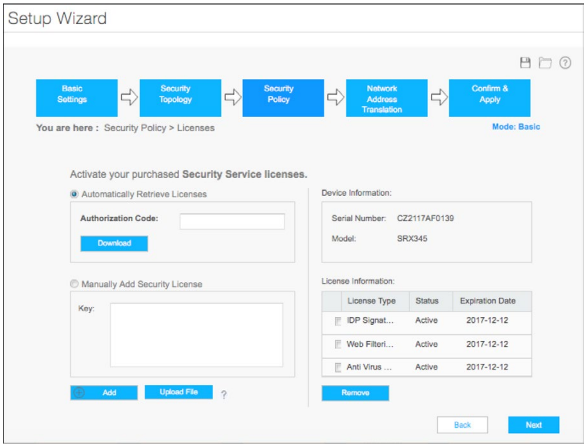
NOTE For this environment, this book uses the IP address 8.8.8.8 as the initially preferred DNS server for the DHCP clients, but you can use your internal DNS server, your ISP DNS server, or any other DNS server you trust and have access to. It's important to mention that the SRX supports the DNS Proxy feature, but won't be taking advantage of it in this book, as it doesn't reflect the majority of deployments.

After the DHCP step is done, the setup wizard will move to the Security Policy portion of the configuration, as evident by the "You are here" process chart at the top of the setup wizard.

Security

First, let's insert the security licenses. You can upload the security file or add the specific licenses manually as shown in Figure 3.18.

TIP If have purchased a license but didn't receive it, contact your Juniper representative or account manager.



Setup Wizard

You are here : Security Policy > Licenses

Mode: Basic

Activate your purchased **Security Service licenses.**

● Automatically Retrieve Licenses

Authorization Code:

○ Manually Add Security License

Key:

Device Information:

Serial Number: CZ2117AF0139

Model: SRX345

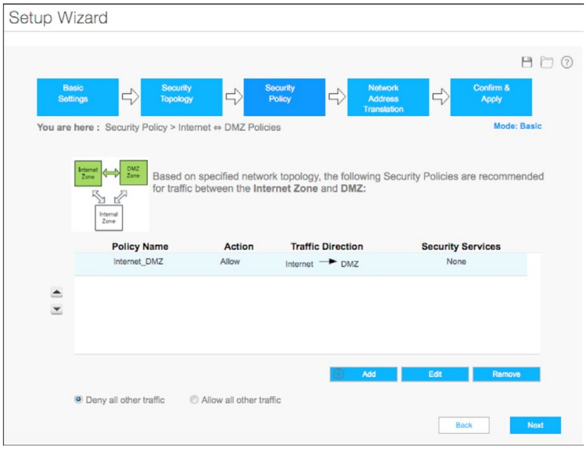
License Information:

	License Type	Status	Expiration Date
□	IDP Signat...	Active	2017-12-12
□	Web Filteri...	Active	2017-12-12
□	Anti Virus ...	Active	2017-12-12

Figure 3.18 License Upload

TIP You may face errors when loading the full license file and this may be caused by having licenses in the file that are not recognized by the system, as they are not supposed to be uploaded. If this happens, just load the licenses individually instead of doing a full bulk load.

The next step is to configure the security policies that will allow or deny communication between the zones. The first policy is to set up the policy from Internet to DMZ. Rename the policy to be meaningful to your environment, accept the default policy, and then click Next (you'll revisit this policy in subsequent chapters):



Setup Wizard

You are here : Security Policy > Internet ⇔ DMZ Policies

Mode: Basic

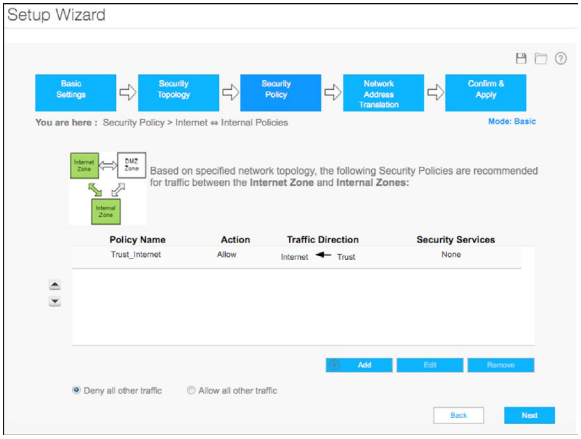
Based on specified network topology, the following Security Policies are recommended for traffic between the **Internet Zone** and **DMZ:**

Policy Name	Action	Traffic Direction	Security Services
Internet_DMZ	Allow	Internet → DMZ	None

● Deny all other traffic ○ Allow all other traffic

Figure 3.19 Internet –> DMZ Security Policy

The next policy is for the Trust zone to Internet. Accept the policy and click Next:



Setup Wizard

You are here : Security Policy > Internet ⇔ Internal Policies

Mode: Basic

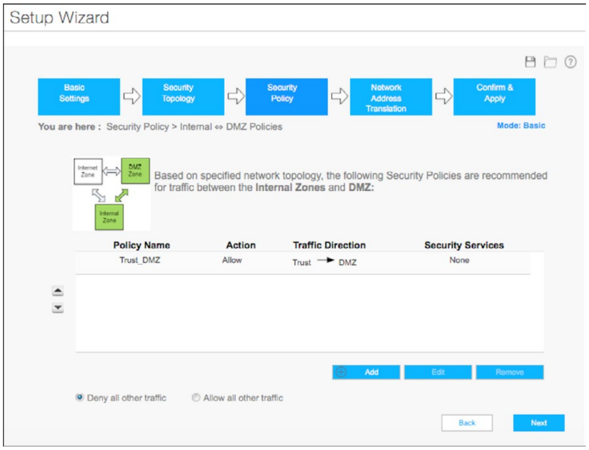
Based on specified network topology, the following Security Policies are recommended for traffic between the **Internet Zone** and **Internal Zones:**

Policy Name	Action	Traffic Direction	Security Services
Trust_Internet	Allow	Internet ← Trust	None

● Deny all other traffic ○ Allow all other traffic

Figure 3.20 *Trust –> Internet Security Policy*

Do the same for the Trust to DMZ policy:



Setup Wizard

You are here : Security Policy > Internal ⇔ DMZ Policies

Mode: Basic

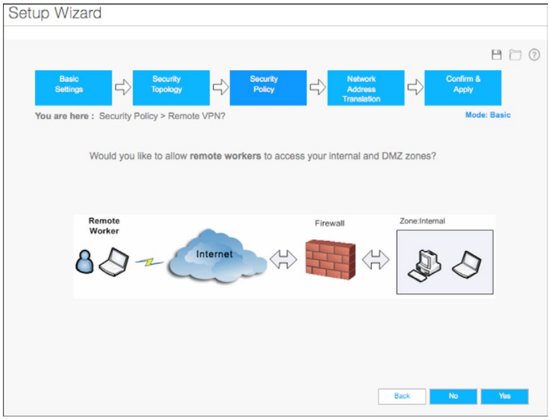
Based on specified network topology, the following Security Policies are recommended for traffic between the **Internal Zones** and **DMZ:**

Policy Name	Action	Traffic Direction	Security Services
Trust_DMZ	Allow	Trust → DMZ	None

● Deny all other traffic ○ Allow all other traffic

Figure 3.21 *Trust –> DMZ Security Policy*

The Setup Wizard will move to set up the Remote Access VPN. Let's skip this step for right now, as Remote Access is covered in a later chapter. Just click No:


Setup Wizard

You are here : Security Policy > Remote VPN?

Mode: Basic

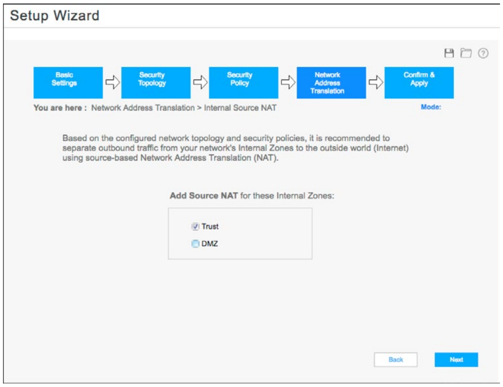
Would you like to allow **remote workers** to access your internal and DMZ zones?

Figure 3.22 *Remote Access VPN Configuration – Save for Later*

NAT

Okay let's move to the NAT portion of the configuration. The setup wizard helps to set up the necessary NAT policies in order to let some basic services be available for Internet users.

Let's create a Source NAT policy that will allow internal clients to access the Internet, and a Destination NAT to allow external clients to access DMZ Services. Select all the zones where Source NAT is necessary. In this book's environment, because we initially just want the clients in the Trust to have Internet access, let's select only the Trust Zone, but if you want to have Internet access from your DMZ servers, remember to add the DMZ zone here:


Setup Wizard

You are here : Network Address Translation > Internal Source NAT

Mode:

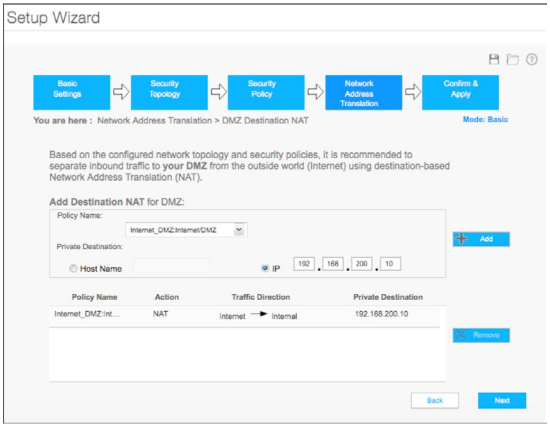
Based on the configured network topology and security policies, it is recommended to separate outbound traffic from your network's Internal Zones to the outside world (Internet) using source-based Network Address Translation (NAT).

Add Source NAT for these Internal Zones:

☑ Trust
□ DMZ

Figure 3.23 *Source NAT Configuration*

To configure Destination NAT, select the IP address or hostname (if internal DNS is configured) of the DMZ server and the security policy that is related to this NAT policy:



Setup Wizard

You are here : Network Address Translation > DMZ Destination NAT

Mode: Basic

Based on the configured network topology and security policies, it is recommended to separate inbound traffic to **your DMZ** from the outside world (Internet) using destination-based Network Address Translation (NAT).

Add Destination NAT for DMZ:

Policy Name: Internet_DMZ:Internet/DMZ

Private Destination:

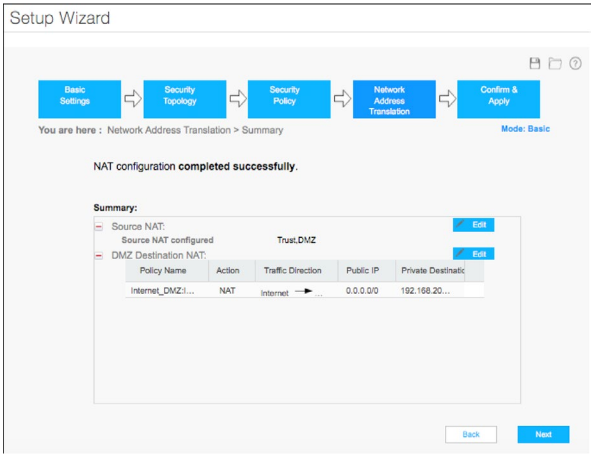
○ Host Name ● IP 192 . 168 . 200 . 10

Policy Name	Action	Traffic Direction	Private Destination
Internet_DMZ:Int...	NAT	Internet → Internal	192.168.200.10

Figure 3.24 Destination NAT Configuration

NOTE If you are creating multiple destination NAT policies for different servers in your DMZ, make sure you are matching them with the security policies matching the NAT traffic.

Review the configurations in Figure 3.25 and click Next:



Setup Wizard

You are here : Network Address Translation > Summary

Mode: Basic

NAT configuration **completed successfully**.

Summary:

− Source NAT:

Source NAT configured Trust,DMZ

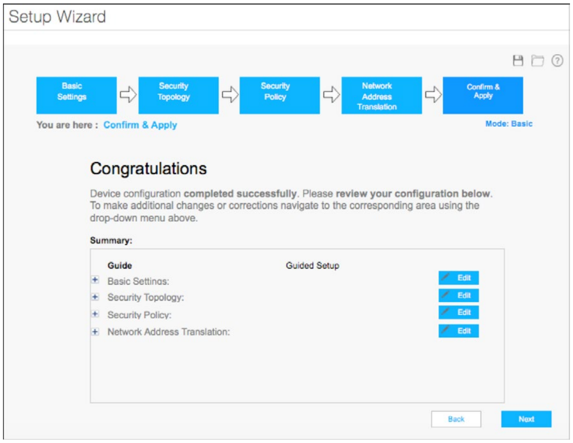
− DMZ Destination NAT:

Policy Name	Action	Traffic Direction	Public IP	Private Destinatic
Internet_DMZ:I...	NAT	Internet → ...	0.0.0.0/0	192.168.20...

Figure 3.25 NAT Configuration Review

Confirm and Apply

The setup wizard will allow you to review the configuration before proceeding, if you are ready to commit to your actual configuration, click Next:



Congratulations

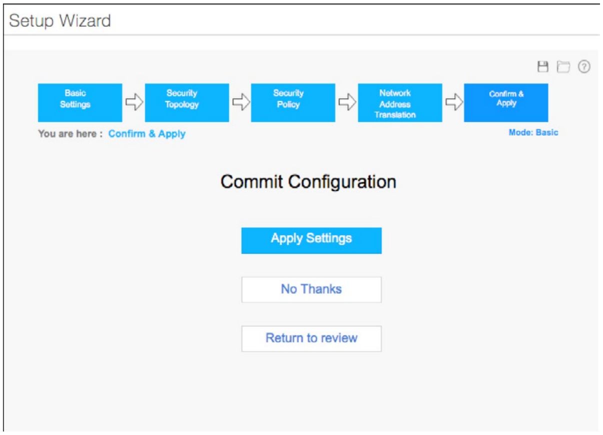
Device configuration **completed successfully**. Please **review your configuration below**. To make additional changes or corrections navigate to the corresponding area using the drop-down menu above.

Summary:

Guide	Guided Setup
+ Basic Settings:	
+ Security Topology:	
+ Security Policy:	
+ Network Address Translation:	

Figure 3.26 *Configuration Review*

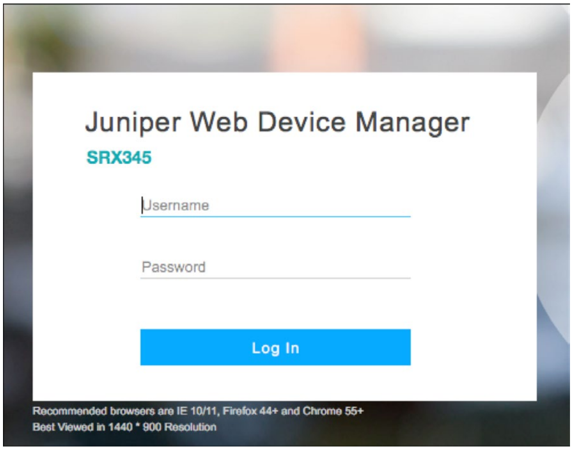
It’s time to commit. Click Apply Settings:



Commit Configuration

Figure 3.27 *Apply Configuration Settings*

After the commit is done, you'll be presented to the WebUI Log In screen (reload your browser, if needed):



Juniper Web Device Manager

SRX345

Username

Password

Recommended browsers are IE 10/11, Firefox 44+ and Chrome 55+
Best Viewed in 1440 * 900 Resolution

Figure 3.28 J-Web Log In Screen

During the setup, we configured a default route for the fxp0 interface and this may conflict with the SRX routes. You need to remove the static route created.

On the CLI, type the following command in configuration mode:

```
delete routing-options static route 0.0.0.0/0
```

Commit the change.

WARNING Depending on how your SRX receives the default route, you may need to manually add another one. You can achieve this on both CLI and GUI (Configuration/Network/Static Routing). If your SRX receives routes or default gateway via DHCP or a dynamic routing protocol, you won't need it.

Congratulations! Now your SRX is functional.

NOTE At this moment, your SRX should be allowing users to connect to the Internet and the servers on the DMZ should be reachable for both internal and external users. If something is not working, please review your configuration.

The following chapters will focus on enabling advanced security features to further enhance the security posture of your network. Let's do it.

Overview of the Graphical User Interface

The new J-Web is divided into five main categories (Dashboard, Monitor, Configure, Reports, and Administration), as you can see in Figure 3.29:

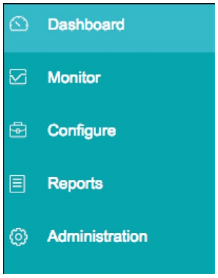
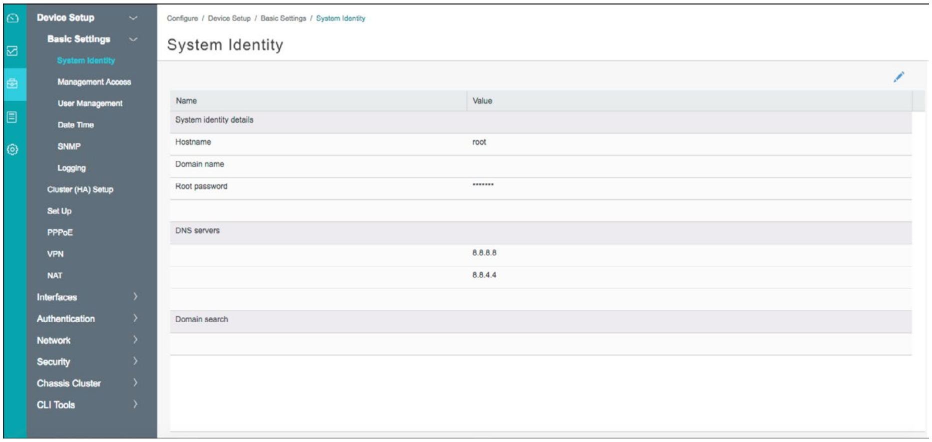


Figure 3.29 J-Web Main Categories Panel

You can access the Menu by moving your mouse to the left at any given time. This allows a fast and easy way to view logs, configure your SRX, generate reports, or perform administrative tasks.

After logging in you will be presented with the Systems Identity page (Figure 3.30) where you can define device information and other basic aspects of your setup, for now, let's just click on the Dashboard icon:



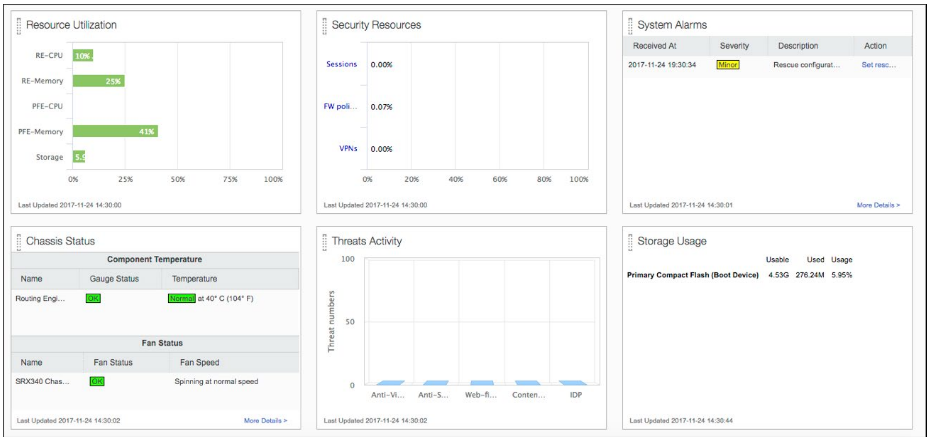
Configure / Device Setup / Basic Settings / System Identity

System Identity

Name	Value
System identity details	
Hostname	root
Domain name	
Root password	*******
DNS servers	
	8.8.8.8
	8.8.4.4
Domain search	

Figure 3.30 System Identity

The Dashboard allows you to quickly visualize important information about your device performance, health, status, and security posture:



Resource Utilization

Last Updated 2017-11-24 14:30:00

Security Resources

Last Updated 2017-11-24 14:30:00

System Alarms

Received At	Severity	Description	Action
2017-11-24 19:30:34	Minor	Rescue configurat…	Set resc…

Last Updated 2017-11-24 14:30:01 More Details >

Chassis Status

Component Temperature		
Name	Gauge Status	Temperature
Routing Engi…	OK	Normal at 40° C (104° F)

Fan Status		
Name	Fan Status	Fan Speed
SRX340 Chas…	OK	Spinning at normal speed

Last Updated 2017-11-24 14:30:02 More Details >

Threats Activity

Last Updated 2017-11-24 14:30:02

Storage Usage

	Usable	Used	Usage
Primary Compact Flash (Boot Device)	4.53G	276.24M	5.95%

Last Updated 2017-11-24 14:30:44

Figure 3.31 Dashboard

You can also select the widgets you want to be displayed. Just click on the gear icon, located on the upper right hand of the screen.

NOTE This book highly recommends you become familiar with the Dashboard and its options so you can profit from the valuable information provided in a quick and graphical way.

Every time you change something in the SRX, you need to commit your changes, so it can start taking effect – just click the Commit button in the upper right of the setup wizard page.

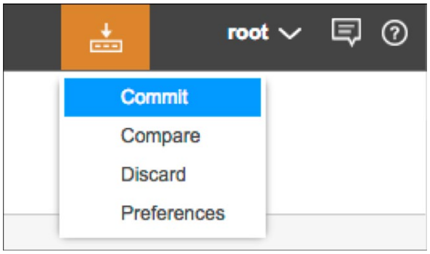


Figure 3.32 Commit Button

You can perform several changes before doing the commit and you can also Compare and Discard changes via the pull-down menu – it's really useful.

Now let's look into ways to increase the security of the SRX itself.

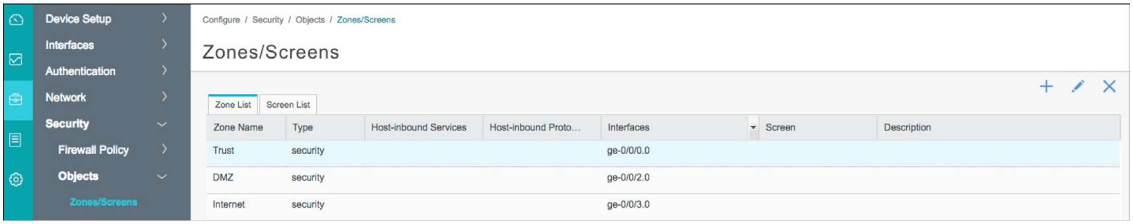
Securing Management Access

It’s always a best practice to restrict admin access to any network device and this is even more critical to security devices. Leaving management access unrestricted will welcome malicious users or attackers to disrupt your network.

A great way of hardening the SRX is using the fxp0 interface to perform any management tasks, as this interface is out-of-band (cannot be accessed from the transit network), although this isn’t an option for every single company or environment, and sometimes, administrators use transit networks for management.

The next steps show you how to enable management over a transit port and how to secure it against unauthorized access.

On the Configure tab, click on Security/Objects/Zones/Screens, then select the Trust Zone and click on Edit:



Zones/Screens

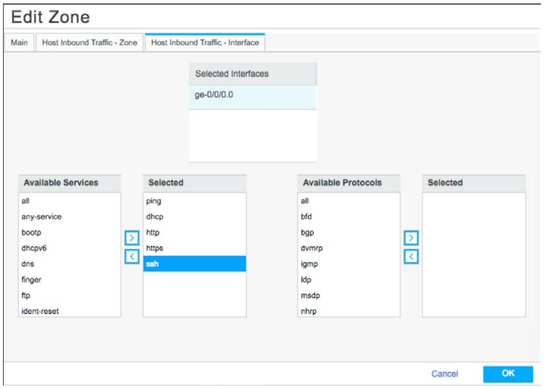
Zone Name	Type	Host-inbound Services	Host-inbound Proto...	Interfaces	Screen	Description
Trust	security			ge-0/0/0.0		
DMZ	security			ge-0/0/2.0		
Internet	security			ge-0/0/3.0		

Figure 3.33 Zones/Screens Panel

Under Edit Zone, select the Host Inbound Traffic – Interface tab, select the interface you want to use for management, and then enable the relevant services for your lab or environment.

NOTE This book recommends enabling SSH, ping, and HTTPS for management in the Trust Zone, not for other zones, and only for the absolutely necessary services and protocols. It also does not recommend enabling protocols such as SSH, HTTP, and HTTPS on interfaces connected to public networks.

TIP If you are using the SRX as a DHCP Server, make sure DHCP remains *allowed* only on the proper interfaces or zones.



Selected Interfaces: ge-0/0/0.0

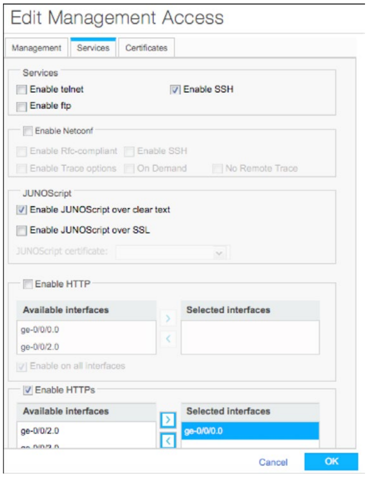
Available Services	Selected	Available Protocols	Selected
all	ping	all	
any-service	dhcp	bfd	
bootp	http	bgp	
dhcpv6	https	dvmrp	
dns	ssh	igmp	
finger		ldp	
ftp		msdp	
ident-reset		nhrp	

Figure 3.34 Zone Services and Protocols Configuration

NOTE You can also restrict the IP addresses or user IDs allowed to access the management IP. You can use firewall filters or security policies.

It's also very important to make sure you disabled all unnecessary services. You can do that by clicking on Configure/Device Setup/Basic Settings/Management Access.

Click on Edit and select the Services tab:



Services
□ Enable telnet ☑ Enable SSH
□ Enable ftp

□ Enable Netconf
□ Enable Rfc-compliant □ Enable SSH
□ Enable Trace options □ On Demand □ No Remote Trace

JUNOScript
☑ Enable JUNOScript over clear text
□ Enable JUNOScript over SSL
JUNOScript certificate:

□ Enable HTTP

Available interfaces	Selected interfaces
ge-0/0/0.0	
ge-0/0/2.0	

☑ Enable on all interfaces

☑ Enable HTTPs

Available interfaces	Selected interfaces
ge-0/0/2.0	ge-0/0/0.0

Figure 3.35 Management Access Panel

This book recommends that you at least deactivate the Telnet service, and on the Enable HTTPS section, disable the Enable on all interfaces option. Select the Trust zone interface under Available interfaces and move it to the Selected interfaces tab – this will restrict web-based management access to the interface connected to the Trust Zone.

Click OK.

Last, under Configure/interfaces, select the fxp0 interface, and Deactivate it (as we won't be using the MGMT interface).

Commit your configuration by using the Commit menu pulldown, as shown previously in Figure 3.32.

Chapter 4

Security Policies

Security policies are a critical component of the SRX Services Gateway platform. By default, traffic entering an interface destined to any address is going to be blocked. This is the expected default behavior and no traffic is allowed through the SRX until a proper configuration is in place to permit it.

NOTE An exception to this traffic rule is the traffic in and out of the fxp0 (management) interface. As the fxp0 interface (MGMT) resides in the control plane of the device, it cannot be used for user data traffic. Also, some SRX models come with a 'trust-to-untrust-allow' policy created by default.

Security Policies Logic

Policy configuration entitles an IF-THEN-ELSE algorithm: IF traffic X is matched, THEN action Y is performed, ELSE drop packet (default behavior).

Matching traffic (IF statement) consists of looking at packets for the four following elements:

- Source zone: the predefined or custom zone created from the perspective of the SRX that you are configuring. The source selected has to match the source zone.
- Destination zone: predefined or custom zone created from the perspective of the SRX that you are configuring.
- Destination IP: any IP address, or address book, that specifies a host IP or a subnet. The destination selected has to match the destination zone.
- Application: predefined or custom service that defines the source/ destination ports, protocol involved, and timeout value.

If an incoming packet matches all previous four elements, the action (THEN statement) defines what to do with this or any other packets matching the same combination:

- Deny: drops the packet (silently).
- Reject: drops the packet and sends a TCP-Reset to the originator of the traffic.
- Permit: permits the packet.
- Log: instructs the SRX to create a log entry for matching packets.
- Count: provides accounting information per session.

You can imagine environments where there can be several—or up to dozens or thousands of policies configured in a SRX device (this number varies by platform). When packets ingress the SRX, they are evaluated against security policies in a top-down fashion until all five of the elements presented above are matched. If a match is found, then the SRX does what it was instructed to do with those packets and stops evaluating through the rest of the policies. If the evaluation process reaches the last policy, and no match was made (ELSE statement), then the default firewall action `deny-all` is applied.

Since the evaluation of firewall policies happens sequentially in a top-down manner, it is a good practice to insert the most specific rules at the top of the list and the most generic policies at the bottom. If you fail to do so, then you may hide a more specific match criteria with a more common one.

MORE? Junos Space Security Director has a feature called Policy Analysis Report that helps administrators to find shadowed, not active, redundant, schedule expired, and never matched policies. This offers a great deal of help to administrators trying to reduce and sanitize their security policy database. See https://www.juniper.net/documentation/en_US/junos-space17.2/topics/task/configuration/junos-space-policy-analysis-report-definition-creating.html.

Security Policies Components

As mentioned, a security policy has several components, such as zones, address books, and applications. Let's quickly review.

A *zone* is a logical container used to group interfaces with similar security requirements. For example, assume your organization has a Human Resources department, so all firewall ports assigned to HR can be bound to the zone HR. All firewall interfaces used by Finance can be bound to a zone Finance, and so on. Zone names are locally significant and you can name them anything that makes the most sense to you.

An *address book* is a collection of addresses. The SRX allows you to configure multiple address books. Address books are objects that may contain network addresses (IPv4 and IPv6), network prefixes, wildcards, and hostnames. You can think of an address book as a building block that is referenced in other configurations such as security policies or NAT, and is used to match source and destination IP addresses.

You can add addresses to address books or use the predefined addresses available to each address book by default.

NOTE It's best practice to keep the address object management simple, using the global address book or zone address books, but not mixing them.

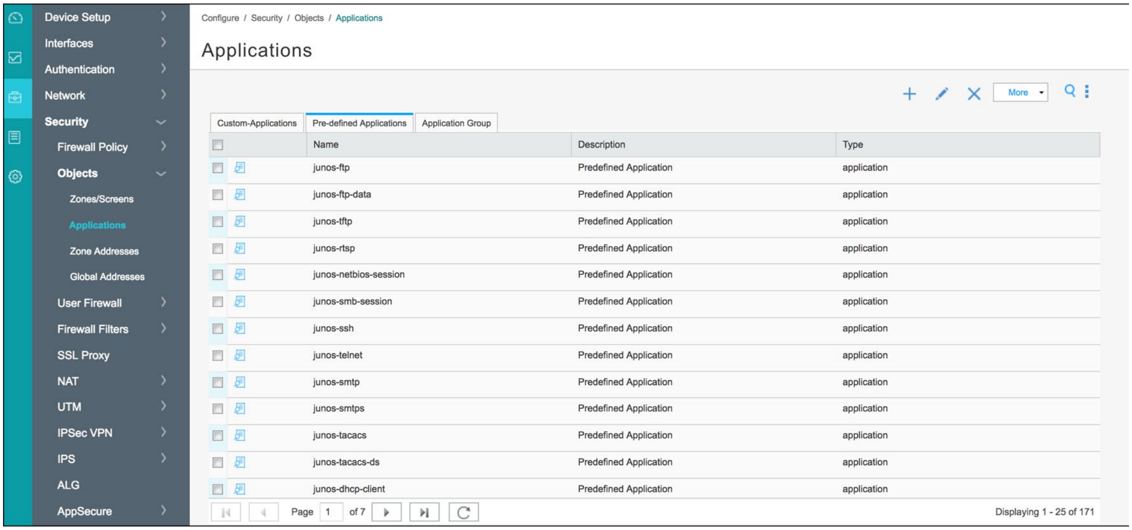
Applications refer to the specific services that a policy is matching. An application can be a combination of source or destination ports, protocols, and its timeout. The ports and protocol are part of the TCP/IP packet header, and the timeout refers to the time that a particular packet will be held in memory before it is purged, if no subsequent packets match the same security policy.

As discussed earlier, the SRX is a stateful firewall. When an incoming packet is matched and an action is taken, then an entry identifying this packet and the corresponding action is held in memory (session table) so that subsequent packets are processed faster. If, after a while (the timeout value), no subsequent packets match the same criteria, the entry is purged from memory. A finite amount of entries can be held in memory and that's why the firewall has to be judicious about what is held there.

You don't always have to configure services. In fact, there is a list of pre-defined services, and you can see their details from configuration mode with the CLI command:

```
[edit]
root@root# show groups junos-defaults applications
```

You can also have the same visualization in the Web GUI, by navigating to the Configure/Security/Objects/Applications page and selecting the pre-defined Applications tab as shown in Figure 4.1:



Name	Description	Type
junos-ftp	Predefined Application	application
junos-ftp-data	Predefined Application	application
junos-tftp	Predefined Application	application
junos-rtsp	Predefined Application	application
junos-netbios-session	Predefined Application	application
junos-smb-session	Predefined Application	application
junos-ssh	Predefined Application	application
junos-telnet	Predefined Application	application
junos-smtp	Predefined Application	application
junos-smtps	Predefined Application	application
junos-tacacs	Predefined Application	application
junos-tacacs-ds	Predefined Application	application
junos-dhcp-client	Predefined Application	application

Figure 4.1 *Zone Services and Protocols Configuration*

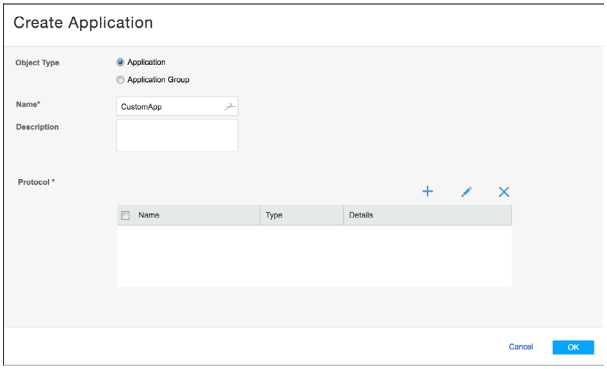
In a situation where you need to create a service to accommodate a particular application in your network, then the process is to gather up the ports and protocols involved, consider the service timeout, make a decision about what it is, and configure a new service.

For example, let's assume you want to configure a custom service called *Custom-App* to accommodate traffic that matches the following criteria:

- Source ports: *any*
- Destination port: *10000*
- Protocol: *TCP*
- Timeout: *360 seconds*

In order to achieve this, click the + sign on the Configure/Security/Objects/Applications page and select the Custom-Applications tab (the first tab shown in Figure 4.1).

Click on the + button and the Create Application page will appear as shown in Figure 4.2:



Create Application

Object Type ● Application
○ Application Group

Name* CustomApp

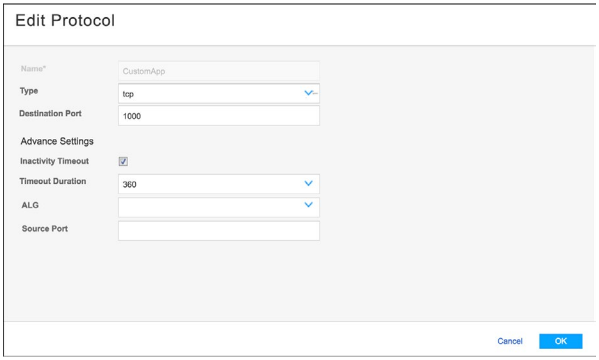
Description

Protocol *

□ Name	Type	Details

Figure 4.2 *Create a Custom Application Screen*

Name the application *CustomApp*. You will notice that an application is made of protocols. Protocols can be a combination of source and destination ports, protocols (UDP, TCP), the timeout, and Application Layer Gateways. Click on the + button and the Edit Protocol window appears:



Edit Protocol

Name* CustomApp

Type tcp

Destination Port 1000

Advance Settings

Inactivity Timeout ☑

Timeout Duration 360

ALG

Source Port

Figure 4.3 *Zone Services and Protocol Configuration*

Just input the values defined for the CustomApp. Click OK and commit your changes.

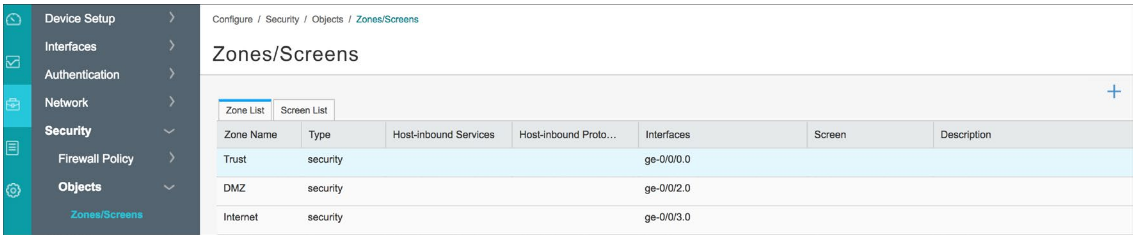
TIP An application can contain several protocols, which is a powerful feature as administrators don't need to set up different protocols and add them into a policy. They can simply add all the protocols within an application and use the application inside a security policy.

Creating Interfaces, Security Zones, Addresses, and Policies

Looking back at this book's topology, you might remember that we didn't create one of the security zones during the Initial Setup (Server Zone). This was on purpose. So now, let's manually create it and its related security policies, interfaces, and objects.

First, let's configure the security zone.

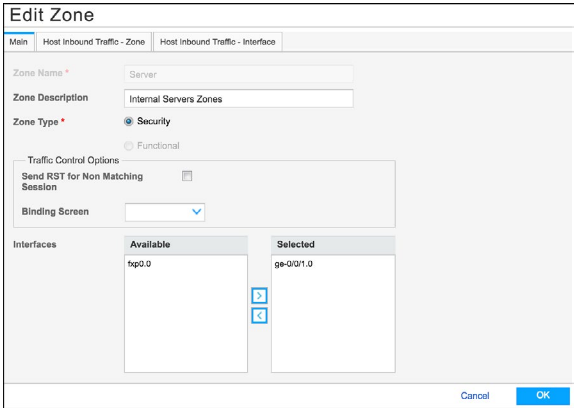
In the J-Web GUI, navigate to Configure/Security/Objects/Zones/Screens as shown in Figure 4.4:



Zone Name	Type	Host-inbound Services	Host-inbound Proto...	Interfaces	Screen	Description
Trust	security			ge-0/0/0.0		
DMZ	security			ge-0/0/2.0		
Internet	security			ge-0/0/3.0		

Figure 4.4 Zone Services and Screens

Click on the + button. In the Edit Zone page, create a new Security Type Zone called *Server*. Do not bind a SCREEN to policy to the new zone. Let it be empty in the interfaces tab for now:



Zone Name * Server

Zone Description Internal Servers Zones

Zone Type * ● Security ○ Functional

Traffic Control Options

Send RST for Non Matching Session □

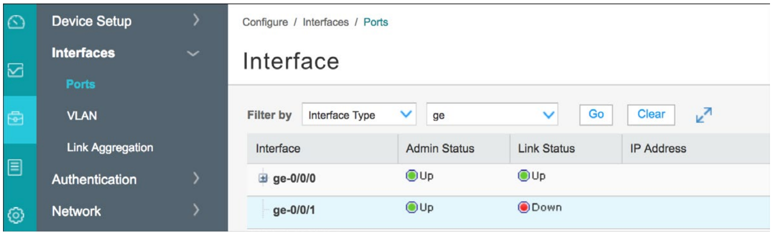
Binding Screen

Interfaces

Available	Selected
fxp0.0	ge-0/0/1.0

Figure 4.5 Zone Configuration

The next step is to create a new network interface. In the J-Web GUI, navigate to Configure/Interfaces/Ports:



Interface	Admin Status	Link Status	IP Address
ge-0/0/0	● Up	● Up	
ge-0/0/1	● Up	● Down	

Figure 4.6 Interface Configuration

Select the ge-0/0/1 interface and click on the + button, then select the Logical Interface option as shown in Figure 4.7:

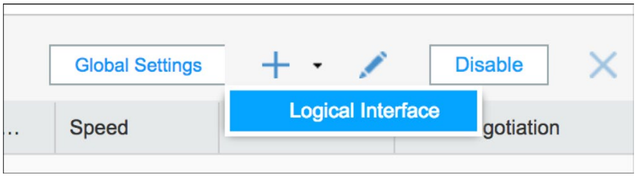
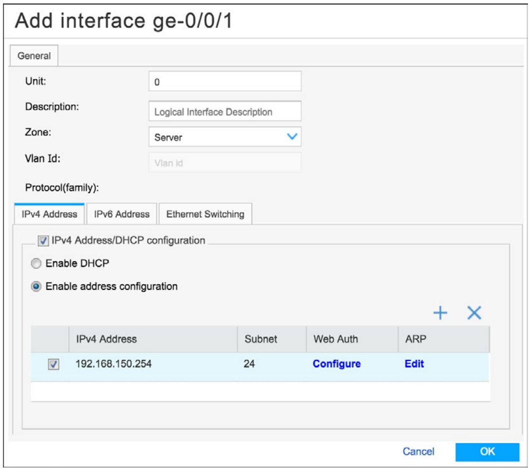


Figure 4.7 Logical Interface Definition

In the logical properties add the following:

- Logical Unit: *0*
- Zone: *Server*
- IPV4 Address: *192.168.150.254/24*



Add interface ge-0/0/1

General

Unit:	0
Description:	Logical Interface Description
Zone:	Server
Vlan Id:	Vlan id

Protocol(family):

IPv4 Address | IPv6 Address | Ethernet Switching

☑ IPv4 Address/DHCP configuration

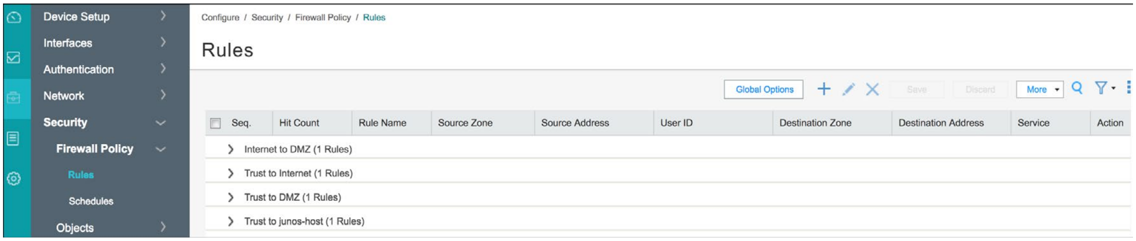
○ Enable DHCP

● Enable address configuration

	IPv4 Address	Subnet	Web Auth	ARP
☑	192.168.150.254	24	Configure	Edit

Figure 4.8 Logical Interface Configuration

Finally, let's add a security policy to allow users in the Trust Zone to log in to the Active Directory server. Go to Configure/Security/Firewall Policy/Rules as shown in Figure 4.9:



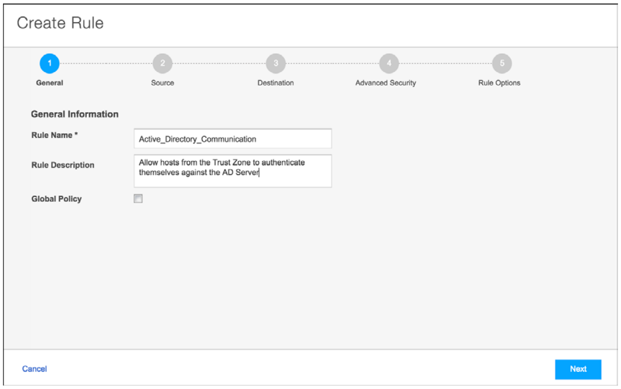
Configure / Security / Firewall Policy / Rules

Rules

☐ Seq.	Hit Count	Rule Name	Source Zone	Source Address	User ID	Destination Zone	Destination Address	Service	Action
› Internet to DMZ (1 Rules)									
› Trust to Internet (1 Rules)									
› Trust to DMZ (1 Rules)									
› Trust to junos-host (1 Rules)									

Figure 4.9 Security Policies

Click on the + button and a new Create Rule Wizard appears:



General Information

Rule Name * Active_Directory_Communication

Rule Description Allow hosts from the Trust Zone to authenticate themselves against the AD Server

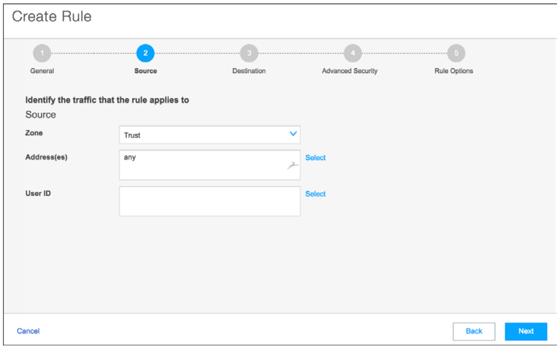
Global Policy □

Figure 4.10 Create Firewall Rule Wizard – Basic Information

Add the Rule Name that fits your environment and process, but this book recommends that as a best practice you name policies based on the communication it controls and always insert a description about the rule objectives, so others can understand what was done.

Do not enable the Global Policy option. Click Next.

The setup wizard will now ask you to define the Source Information parameters as shown in Figure 4.11. Select the Trust as the Source Zone and in the Address(es) field, click Select:



Identify the traffic that the rule applies to

Source

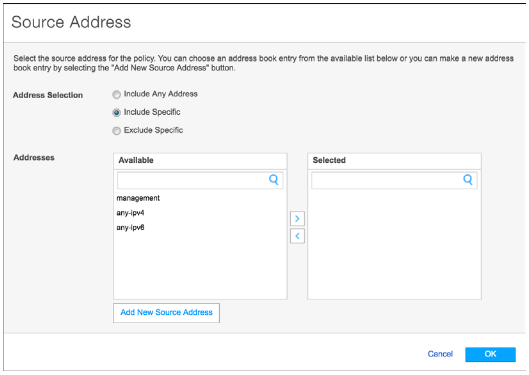
Zone Trust

Address(es) any

User ID

Figure 4.11 Create Firewall Rule Wizard – Source Info

Because an address object hasn't been created yet, let's take advantage of the fact that the rule wizard allows us to do it here:



Source Address

Select the source address for the policy. You can choose an address book entry from the available list below or you can make a new address book entry by selecting the "Add New Source Address" button.

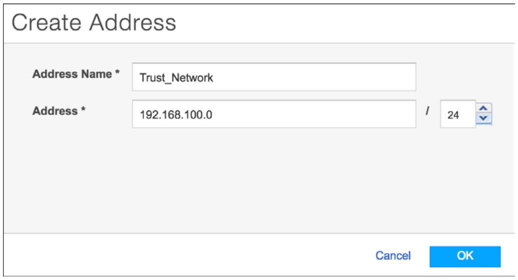
Address Selection
○ Include Any Address
● Include Specific
○ Exclude Specific

Addresses

Available	Selected
management	
any-ipv4	
any-ipv6	

Figure 4.12 Create a New Address Object

In Figure 4.12, select the Include Specific option, and then click the Add New Source Address button. Figure 4.13 appears. Define the new object named *Trust_Network* and in the address field, insert the network. Don't forget to add the subnet value, here, *24*:



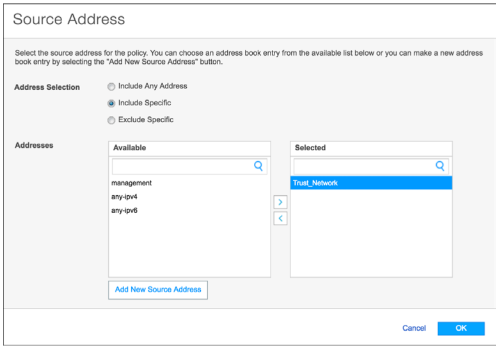
Create Address

Address Name * Trust_Network

Address * 192.168.100.0 / 24

Figure 4.13 Address Object Definition

Click OK. Now in the Source Address dialog, move the new address to the Selected tab and click OK:



Source Address

Select the source address for the policy. You can choose an address book entry from the available list below or you can make a new address book entry by selecting the "Add New Source Address" button.

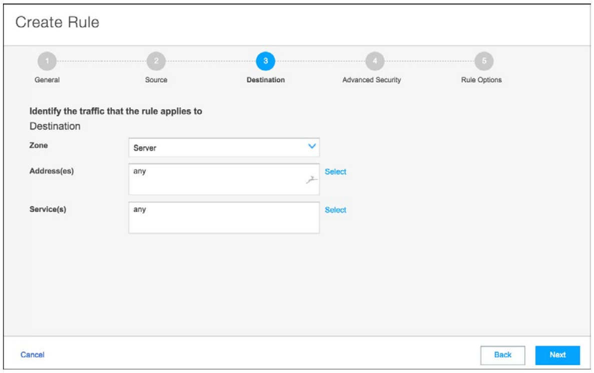
Address Selection
○ Include Any Address
● Include Specific
○ Exclude Specific

Addresses

Available	Selected
management	Trust_Network
any-ipv4	
any-ipv6	

Figure 4.14 Source Address Selection

Next, the wizard moves you to define the destination Zone and the destination address. At the Destination Zone, select *Server* as the Zone:



Identify the traffic that the rule applies to

Destination

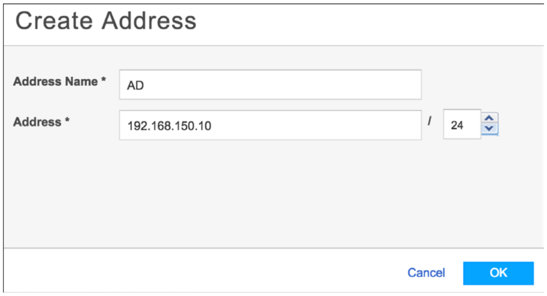
Zone: Server

Address(es): any

Service(s): any

Figure 4.15 Create Firewall Rule Wizard – Destination Info

You need to create another address object for the destination address. Follow the same steps used to create the source address, but now in the Destination sequence. Name it as AD and insert its IP address and mask:



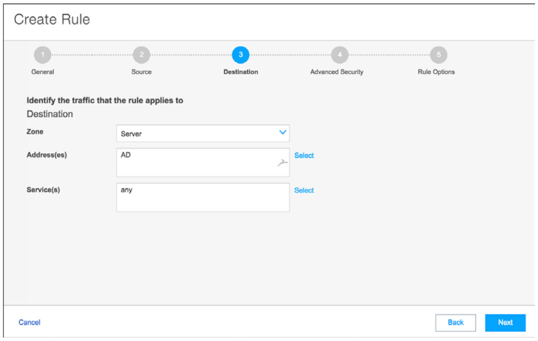
Address Name *: AD

Address *: 192.168.150.10 / 24

Figure 4.16 Adding Another Address Object

Click OK in the Figure 4.16 dialog.

Select the AD server as the destination address, so your Destination set looks like Figure 4.17:



Identify the traffic that the rule applies to

Destination

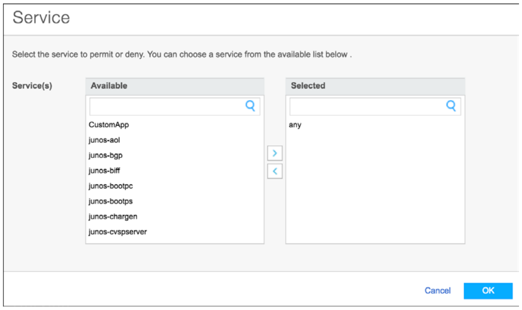
Zone: Server

Address(es): AD — Select

Service(s): any — Select

Figure 4.17 *Create Firewall Rule Wizard – Destination Info with Address*

For Services, let's use *any* for now, but you do need to restrict the ports according to your own environment:



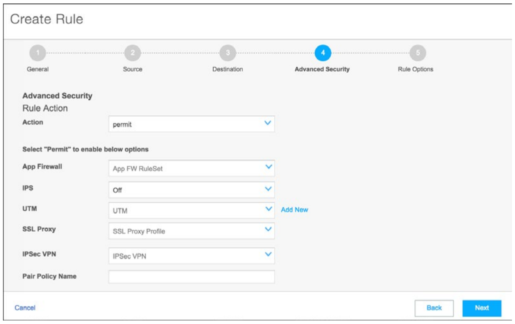
Select the service to permit or deny. You can choose a service from the available list below .

Service(s)

Available	Selected
CustomApp	any
junos-aol	
junos-bgp	
junos-biff	
junos-bootpc	
junos-bootps	
junos-chargen	
junos-cvspserver	

Figure 4.18 *Service Definition*

Click OK. Review the configuration. When you're done, click Next to move to the Advanced Security tab. In Figure 4.19, let's just configure the Action to *permit* and then click on Next:



Advanced Security

Rule Action

Action: permit

Select "Permit" to enable below options

App Firewall: App FW RuleSet

IPS: Off

UTM: UTM

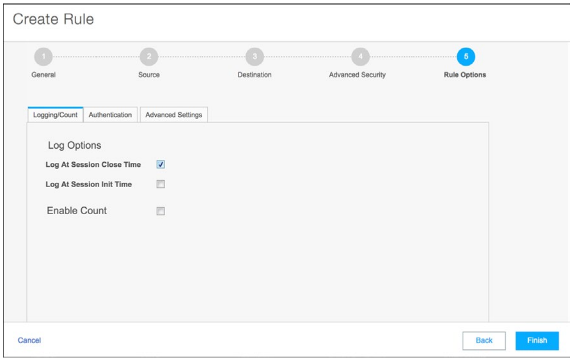
SSL Proxy: SSL Proxy Profile

IPSec VPN: IPSec VPN

Pair Policy Name:

Figure 4.19 *Create Policy Wizard – Advanced Security Settings*

In the Log Options dialog, enable the Log At Session Close Time option and click on Finish:



Log Options

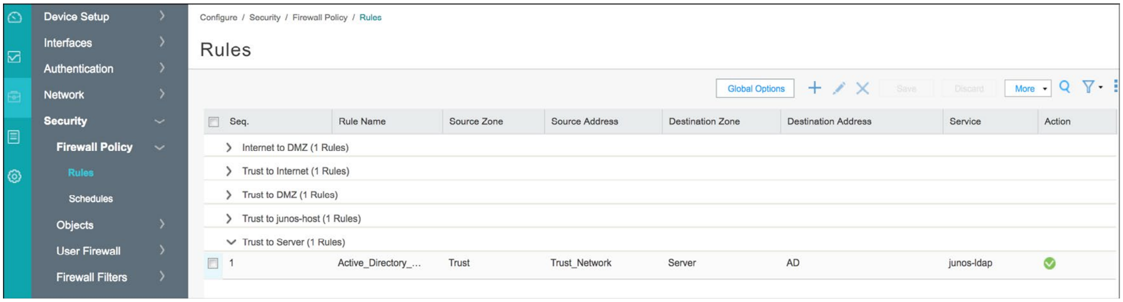
Log At Session Close Time ☑

Log At Session Init Time ☐

Enable Count ☐

Figure 4.20 *Create Policy Wizard – Rule Options*

Review the policy summary and if everything is in place, click OK. Save your rules and Commit. Your new rule will appear in the GUI:



☐	Seq.	Rule Name	Source Zone	Source Address	Destination Zone	Destination Address	Service	Action
	› Internet to DMZ (1 Rules)							
	› Trust to Internet (1 Rules)							
	› Trust to DMZ (1 Rules)							
	› Trust to junos-host (1 Rules)							
	⌄ Trust to Server (1 Rules)							
☐	1	Active_Directory_...	Trust	Trust_Network	Server	AD	junos-ldap	✓

Figure 4.21 *Rule Policies Screen (with the new rule highlighted)*

Chapter 5

Network Address Translation

By default, packets arriving to the SRX are routed to each specific destination, as the SRX is also a router. This is a powerful capability that enhances the SRX efficiency in complex environments, but makes it almost impossible for your internal networks to access public ones, such as the Internet, because private IP addresses cannot be routed over the Internet (as mandated by RFC1918). This also makes it impossible for addresses on the Internet to access applications hosted in your private network.

To overcome this issue and several others, Network Address Translation (NAT) comes to the rescue.

NAT Types

The SRX is capable of performing different forms of translation of the source and destination headers. The options are: *source*, *destination*, and *static*.

MORE? This chapter covers a basic introduction to each type of NAT, as well as how to configure the basic NAT configurations for each mode, so you can perform most of the routine tasks. More advanced scenarios such as CGNAT, IPV6 NAT, NAT64, NAT, multicast, and NAT hair-pinning are beyond the scope of this book. See the Juniper TechLibrary for more on these advanced scenarios: http://www.juniper.net/documentation.

NOTE This book only uses Source and Destination NAT, but for your reference it will also cover the use of Static NAT.

Source NAT

Source NAT is a many-to-one NAT that can map many IP addresses to one or more addresses, but not in a one-to-one fashion.

Source NAT is dynamically allocated in real time based on the available IP addresses and ports in the pool. For instance, you might want to hide all hosts in the Trust zone in the subnet 192.168.100.0/24 behind a public IP address, let's say the SRX public IP address, when they connect out to the Internet. Hosts on the Internet cannot make a new connection back to the hosts because it is not a bidirectional form of NAT-like Static NAT.

The typical use case for Source NAT is to give clients behind a network one or more IP addresses that they can use to connect to the Internet.

Some administrators also feel that NAT is a security mechanism. Although there is some truth to this, security is more of a side effect than the true purpose of NAT, and attackers have found numerous ways around NAT as a security mechanism. Source NAT can also be used to connect to trading partners when you use internal IP addresses to hide, overlap, or to simplify routing and security on both sides.

During the initial setup, you already defined a Source NAT policy to allow internal computers in the Trust Zone to access the Internet Zone. In this case, you are using Source Egress Interface NAT, but it's important to mention that other types of Source NAT are supported:

- Translation of the original source IP address to the egress interface IP address (also called *interface NAT*).
- Translation of the original source IP address to an IP address from a user-defined address pool without port address translation. The association between the original source IP address to the translated source IP address is dynamic. However, once there is an association, the same association is used for the same original source IP address for new traffic that matches the same NAT rule.
- Translation of the original source IP address to an IP address from a user-defined address pool with port address translation. The association between the original source IP address to the translated source IP address is dynamic. Even if an association exists, the same original source IP address may be translated to a different address for new traffic that matches the same NAT rule.
- Translation of the original source IP address to an IP address from a user-defined address pool by shifting the IP addresses. This type of translation is one-to-one, static, and without port address translation. If the original source IP address range is larger than the IP address range in the user-defined pool, untranslated packets are dropped.

Overview of a Source NAT Rule

The main configuration tasks for a Source NAT rule using an interface as a translated address, are as follows:

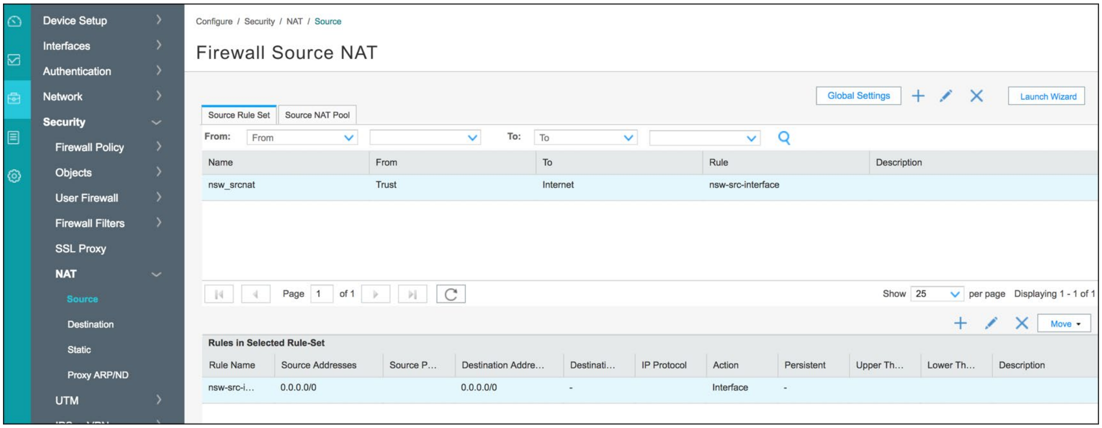
- Configure an interface NAT mapping of private addresses to the public address of an egress interface.
- (Optional) Configure the persistent address.
- Configure source NAT rules that align with your network and security requirements.

NOTE Remember that in order for traffic to go across the SRX, you also need to configure a security policy. A NAT configuration looks similar to a security policy, but this will not allow the traffic through, it will just manipulate the traffic according to the NAT rule once it has been permitted by a security policy. This applies to all NAT Types.

Configuring Source NAT Rules

There are several options available when executing this kind of translation. For example, you can configure it so that the source IP is translated to the IP of the egress interface, or you can use a different pool of IP addresses, or use port address translation, etc.

Remember that in Chapter 4, you already defined a Source NAT policy during the initial setup. Let's check this policy and its components. On the SRX GUI, click on Configure/Security/NAT/Source. Figure 5.1 appears on screen:



Firewall Source NAT

Name	From	To	Rule	Description
nsw_srcnat	Trust	Internet	nsw-src-interface	

Displaying 1 - 1 of 1

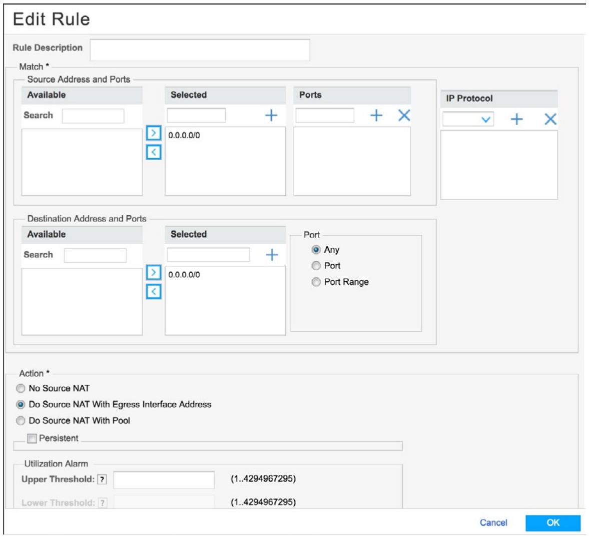
Rules in Selected Rule-Set

Rule Name	Source Addresses	Source P...	Destination Addre...	Destinati...	IP Protocol	Action	Persistent	Upper Th...	Lower Th...	Description
nsw-src-i...	0.0.0.0/0		0.0.0.0/0	-		Interface	-			

Figure 5.1 Source NAT Configuration Screen

You can see that there's a created policy named *nsw_srcnat*. This is the policy the setup wizard created when you enabled Source NAT for the Trust Zone.

Select the rule *nsw_srcnat* under the Source Rule Set, and click on Edit. The Edit Rule wizard should appear as in Figure 5.2:


Edit Rule

Rule Description:

Match *

Source Address and Ports

Available: Search:

Selected: 0.0.0.0/0

Ports:

IP Protocol:

Destination Address and Ports

Available: Search:

Selected: 0.0.0.0/0

Port: ● Any ○ Port ○ Port Range

Action *

○ No Source NAT
● Do Source NAT With Egress Interface Address
○ Do Source NAT With Pool

□ Persistent

Utilization Alarm

Upper Threshold: (1..4294967295)

Lower Threshold: (1..4294967295)

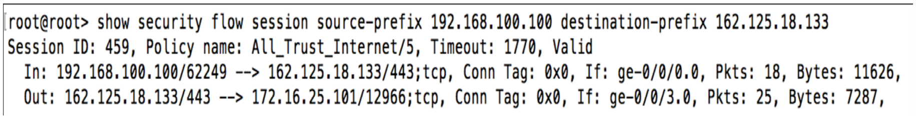
Figure 5.2 *Source NAT Rule Options*

You can see all the options available for a Source NAT rule:

- Source and Destination Address and Ports.
- Actions (when the conditions are met).
- You can verify that three actions are available:
  - No Source NAT
  - Source NAT with Egress Interface Address
  - Source NAT with Pool
- Persistent NAT
- Utilization Alarm (for NAT Pools)

As mentioned previously, since we are using the Egress Interface option, and as this rule was defined during the initial setup wizard, no further changes are necessary.

If you haven't tested Internet access, this is a great moment to do so. After accessing a website, you can connect on the SRX CLI and inspect the session table using the Junos `show security flow session` command. For example, the output in Figure 5.3 shows the NAT translation for a specific session:



```
root@root> show security flow session source-prefix 192.168.100.100 destination-prefix 162.125.18.133
Session ID: 459, Policy name: All_Trust_Internet/5, Timeout: 1770, Valid
  In: 192.168.100.100/62249 --> 162.125.18.133/443;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 18, Bytes: 11626,
  Out: 162.125.18.133/443 --> 172.16.25.101/12966;tcp, Conn Tag: 0x0, If: ge-0/0/3.0, Pkts: 25, Bytes: 7287,
```

Figure 5.3 Session Using Source NAT

The output indicates that there is an incoming packet with a source IP address of 192.168.100.100 (an IP address from the Trust Zone), destined to 162.125.18.133 in the TCP port 443. The return traffic shows a packet being sourced from 209.239.112.126, destined to the SRX Egress Interface IP address, 172.16.25.101.

It's worth mentioning that you can also find this information in J-Web by accessing the Monitor/Security/Flow Session page.

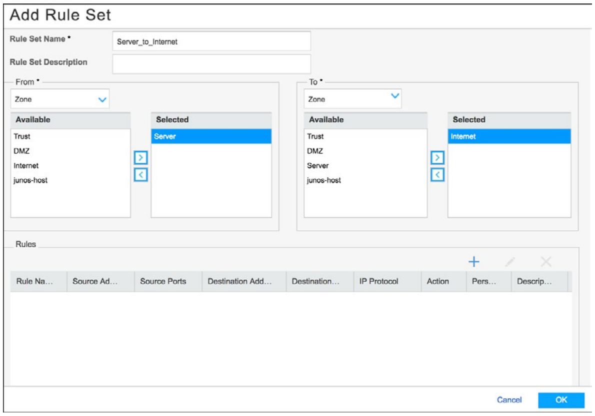
NOTE The `show security flow sessions` command is very helpful and it will be covered in more detail later on in this book.

Also, it's important to remember that back in Chapter 4, you created a new Security Zone named Server to host our Internal Services (in our case, Active Directory). In some environments, Source NAT is not necessary for this zone as the servers may be prevented from accessing the Internet or may use a different method, such as a Web Proxy.

In other environments there may be a need for the servers to direct access the Internet, and then Source NAT is needed.

In this book's setup, Source NAT is needed, and we'll configure it now. It is up to you to define the need for it in your own environment.

Let's open the Source NAT page and click on the + sign. Add a new Rule Set called *Server_to_Internet* and on the *From* and *To* fields, select Zone as the parameter. Now, from the Source Zone, select Server and from the Destination Zone select Internet, as you can see in Figure 5.4:



Add Rule Set

Rule Set Name * Server_to_Internet

Rule Set Description

From *: Zone

Available: Trust, DMZ, Internet, junos-host

Selected: Server

To *: Zone

Available: Trust, DMZ, Server, junos-host

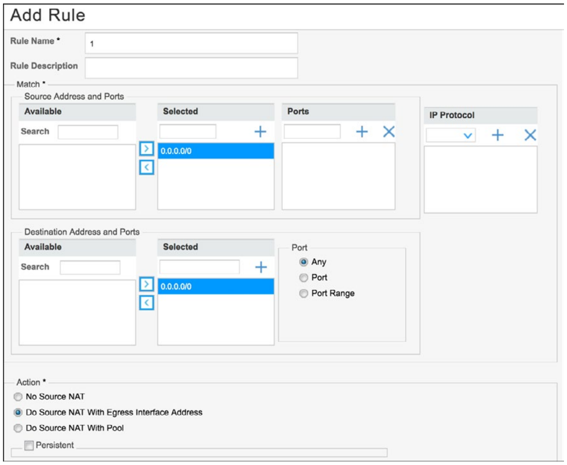
Selected: Internet

Rules

Rule Na...	Source Ad...	Source Ports	Destination Add...	Destination...	IP Protocol	Action	Pers...	Descrip...

Figure 5.4 Source NAT Rule Set

Let's add a Source NAT rule to the rule set just created. Name it *1* and use *0.0.0.0/0* for both the Source and Destination Addresses. Select the action at the bottom of the wizard dialog box as Source NAT with Egress Interface Address:



Add Rule

Rule Name * 1

Rule Description

Match *

Source Address and Ports

Available — Search

Selected: 0.0.0.0/0

Ports

IP Protocol

Destination Address and Ports

Available — Search

Selected: 0.0.0.0/0

Port
● Any
○ Port
○ Port Range

Action *
○ No Source NAT
● Do Source NAT With Egress Interface Address
○ Do Source NAT With Pool

□ Persistent

Figure 5.5 Source NAT Rule

Click OK. The new Source NAT policy is done. Remember, now you must add a security policy to permit the necessary traffic.

Destination NAT

Destination NAT is a one-to-many form of NAT that allows you to map a single IP address to multiple IP addresses.

For instance, inbound connections to a public IP address in your control (let's say, the SRX IP address) could be mapped to the internal machines at a security zone of your choice (here, it's the DMZ Zone).

The mechanism to determine which internal host to map them to would be based on the port number in the destination IP address of the connection.

For instance, if a packet arrives on your public IP address with destination port 443, it will go to 192.168.200.10:443. The main use case for this is when you are limited in the public IP addresses that you have, but you need to make multiple services available on the Internet. If you don't have enough public IP addresses to map one-to-one using static NAT, then you would need to use destination NAT.

Destination NAT maps a table based on the destination IP address and destination port. This will translate the IP address to the internal address, and optionally you can also translate the destination port as well.

The following types of destination NAT are supported:

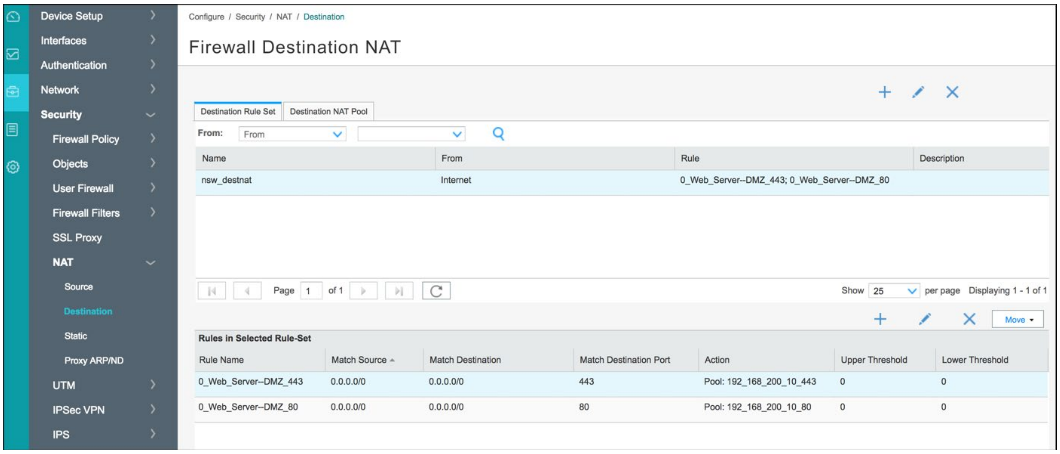
- Translation of the original destination IP address to an IP address from a user-defined pool. This type of translation does not include Port Address Translation (PAT). If the original destination IP address range is larger than the address range in the user-defined address pool, any untranslated packets are dropped.
- Translation of the original destination IP address (and optional port number) to one specific IP address (and port number) from a user-defined pool.

The main configuration tasks for destination NAT are:

- Configure a destination NAT address pool that aligns with your network and security requirements.
- Configure destination NAT rules that align with your network and security requirements.
- Configure NAT proxy ARP entries for IP addresses in the same subnet of the ingress interface.

Configuring Destination NAT Rules

Remember that in Chapter 4 you already defined a destination NAT policy during the initial setup. Let's check this policy and its components. On the SRX GUI, click on Configure/Security/NAT/Destination. The configuration screen in Figure 5.6 appears:



Firewall Destination NAT

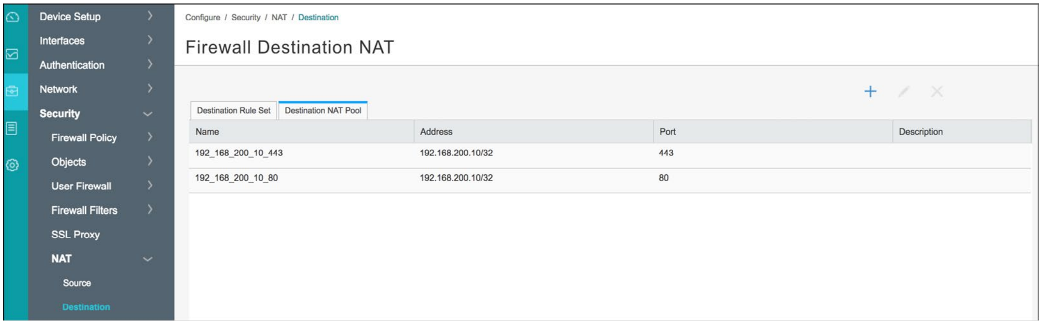
Name	From	Rule	Description
nsw_destnat	Internet	0_Web_Server--DMZ_443; 0_Web_Server--DMZ_80	

Rules in Selected Rule-Set

Rule Name	Match Source	Match Destination	Match Destination Port	Action	Upper Threshold	Lower Threshold
0_Web_Server--DMZ_443	0.0.0.0/0	0.0.0.0/0	443	Pool: 192_168_200_10_443	0	0
0_Web_Server--DMZ_80	0.0.0.0/0	0.0.0.0/0	80	Pool: 192_168_200_10_80	0	0

Figure 5.6 Destination NAT Configuration Screen

As you can see, there's a policy named *nsw_dstnat* with several attributes defined. Let's check each one of them. First, click on the Destination NAT Pool tab in Figure 5.6 and the 5.7 should appear:

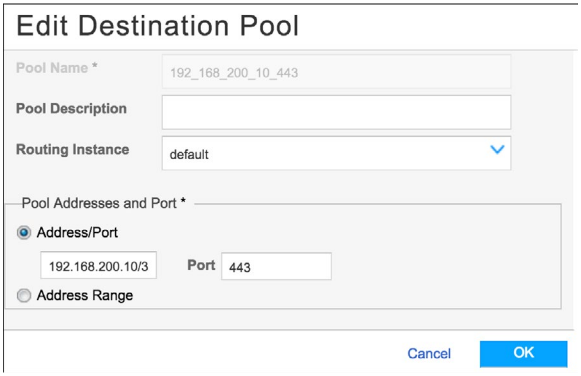


Firewall Destination NAT

Name	Address	Port	Description
192_168_200_10_443	192.168.200.10/32	443	
192_168_200_10_80	192.168.200.10/32	80	

Figure 5.7 Destination NAT Pools

You can see there are two NAT Pools created, each one points to the Web Server (192.168.200.10), with the difference being the NAT'd port (80 and 443). Let's select the first one (443) and then click on Edit. The details appear for this pool:



Edit Destination Pool

Pool Name * 192_168_200_10_443

Pool Description

Routing Instance default

Pool Addresses and Port *

● Address/Port

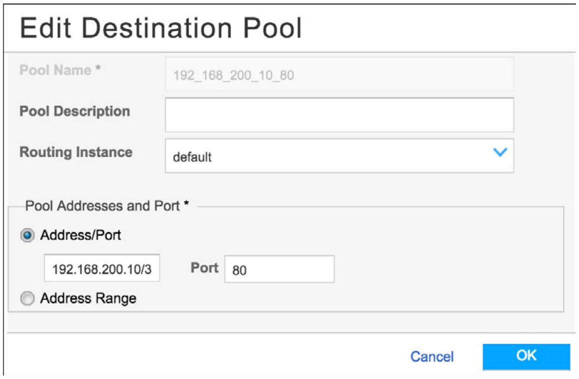
192.168.200.10/3 Port 443

○ Address Range

Cancel OK

Figure 5.8 *Destination NAT Pool (443) details*

It becomes clear that the Destination Pool refers to the IP address of the web server and its translated Port (443). Let's check the other destination pool using the same steps:



Edit Destination Pool

Pool Name * 192_168_200_10_80

Pool Description

Routing Instance default

Pool Addresses and Port *

● Address/Port

192.168.200.10/3 Port 80

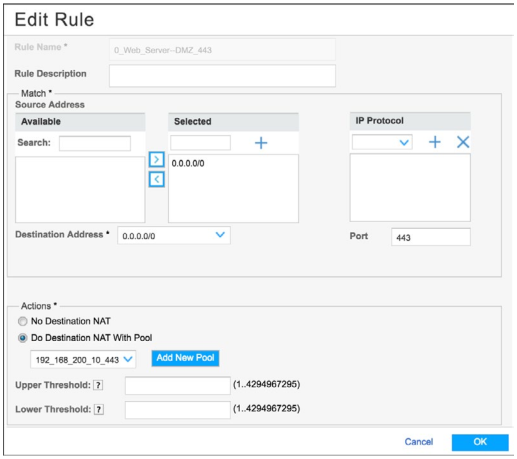
○ Address Range

Cancel OK

Figure 5.9 *Destination NAT Pool (80) Details*

As you can see, the only difference between the destination pools is the translated Port (80). This makes it easy for an administrator to enable PAT (Port Address Translation).

PAT allows several IP addresses to share a single address (in our case, the SRX Egress IP) by creating destination pools with different IP addresses and ports. Let's review the first destination NAT rule (it should be named 0_Web_Server—DMZ_443). Select the rule and click on Edit and the edit rule wizard dialog should appear as shown in Figure 5.10:



Edit Rule

Rule Name * 0_Web_Server--DMZ_443

Rule Description

Match *

Source Address

Available

Search:

Selected

0.0.0.0/0

IP Protocol

Destination Address * 0.0.0.0/0

Port 443

Actions *

○ No Destination NAT

● Do Destination NAT With Pool

192_168_200_10_443

Upper Threshold: ? (1..4294967295)

Lower Threshold: ? (1..4294967295)

Figure 5.10 *Destination NAT Rule Details*

As you can see, many options are available, such as:

- Source Address
- Destination Address
- Destination Port
- Actions
  - No Destination NAT
  - Destination NAT with Pool
- Utilization Thresholds

As mentioned previously, you are using the SRX external interface for destination NAT, and as this rule was defined during the initial setup wizard, no further changes are necessary.

Static NAT

Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction. From the NAT device, the original destination address is the virtual host IP address, while the mapped-to address is the real host IP address.

Static NAT allows connections to be originated from either side of the network, but translation is limited to one-to-one or between blocks of addresses of the same size.

The main use case for this type of NAT is when you have a host on which you want to perform NAT and you want both inbound access to this host and outbound access to come from the same IP address. Often it is used in DMZ scenarios where you have enough IP addresses present that you don't want to overload the public IP addresses, or if you want to simply hide the internal addressing scheme without overloading or multiplexing the IP addresses.

The main configuration tasks for static NAT are:

- Configure static NAT rules that align with your network and security requirements.
- Configure NAT proxy ARP entries for IP addresses in the same subnet of the ingress interface.

Configuring Static NAT Rules

When administrators need to configure NAT (source, destination or static), they can use the NAT wizard to do it. For the static NAT wizard configuration, in the SRX GUI, go to Configure/Security/NAT/Static:

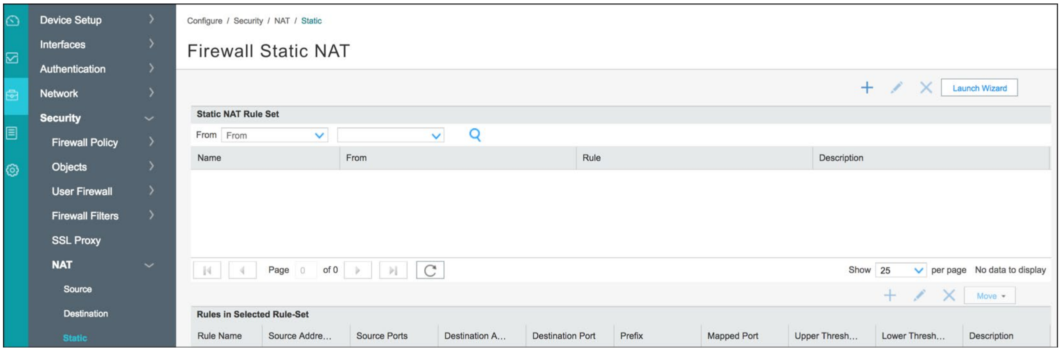
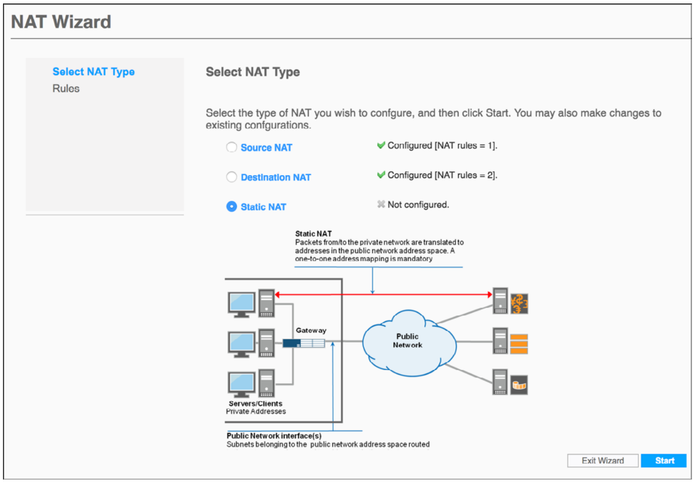


Figure 5.11 *Static NAT*

Click the Launch Wizard button in the upper right of the window:



NAT Wizard

Select NAT Type
Rules

Select NAT Type

Select the type of NAT you wish to configure, and then click Start. You may also make changes to existing configurations.

○ Source NAT ✓ Configured [NAT rules = 1].

○ Destination NAT ✓ Configured [NAT rules = 2].

● Static NAT ✗ Not configured.

Static NAT
Packets from/to the private network are translated to addresses in the public network address space. A one-to-one address mapping is mandatory
Gateway
Public Network
Servers/Clients
Private Addresses
Public Network interface(s)
Subnets belonging to the public network address space routed
Exit Wizard
Start

Figure 5.12 Static NAT Creation Wizard

Just follow the instructions in order to configure static NAT for your environment.

Proxy ARP

Proxy ARP is a useful feature that allows the SRX to respond to ARP requests in the following scenarios:

- When addresses defined in the static NAT and source NAT pool are in the same subnet as that of the ingress interface (Source NAT and Static NAT scenario).
- When addresses in the original destination address entry in the destination NAT rules are in the same subnet as that of the ingress interface (destination NAT scenario).

As an example, reference the following scenario illustrated in Figure 5.13: the SRX is an external IP address (1.1.1.1), but the administrator wants to enable a destination NAT for the webserver in the DMZ using a different public IP address (1.1.1.2). In this case, the SRX doesn't have the 1.1.1.2 IP address configured on its interface and therefore it can't respond on ARP requests for it. This is where Proxy ARP comes in.

Proxy ARP simply informs the interface to which it is applied to respond to incoming ARP requests for IP addresses with its own interface MAC address so that the peer device will forward traffic destined to the NAT addresses to the firewall, which will handle the traffic properly.

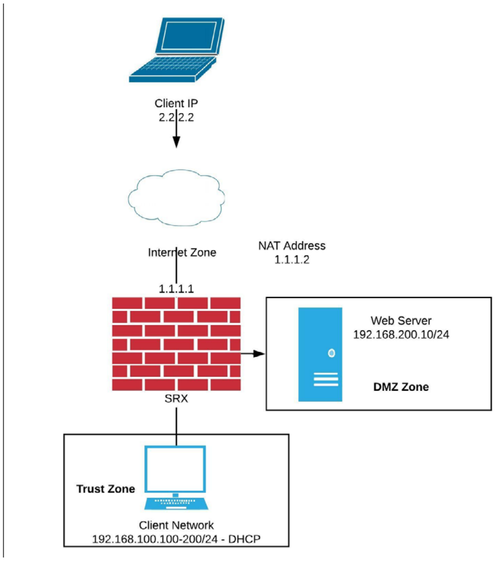
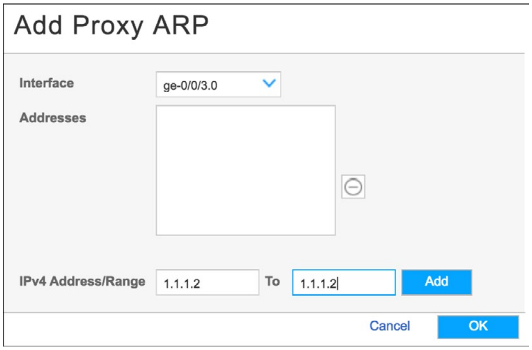


Figure 5.13 Proxy ARP Usage

Configuring Proxy ARP

To enable proxy ARP, navigate to Configure/Security/NAT/Proxy ARP/ND. Click on the + button and select the Proxy ARP option:



Add Proxy ARP

Interface: ge-0/0/3.0

Addresses

IPv4 Address/Range: 1.1.1.2 To 1.1.1.2

Figure 5.14 Proxy ARP Configuration

Select the interface that will proxy the ARP requests (ge-0/0/3.0) in this scenario, and the IP address or range that will be proxied. Click on Add to include the IP addresses in the proxy ARP configuration. Click OK and commit when finished.

Chapter 6

Next-Generation Firewall

As discussed earlier, the SRX is a stateful firewall capable of controlling traffic in the network by inspecting source and destination addresses, ports, and protocols up to Layer 4 of the OSI model.

This works really well to protect networks and services against malicious users, but with the increasing sophistication of attacks and with the fact that the majority of the applications are now using standard ports like TCP 80 and 443 to run, there's a need to also inspect the application layer (Layer 7) to identify and control applications and to detect and block attacks.

This is the place where a next-generation firewall (NGFW) comes into play. Lucky for us, the SRX can also be configured as a next-generation firewall. Even better, you, as the administrator have the power to choose on which rules you want to enable the Application Inspection capability and which ones you don't.

This is a powerful capability as you can choose on where you want to focus your security with higher performance and low latency and where you want to focus on deep packet inspection to achieve application control, visibility, and advanced inspection against attacks.

SRX Next-Generation Firewall Features

The SRX, when configured as a next-generation firewall, will have the following features available:

- Integrated User Firewall (UserFW): Enforce security policies using user identities, rather than just IP addresses.

- Application Visibility and Control: Enforce policies based on applications.
- SSL Proxy: Enforce security policies on encrypted SSL connections.
- IPS: Integrated Intrusion Prevention system.

This chapter covers Integrated User Firewall, Application Visibility and Control, and the SSL Forward Proxy. IPS will be covered later, in Chapter 8.

Understanding How Integrated User Firewall and AppSecure Works

An individual can connect to the network simultaneously using multiple devices, making it impractical to identify a user, an application, or a device by a group of statically allocated IP addresses and port numbers. To solve this problem, the SRX integrates with different sources of user identity information, like Microsoft Active Directory, Microsoft Exchange Server, Pulse Secure UAC, and Aruba ClearPass. It also uses an advanced pattern matching and heuristics application identification engine, called *AppSecure,* to recognize traffic at different network layers using characteristics other than port numbers.

The integrated user firewall feature enables the SRX to communicate with an Active Directory server to obtain the user identity information. It retrieves user-to-IP address mappings from the Windows Active Directory to use in firewall policies as match criteria. This feature consists of the SRX Series polling the event log of the Active Directory controller to determine, by username and source IP address, who has logged in to the SRX Series device. Then the username and group information are queried from the LDAP service in the Active Directory controller. Once the SRX Series has the IP address, username, and group relationship information, it generates authentication entries. With the authentication entries, the SRX Series User FW module enforces user and group-based policies.

With more details, the SRX reads the Windows event log from the Active Directory controller and abstracts IP address-to-user mapping information. If the information is not readable from the AD itself, the SDRX will probe the computer to try to obtain the information.

The User Firewall process then correlates users to the groups to which they belong via the LDAP protocol in the Active Directory controller. Thus, the process has gathered enough information to generate authentication entries. Next, the firewall administrator references the authentication entries in user based security policies to control traffic.

NOTE On larger Microsoft Active Directory environments with several *forests* and *domain controllers,* or situations where the information source is not based on Microsoft Active Directory, Juniper supports an agent-based authentication solution, called Juniper Identity Management Service, or JIMS.

MORE? JIMS is free to use and its documentation is available from the Juniper TechLibrary: https://www.juniper.net/documentation/en_US/jims1.0.0/topics/concept/jims-feature-descriptions.html .

AppSecure service modules are used to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the application ID of the traffic.

The following modules are part of the AppSecure Engine:

- *AppTrack*: Tracks and reports applications passing through the device.
- *AppFW*: Enforces policies on flows based on the AppTrack information by using application-based rules.
- *AppQoS*: Provides quality-of-service (QoS) prioritization based on application awareness.
- *AppRoute*: Classifies sessions based on applications and applies the configured rules to reroute the traffic.

A very important aspect of AppSecure is that it *doesn't rely on protocols or ports* to define what application is being used on a given flow. In fact, AppSecure leverages a full application-level identification functionality providing in-depth and effective detection capabilities, even for evasive applications. AppSecure uses a *protocol bundle* that contains application signatures and parsing information. The identification is based on protocol parsing, decoding, and session management. The detection mechanism has its own data feed and constructs to identify applications.

The following features are supported in application identification:

- Support for protocols and applications, including video streaming, peer-to-peer communication, social networking, games, and messaging.
- Identification of applications within applications (called *Nested Applications*).
- Ability to distinguish actions launched within an application (such as login, browse, chat, and file transfer).
- Support for all versions of protocols and application decoders and dynamic updates of decoders.
- Support for encrypted and compressed traffic and complex tunneling protocols.
- Ability to identify all protocols from Layer 3 to Layer 7.

A great advantage of the AppSecure Application Identification Engine is that it is optimized in a way that results in very little impact on the SRX overall performance. This is because, opposed to an IPS, AppSecure needs just a few packets of a flow to match most of the applications. Of course, some applications require more in-depth analysis, but the rule of thumb is that the majority of the applications are detected with just a few packets. Figure 6.1 illustrates the AppSecure workflow.

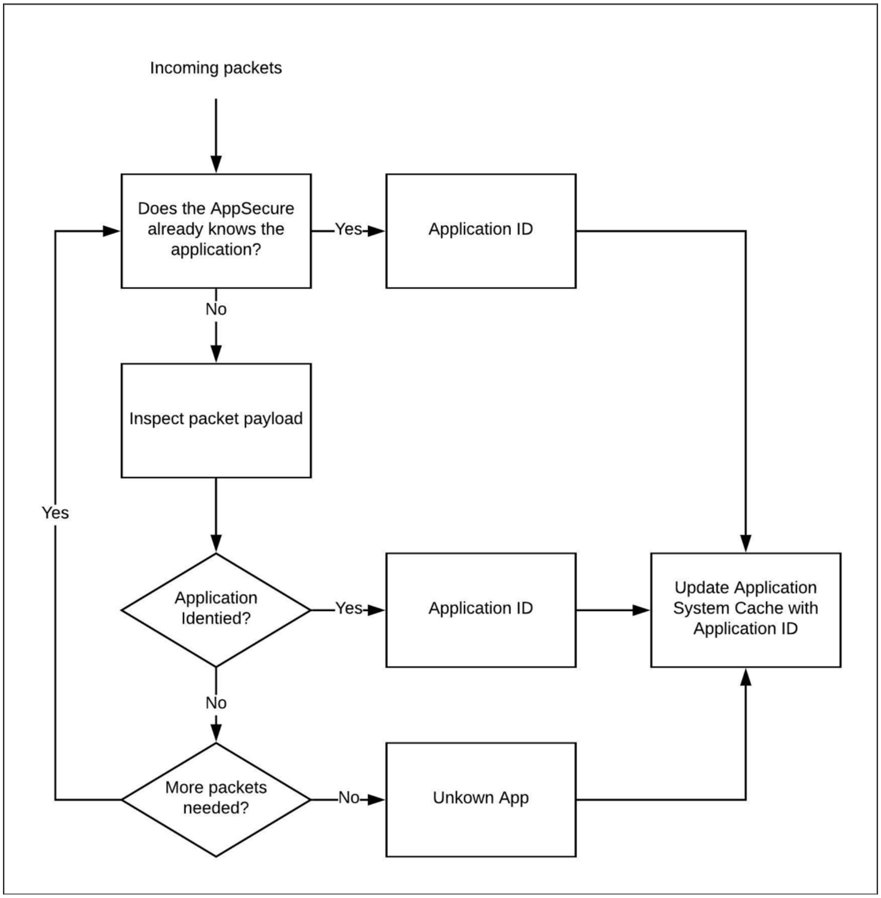


Figure 6.1 *AppSecure Workflow*

As you can see in Figure 6.1, the AppSecure engine looks for packets in a flow until the application is identified. Once an application match is found, the information is saved in the application system cache (ASC) to expedite future identification processes, so from this moment on, as the SRX already knows the application in the flow, subsequent packets are matched just by the ASC.

Application signatures identify an application based on protocol grammar analysis in the first few packets of a session. If the application identification engine has not yet identified the application, it passes the packets and waits for more data.

The application identification module matches applications for both client-to-server and server-to-client sessions.

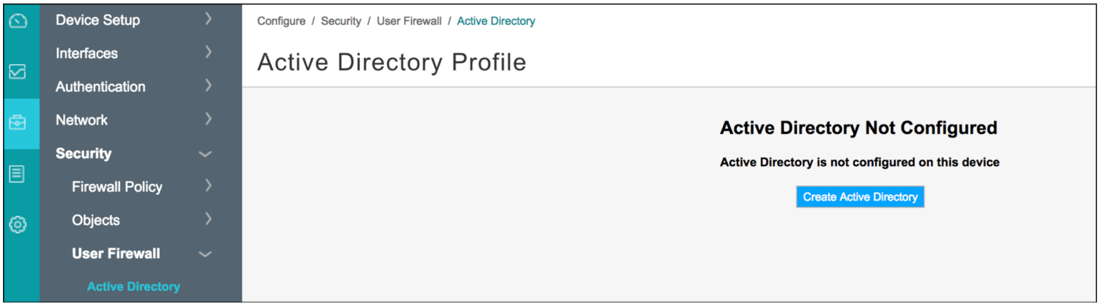
Once the application is determined, AppSecure service modules can be configured to monitor and control traffic for tracking, prioritization, access control, and attack detection and prevention.

Configuring Microsoft Active Directory Integration

The first step to enable next-generation firewall features is to integrate the SRX with an Active Directory domain controller. As a reference, the domain name used is *dayone.lab.net* and the Active Directory server has the IP address *192.168.150.10*.

NOTE Microsoft Active Directory installation and configuration is way beyond the scope of this book. Please check the official Microsoft documentation for support.

On J-Web, navigate to the Configure/Security/User Firewall/Active Directory, as shown in Figure 6.2, and then Click on Create Active Directory:



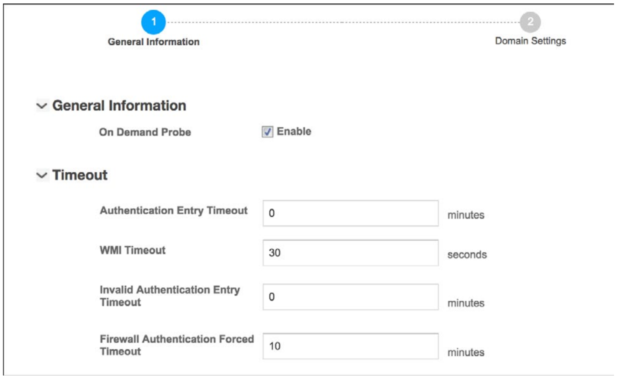
Active Directory Profile

Active Directory Not Configured

Active Directory is not configured on this device

Figure 6.2 Active Directory Profile Configuration

The Create Active Directory profile screen appears:



1 General Information
2 Domain Settings

General Information

On Demand Probe ☑ Enable

Timeout

Authentication Entry Timeout	0	minutes
WMI Timeout	30	seconds
Invalid Authentication Entry Timeout	0	minutes
Firewall Authentication Forced Timeout	10	minutes

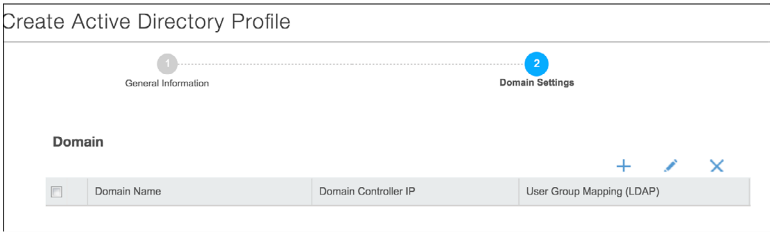
Figure 6.3 Active Directory Profile Configuration Details

Input the general information values, noted here:

- On Demand Probe: *Enable*
- Authentication Timeout: *0*
- WMI Timeout: *30*
- Invalid Authentication Timeout: 0
- Firewall authentication Forced Timeout: *10*

Click Next.

Now you need to insert the Active Directory domain information. This is specific to your environment, so use the information below as a reference. In the domain settings, click on the + sign as in Figure 6.4:



Create Active Directory Profile

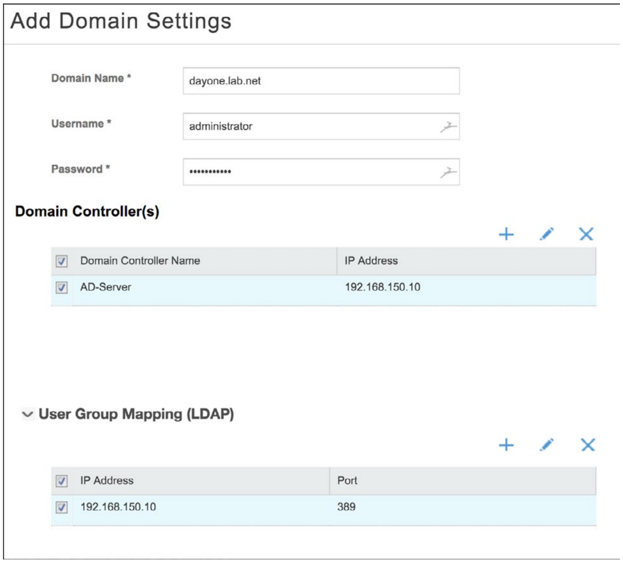
1 General Information
2 Domain Settings

Domain

□	Domain Name	Domain Controller IP	User Group Mapping (LDAP)

Figure 6.4 Active Directory Profile (Domain Settings)

The Add Domain Settings page will open as shown in Figure 6.5:



Add Domain Settings

Domain Name *	dayone.lab.net
Username *	administrator
Password *	•••••••••••

Domain Controller(s)

☑	Domain Controller Name	IP Address
☑	AD-Server	192.168.150.10

User Group Mapping (LDAP)

☑	IP Address	Port
☑	192.168.150.10	389

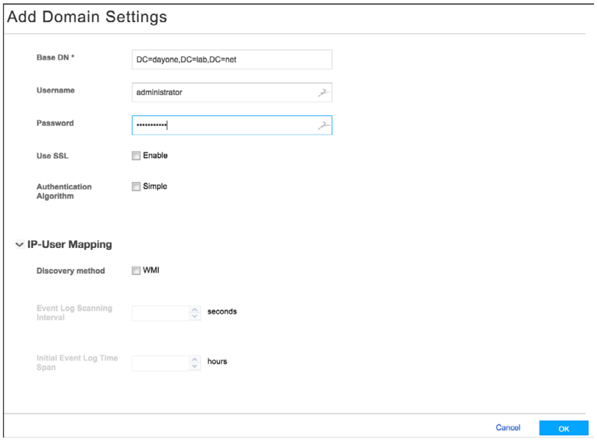
Figure 6.5 Active Directory Profile (Domain Settings Details)

Using your domain-specific information, input the information below:

- Domain Name: *dayone.lab.net*
- Username: *administrator* (or a read-only user with domain administrator level permissions)
- Password: *Your user password*
- Domain Controller: *Server Name and IP address*
- User Group mapping: *Usually, the same Domain Controller server* (check with your AD admin)
- Port: *Usually, port 389* (check with your AD admin)

Scrolling down the page, you will be presented with additional information shown in Figure 6.6 that needs to be inserted:

- Base DN: *DC=dayone,DC=lab,DC=net*
- Username: *Administrator* (or other account with administrator level privileges—the account can have read-only permissions)
- Password: *Your user password*



Add Domain Settings

Base DN * DC=dayone,DC=lab,DC=net

Username administrator

Password ••••••••••••

Use SSL □ Enable

Authentication Algorithm □ Simple

IP-User Mapping

Discovery method □ WMI

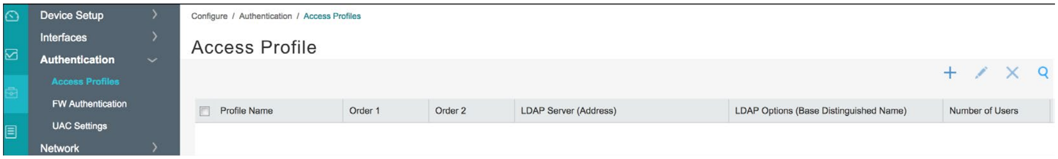
Event Log Scanning Interval seconds

Initial Event Log Time Span hours

Figure 6.6 Active Directory Profile (Domain Settings details – cont.)

After you're done, click OK. Review the configuration, and if everything is correct, click Finish.

You need to set up the LDAP access profile. On J-Web, navigate to Configure/Authentication/Access Profile, as shown in Figure 6.7, and click on the + sign to create an access profile:



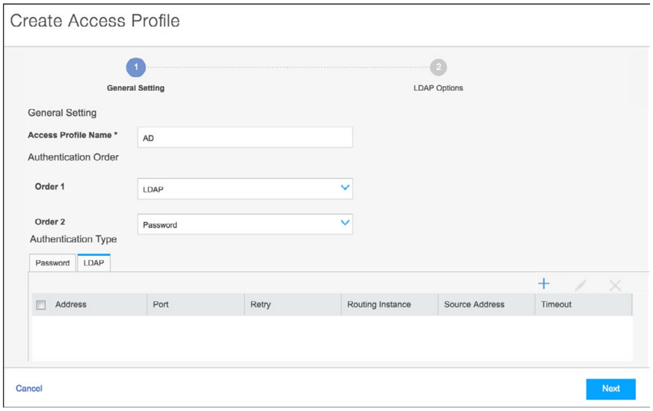
Configure / Authentication / Access Profiles

Access Profile

□	Profile Name	Order 1	Order 2	LDAP Server (Address)	LDAP Options (Base Distinguished Name)	Number of Users

Figure 6.7 Access Profile

The Create Access Profile page will open. Define a name for your Access Profile and select the authentication order shown in Figure 6.8:



Create Access Profile

General Setting

Access Profile Name * AD

Authentication Order

Order 1 LDAP

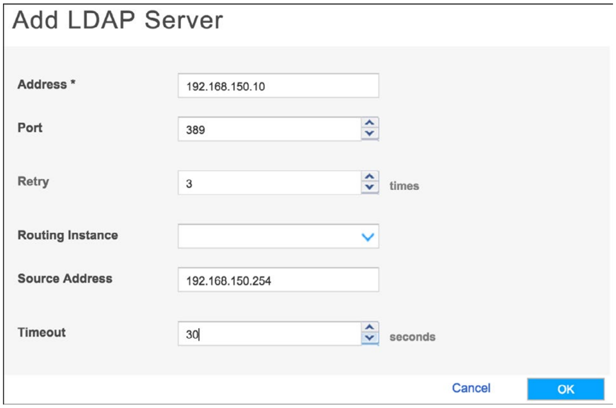
Order 2 Password

Authentication Type

☐ Address	Port	Retry	Routing Instance	Source Address	Timeout

Figure 6.8 Access Profile Settings

Under Authentication Type, select the LDAP tab and click on the + sign. Include the information related to your LDAP server and the source address the SRX will use to contact it:



Add LDAP Server

Address * 192.168.150.10

Port 389

Retry 3 times

Routing Instance

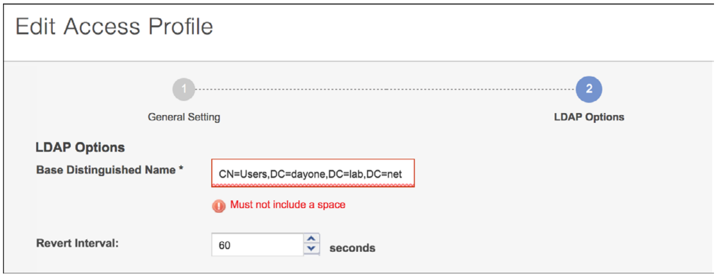
Source Address 192.168.150.254

Timeout 30 seconds

Figure 6.9 LDAP Server Connection Details

When you’re done, click OK and then, click Next.

In the LDAP Option portion of the configuration, you will need to include the LDAP search options, to input the Base DN and Interval:



Edit Access Profile

LDAP Options

Base Distinguished Name * CN=Users,DC=dayone,DC=lab,DC=net

Must not include a space

Revert Interval: 60 seconds

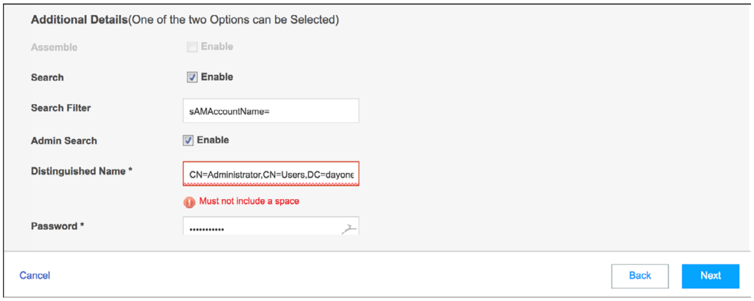
Figure 6.10 LDAP Options (Base DN Parameters)

Input the following:

- Base Distinguished Name: *CN=Users,DC=dayone,DC=lab,DC=net*
- Revert Interval: *60 seconds*

Scroll down the page and under Additional Details select the *Search* and *Admin Search* options, to input the following information, modifying the specifics to your own environment:

- Search Filter: *sAMAccountName=*
- Distinguished Name: *CN=Administrator,CN=Users,DC=dayone,DC=lab,DC =net* (adjust it to your environment)
- Password: *Your user password*



Additional Details(One of the two Options can be Selected)

Assemble □ Enable

Search ☑ Enable

Search Filter sAMAccountName=

Admin Search ☑ Enable

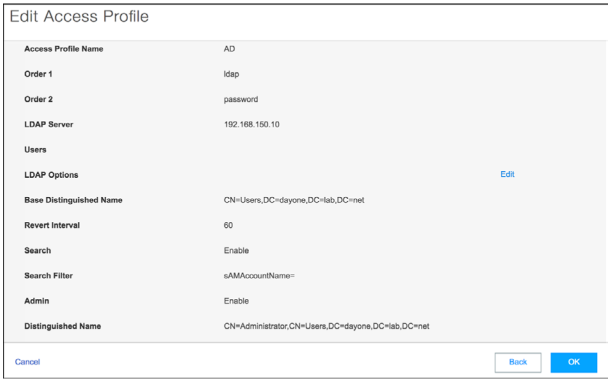
Distinguished Name * CN=Administrator,CN=Users,DC=dayone

Must not include a space

Password * ••••••••••

Figure 6.11 – LDAP Options (Search Parameters)

Click Next. Review your information as shown in Figure 6.12, and if everything seems fine, click OK:



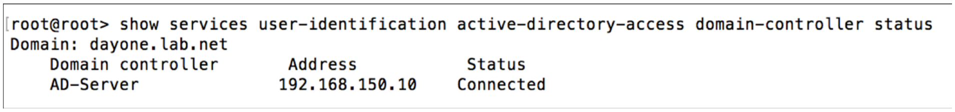
Edit Access Profile

Access Profile Name	AD
Order 1	ldap
Order 2	password
LDAP Server	192.168.150.10
Users	
LDAP Options	
Base Distinguished Name	CN=Users,DC=dayone,DC=lab,DC=net
Revert Interval	60
Search	Enable
Search Filter	sAMAccountName=
Admin	Enable
Distinguished Name	CN=Administrator,CN=Users,DC=dayone,DC=lab,DC=net

Figure 6.12 Access Profile Review

Commit your configuration.

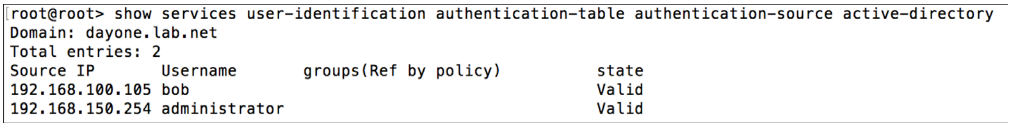
You can check the AD Server status from the CLI. In operational mode, use the `show services user-identification active-directory-access domain-controller status` command. A `Connected` status message should appear like the one in Figure 6.13:



```
root@root> show services user-identification active-directory-access domain-controller status
Domain: dayone.lab.net
    Domain controller        Address          Status
    AD-Server              192.168.150.10    Connected
```

Figure 6.13 Domain Controller Status

You can also check for authenticated users by using the `show services user-identification authentication-table authentication-source active-directory` in operational CLI mode as shown in Figure 6.14:



```
root@root> show services user-identification authentication-table authentication-source active-directory
Domain: dayone.lab.net
Total entries: 2
Source IP       Username       groups(Ref by policy)          state
192.168.100.105 bob                                           Valid
192.168.150.254 administrator                                 Valid
```

Figure 6.14 AD Connected Users

Configuring Application Visibility and Control

Now, let's configure the SRX to identify and enforce applications.

First, you need to download and install an application pack. The application pack is the signature database that AppSecure uses to identify applications.

On J-Web, navigate to Configure/Security/Applications/App Signatures and click the Download button:

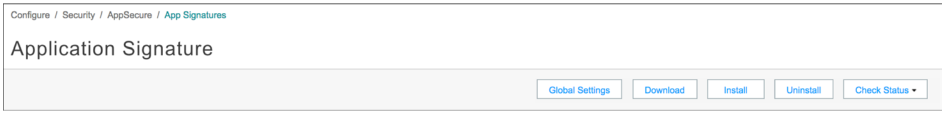
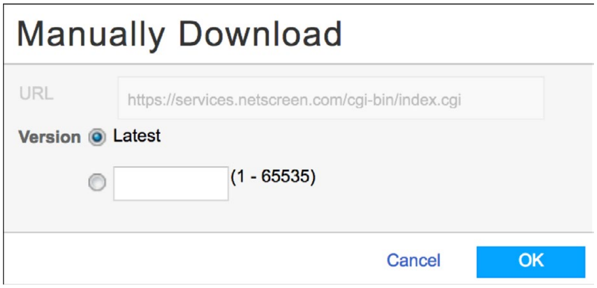


Figure 6.15 Application Signature Settings

Because you are executing a manual download, the system will present you with a few options, such as "download the latest signature pack" or "download a specific package." Select Latest and click OK:



URL https://services.netscreen.com/cgi-bin/index.cgi

Version ● Latest

○ (1 - 65535)

Figure 6.16 Application Signature Download

Check on the download status by clicking the Check Status button and selecting the Download Status option:

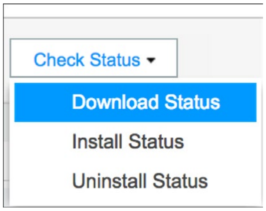
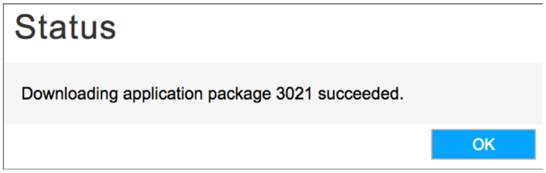


Figure 6.17 Application Signature Download Status

When the download is done, click on Download Status. You'll get will a message similar to Figure 6.18:

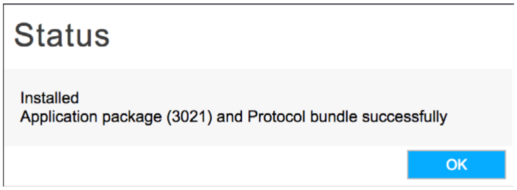


Status

Downloading application package 3021 succeeded.

Figure 6.18 Application Signature Download Succeeded Message

Click on Install. When the installation is done, clicking on Install Status will present a similar message to the screen in Figure 6.19:

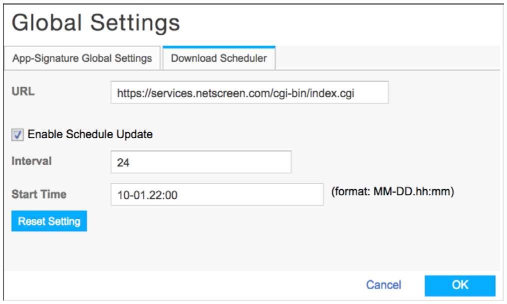


Status

Installed
Application package (3021) and Protocol bundle successfully

Figure 6.19 Application Signature Installation Status Message

If you want to enable automatic signature updates, click on Global Settings and select the Download Scheduler tab. You can define the update interval (hours) and the Start Time:



Global Settings

URL: https://services.netscreen.com/cgi-bin/index.cgi

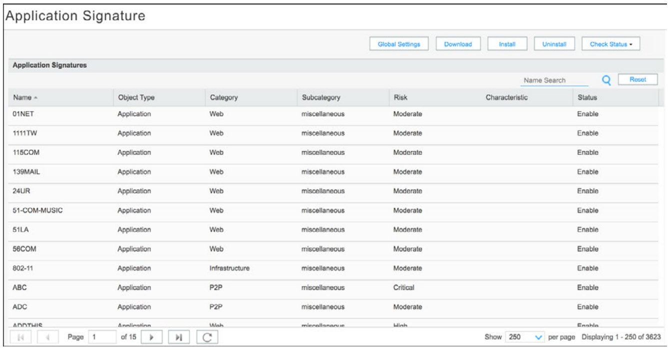
☑ Enable Schedule Update

Interval: 24

Start Time: 10-01.22:00 (format: MM-DD.hh:mm)

Figure 6.20 Application Signature Automatic Download Settings

Check that everything is fine by navigating to Configure/Security/AppSecure/Application Signatures and verifying that the Application Signatures are loaded as shown Figure 6.21. You can also perform searches for specific applications and sort the applications based on Name, Type, Category, Subcategory, Risk level, and Characteristics.



Application Signature

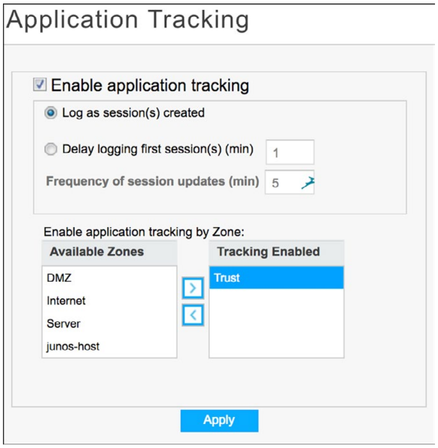
Application Signatures

Name	Object Type	Category	Subcategory	Risk	Characteristic	Status
01NET	Application	Web	miscellaneous	Moderate		Enable
1111TW	Application	Web	miscellaneous	Moderate		Enable
115COM	Application	Web	miscellaneous	Moderate		Enable
139MAIL	Application	Web	miscellaneous	Moderate		Enable
24UR	Application	Web	miscellaneous	Moderate		Enable
51-COM-MUSIC	Application	Web	miscellaneous	Moderate		Enable
51LA	Application	Web	miscellaneous	Moderate		Enable
56COM	Application	Web	miscellaneous	Moderate		Enable
802-11	Application	Infrastructure	miscellaneous	Moderate		Enable
ABC	Application	P2P	miscellaneous	Critical		Enable
ADC	Application	P2P	miscellaneous	Moderate		Enable
ADDTHIS	Application	Web	miscellaneous	High		Enable

Page 1 of 15 Show 250 per page Displaying 1 - 250 of 3623

Figure 6.21 AppSecure Application Signatures List

Now that you have the application signature database loaded, you can enable Application Tracking. To do that, click on App Tracking, under Configure/Security/AppSecure:



Application Tracking

☑ Enable application tracking

● Log as session(s) created

○ Delay logging first session(s) (min) 1

Frequency of session updates (min) 5

Enable application tracking by Zone:

Available Zones	Tracking Enabled
DMZ	Trust
Internet	
Server	
junos-host	

Figure 6.22 Application Tracking Configuration

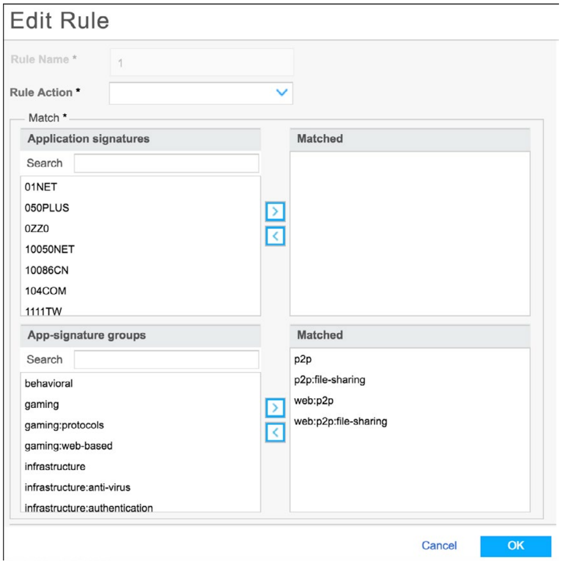
Click on Enable application tracking and select the Trust Zone as the tracking zone. Click on Apply.

Let’s create an application policy to block P2P applications.

On the Application Firewall page, click on the + sign. Name the Application Rule Set as *Block_P2P* and on *Rules*, under *Selected Rule Set*, click on the + sign. You are now adding rules to the application rule set.

NOTE This may seem complex, but in fact, it's a powerful tool. Once you get used to it you can add several rules and conditions to the rule set and once you reference it in a security policy, all of these conditions are evaluated all at once.

Let's name the Rule as *1*. As Rule Action, select Deny, and on the App Signature groups, select all the p2p related groups:



Edit Rule

Rule Name * 1

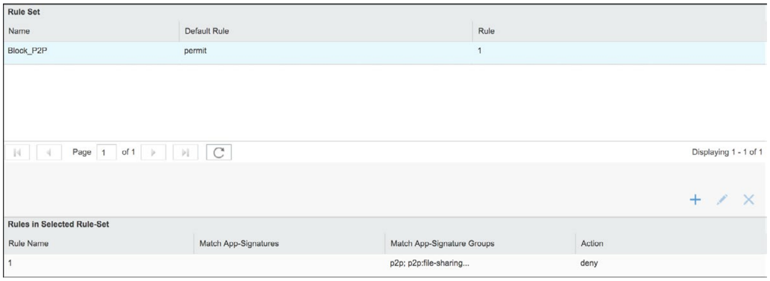
Rule Action *

Match *

p2p
p2p:file-sharing
web:p2p
web:p2p:file-sharing

Figure 6.23 *Application Rule Configuration*

Click OK and your rule set should be similar to the one shown in Figure 6.24:



Rule Set

Name	Default Rule	Rule
Block_P2P	permit	1

Rules in Selected Rule-Set

Rule Name	Match App-Signatures	Match App-Signature Groups	Action
1		p2p; p2p:file-sharing...	deny

Figure 6.24 *Application Firewall Rule Set*

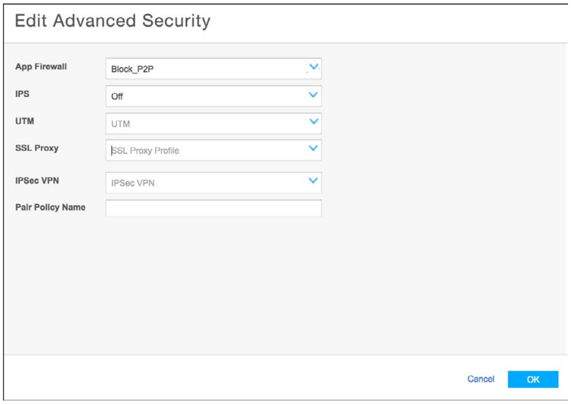
So, basically, you created an application that will block all P2P related traffic and allow all the other apps. This is because application rule sets are based on the concept of a default rule action that will permit, reject, or deny the traffic and an opposite action that will be applied to the applications in the rules. Now, all that remains is to invoke the AppFW rule set from a security policy.

NOTE Sometimes you will verify that an unknown application is displayed in the logs. The Junos UNKNOWN keyword is reserved for unknown dynamic applications. In the following cases, the application ID is set to Junos UNKNOWN:

- The traffic does not match an application signature in the database.
- The system encounters an error when identifying the application.
- The session fails over to another device.

Let's edit the *All_Trust_Internet* policy (Trust to Internet) by selecting the policy and clicking on the pencil (edit) button.

On Advanced Security, select the App FW Rule Set, *Block_P2P,* on the App Firewall configuration:



Edit Advanced Security

App Firewall: Block_P2P

IPS: Off

UTM: UTM

SSL Proxy: SSL Proxy Profile

IPSec VPN: IPSec VPN

Pair Policy Name:

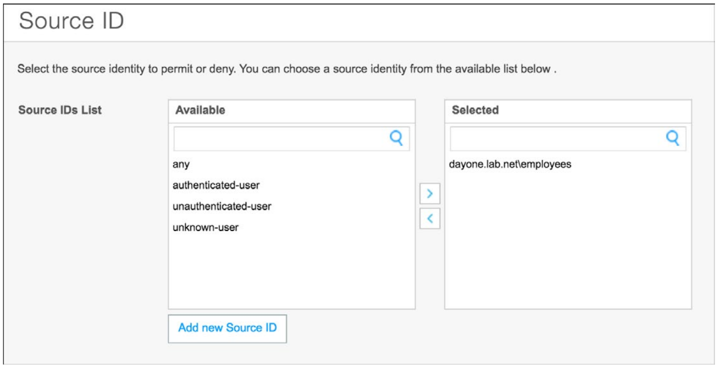
Figure 6.25 Enabling AppFW in a Security Policy

Click OK, save, and then commit your configuration.

Enabling User Firewall

Let's add a Source ID to the security policy, so the SRX can enforce policies on user identities instead of IP addresses only. To achieve this, edit the same security policy where you just enabled AppFW.

Click in User ID field, then add a new Source ID with the format *domain\group*, where group is the AD group of users that you want to manage:



Source ID

Select the source identity to permit or deny. You can choose a source identity from the available list below .

Source IDs List

Available
any
authenticated-user
unauthenticated-user
unknown-user

Selected
dayone.lab.net\employees

Figure 6.26 Adding a New Source ID to a Security Policy

Click OK, save, and commit the changes.

Configuring SSL Proxy

SSL proxy, in the context of the SRX, can be divided into two different categories:

- *SSL Forward Proxy*: The ability to inspect SSL traffic from an inside-out perspective – for example, internal users trying to connect to Internet services.
- *SSL Reverse Proxy*: The ability to inspect SSL traffic from an outside-in perspective – for example, external users trying to connect to internal services.

The SRX supports both methods, but this book focuses only on the SSL forward proxy configuration. It's also important to mention that if none of the advanced security services (AppFW, IDP, or AppTrack) are configured in a given security policy, then SSL proxy services are bypassed even if an SSL proxy profile is attached to the firewall policy.

NOTE At the time this book was being written, not all SRX models supported SSL Proxy. Always check your specific model documentation for details.

SSL forward proxy configuration can be achieved from both the CLI and the GUI. As this is a one-time task, let's execute it from a CLI perspective, because simply put, it's faster and administrators can take advantage of that fact.

First, let's start by configuring a root CA (certificate authority) certificate. You can generate a SRX certificate or import one. Here, we will use the SRX to generate its own root CA.

From operational mode, generate a PKI public/private key pair for a local digital certificate by issuing the following command (this can take a while):

```
request security pki generate-key-pair certificate id (certificate-id name) size (2048) type rsa
```

From operation mode, define a self-signed certificate to your specific domain (use the command below as a template and adjust with your domain):

```
request security pki local-certificate generate-self-signed certificate-id (certificate id name) domain-
name dayone.lab.net subject DC=dayone.lab.net,CN=dayone,OU=Education add-ca-constraint
```

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

```
set services ssl proxy profile (profile name) root-ca (certificate id name)
```

Commit the configuration.

It's time to configure the CA profile group. From operational mode, load the list of trusted CA certificates. You can use the pre-loaded list of root CAs on Junos, or import one of your preference. Here, we're using the Junos pre-loaded list. The command is:

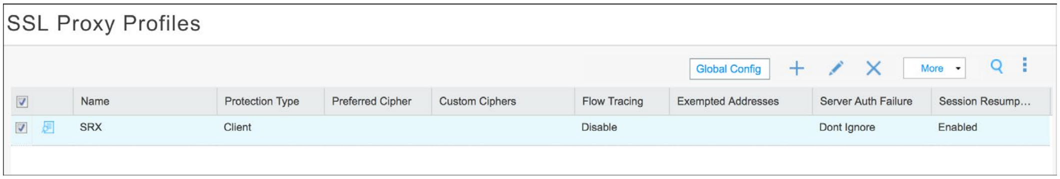
```
request security pki ca-certificate ca-profile-group load ca-group-name root-ca filename default
```

After the **`root-ca`** list is loaded, from configuration mode, attach the CA profile group to the SSL proxy profile:

```
set services ssl proxy profile (profile name) trusted-ca all
```

Commit the configuration. This concludes the CLI part of the configuration.

Now let's customize the SSL Proxy using the GUI. On J-Web, navigate to Configure/SSL Proxy, and select the SSL Proxy profile you just created. Click on Edit:

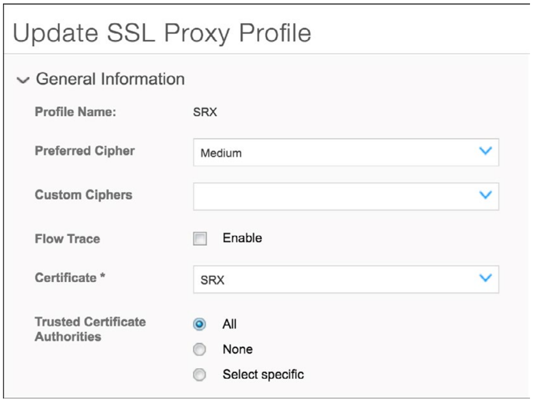


SSL Proxy Profiles

☑		Name	Protection Type	Preferred Cipher	Custom Ciphers	Flow Tracing	Exempted Addresses	Server Auth Failure	Session Resump...
☑		SRX	Client			Disable		Dont Ignore	Enabled

Figure 6.27 SSL Proxy Profile

In the Update SSL Proxy Profile page, on Preferred Cipher, select *Medium*, and on Trusted Certificated Authorities, click in the *All* option:



Update SSL Proxy Profile

General Information

Profile Name: SRX

Preferred Cipher: Medium

Custom Ciphers:

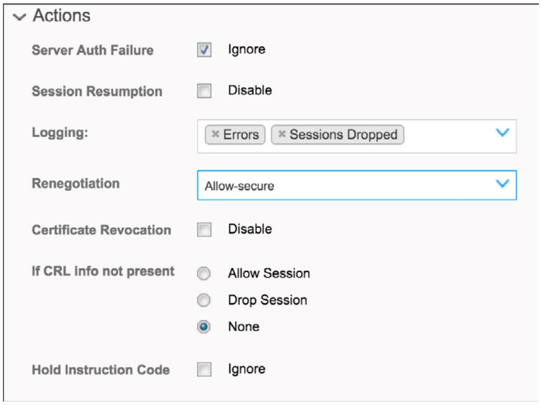
Flow Trace: □ Enable

Certificate *: SRX

Trusted Certificate Authorities: ● All ○ None ○ Select specific

Figure 6.28 *Edit the SSL Proxy Profile*

Scrolling down the page, under Actions, click on the Ignore button in the *Server Auth Failure* option. For logging, select *Errors* and *Sessions Dropped*. On Renegotiation, select the *Allow-secure* option:



Actions

Server Auth Failure: ☑ Ignore

Session Resumption: □ Disable

Logging: × Errors × Sessions Dropped

Renegotiation: Allow-secure

Certificate Revocation: □ Disable

If CRL info not present: ○ Allow Session ○ Drop Session ● None

Hold Instruction Code: □ Ignore

Figure 6.29 *Application Signature Download (cont.)*

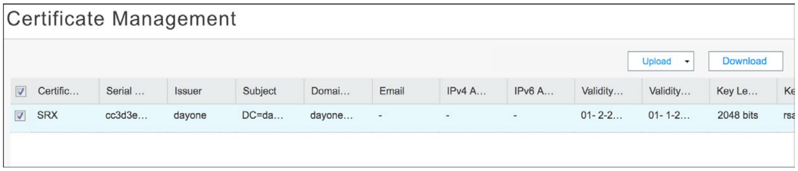
Review and save the SSL Proxy profile.

Exporting the SRX Root CA

In order to have your browser or system automatically trust all certificates signed by the root CA configured in the SSL proxy profile, you must instruct your platform or browser to trust the SRX CA root certificate. To do this, you need to load the SRX certificate into the client browsers.

NOTE There are several ways to distribute and import the certificate into client browsers (AD Group Policies, PKI, scripts, etc.), but that task is beyond the scope of this book.

Here, let's download the certificate from the SRX, so administrators can distribute it. Navigate to Administration/Certificate Management. Select the certificate generated previously and click on Download as shown in Figure 6.30:

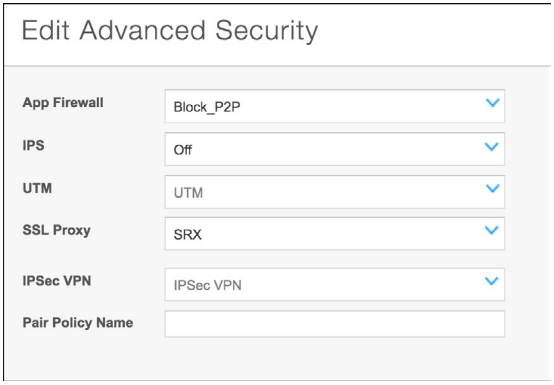

Certificate Management

☑	Certific...	Serial ...	Issuer	Subject	Domai...	Email	IPv4 A...	IPv6 A...	Validity...	Validity...	Key Le...	Ke
☑	SRX	cc3d3e...	dayone	DC=da...	dayone...	-	-	-	01- 2-2...	01- 1-2...	2048 bits	rsa

Figure 6.30 Certificate Management Screen

Enabling the SSL Proxy Profile in a Security Policy

Go back to your Trust to Internet security policy and add the SSL Proxy Profile on the Edit Advanced Security pane:


Edit Advanced Security

App Firewall	Block_P2P
IPS	Off
UTM	UTM
SSL Proxy	SRX
IPSec VPN	IPSec VPN
Pair Policy Name	

Figure 6.31 Enabling SSL Forward Proxy in a Security Policy

Click OK, save, and then commit your configuration.

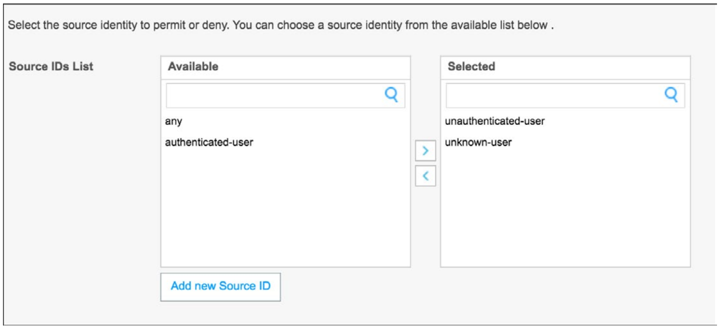
Configuring Captive Portal for Unauthenticated Users

The SRX can provide a captive portal to allow non-domain users or domain users on a non-domain machine to navigate upon authentication. The administrator specifies a captive portal to force the user to do firewall authentication. After the user enters their active directory name and password, the SRX gets firewall authentication and user or group information from the Active Directory server and can enforce the user firewall policy to control the user accordingly.

In addition to captive portal, if the IP address or user information is not available from the event log, the user can again log in to the Windows PC to generate an event log entry. Then the system generates the user's authentication entry accordingly.

To configure a captive portal policy, create a new security policy. Then fill in the fields with the following information:

- Policy Name: *Unauthenticated_Users*
- Source Zone: *Trust*
- Source Address: *Trust_Network*
- Source Identity: *unauthenticated-user* and *unknown-user* (as detailed in Figure 6.32):



Select the source identity to permit or deny. You can choose a source identity from the available list below .

Source IDs List

Available: any, authenticated-user

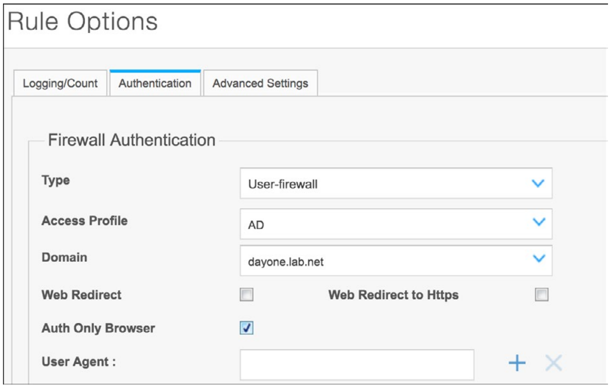
Selected: unauthenticated-user, unknown-user

Figure 6.32 Unauthenticated Users

- Destination Zone: *Internet*
- Destination Address: *any*
- Application: *any*
- Action: *permit*

In the Rule Options in Figure 6.32, select the following:

- Logging: *Enable Log Init and Log Close*
- Authentication Type: *User-firewall*
- Access Profile: *AD* (the profile created earlier)
- Domain: *dayone.lab.net* (insert your domain info here)
- Auth Only Browser: *Enable* (this will prevent the SRX from redirecting non-web browser requests to the captive portal)
- User Agent: Add *user agent information* here if you want to restrict the captive portal to specific user agents



Rule Options

Firewall Authentication

Type: User-firewall

Access Profile: AD

Domain: dayone.lab.net

Web Redirect ☐ Web Redirect to Https ☐

Auth Only Browser ☑

User Agent :

Figure 6.33 Authentication Options

WARNING Make sure the *Unauthenticated* policy is placed before any user-firewall policies.

Save and then commit. Now, users that are not authenticated will be presented with a captive portal when navigating over HTTP:

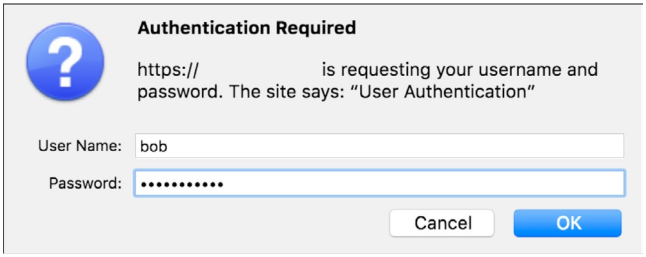
To enable captive portal over HTTPS, you need to add a SSL profile termination to the secure policy. To do this, go to the CLI and add the following commands:

```
set services ssl termination profile Unauthenticated server-certificate SRX
```

Add the SSL termination profile to the security policy with the following:

```
set security policies from-zone Trust to-zone Internet policy Unauthenticated then permit firewall-authentication user-firewall ssl-termination-profile Unauthenticated
```

Once committed, the following authentication screen will be presented to non-authenticated users and once authenticated, they are allowed to navigate based on the next-generation firewall policy matching the user identity:



Authentication Required

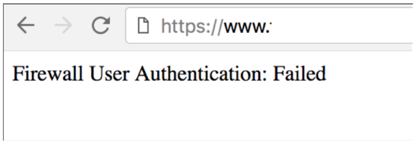
https://   is requesting your username and password. The site says: “User Authentication”

User Name: bob

Password: •••••••••••

Figure 6.34 *User Authentication Dialog*

If the user fails to authenticate, Figure 6.35 will be displayed:



https://www.

Firewall User Authentication: Failed

Figure 6.35 *Failed User Authentication*

Chapter 7

Unified Threat Management

Unified threat management, or UTM, is the combination of multiple advanced security features in a single appliance designed to protect networks while simplifying their infrastructure.

Traditionally, UTM combined network security, email security, and web security together in a single solution. Today, leading UTM solutions have also added advanced persistent threats detection, anti-botnet, and other security functions to their UTM.

This chapter covers basic UTM functionalities in the SRX, like Antivirus, Antispam, Content Filtering, and Web Filtering.

More advanced features like advanced persistent threat detection and anti-botnet will be discussed in Chapter 10.

Antivirus Overview

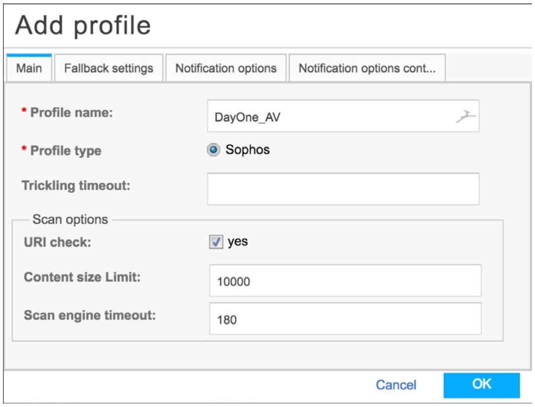
The SRX antivirus is a cloud-based antivirus solution. The virus pattern and malware database are located on external servers, thus there is no need to download and maintain large pattern databases on the SRX. The antivirus scanner also uses a local internal cache to maintain query responses from the external list server to improve lookup performance.

Because a significant amount of traffic processed by the Antivirus engine is HTTP based, Uniform Resource Identifier (URI) checking is used to effectively prevent malicious content from reaching the endpoint client or server. The following checks are performed for HTTP(S) traffic: URI lookup, true file type detection, and file checksum lookup.

SRX antivirus engine supports the following application layer protocols: HTTP, HTTPS (using SSL-FP), FTP, SMTP, POP3, and IMAP.

Configuring the Antivirus Profile

On the J-Web GUI open the path, Configure/Security/UTM/Antivirus, and then click on the + sign. You'll get the Add profile screen shown in Figure 7.1. In the Main tab, name the AV profile according to your preference and fill the other parameters as shown:



Add profile

Main | Fallback settings | Notification options | Notification options cont...

* Profile name: DayOne_AV

* Profile type: ● Sophos

Trickling timeout:

Scan options

URI check: ☑ yes

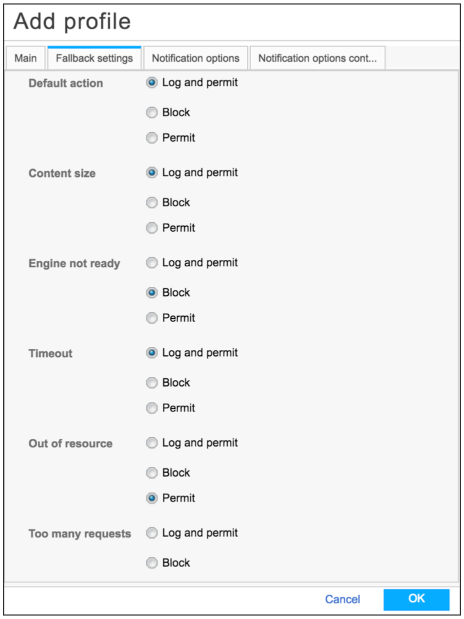
Content size Limit: 10000

Scan engine timeout: 180

Cancel | OK

Figure 7.1 AV Profile Page

Next, configure the Fallback settings tab fields, using your own preferences:



Add profile

Main | Fallback settings | Notification options | Notification options cont...

Default action: ● Log and permit ○ Block ○ Permit

Content size: ● Log and permit ○ Block ○ Permit

Engine not ready: ○ Log and permit ● Block ○ Permit

Timeout: ● Log and permit ○ Block ○ Permit

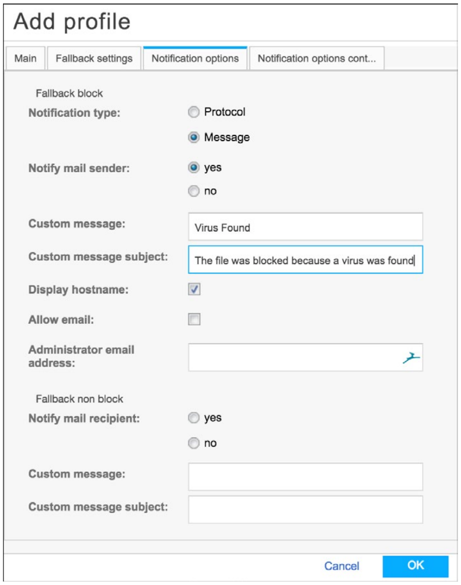
Out of resource: ○ Log and permit ○ Block ● Permit

Too many requests: ○ Log and permit ○ Block

Cancel | OK

Figure 7.2 AV Fallback Options

In the Notification options tab, define your custom message to alert users when a virus a found:



Add profile

Fallback block

Notification type: ○ Protocol ● Message

Notify mail sender: ● yes ○ no

Custom message: Virus Found

Custom message subject: The file was blocked because a virus was found

Display hostname: ☑

Allow email: ☐

Administrator email address:

Fallback non block

Notify mail recipient: ○ yes ○ no

Custom message:

Custom message subject:

Figure 7.3 AV Notification Options

Click on OK. This concludes the configuration of the AV profile.

Web Filtering Overview

SRX UTM Enhanced Web Filtering (EWF) is an integrated URL filtering solution that intercepts HTTP and HTTPS requests and sends the URL or the Server Name Identifier information (for HTTPS) to the URL filter cloud service

The cloud service categorizes the URL into one of the predefined categories and also provides site reputation information. The cloud then returns the URL category and the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the cloud.

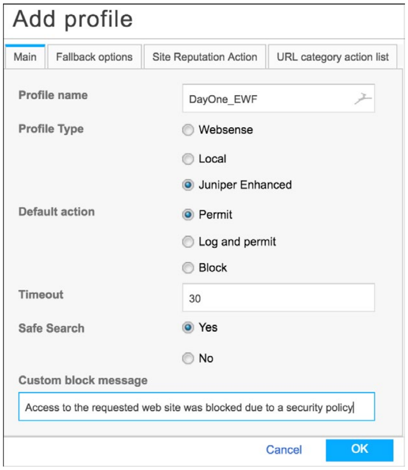
It's important to mention that the SRX supports the analysis of URLs even on HTTPS traffic without the need of having a SSL Forward Proxy enabled.

This is achieved by intercepting HTTPS traffic passing through the SRX Series device and analyzing the Server Name Indication (SNI), which is an extension of the SSL/TLS header that carries the destination server's hostname during the HTTPS client hello exchange. SRX uses this server name along with the destination IP address to send the query for the web filtering service.

NOTE Since only the server name is available during the handshake, you cannot block specific links within a website using this feature. Hence, you would have to deploy the SSL Forward Proxy if you want to perform a more granular filtering.

Configuring the Web Filtering Profile

On J-Web, go to Configure/Security/UTM/Web Filtering and click on the + sign to get a new Add profile page, and then name the EWF profile according to your preference and fill in the other parameters in the Main tab as shown in Figure 7.4. Make sure you selected the Juniper Enhanced option in the Profile Type:



Profile name: DayOne_EWF

Profile Type: ○ Websense ○ Local ● Juniper Enhanced

Default action: ● Permit ○ Log and permit ○ Block

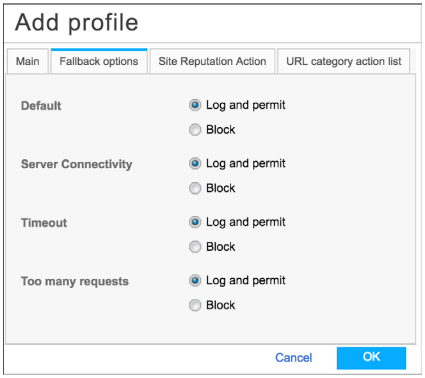
Timeout: 30

Safe Search: ● Yes ○ No

Custom block message: Access to the requested web site was blocked due to a security policy

Figure 7.4 EWF Profile Page

Next, configure the fields in the Fallback options tab with your preferences . Leave the Site Reputation Actions tab alone for now:



Default: ● Log and permit ○ Block

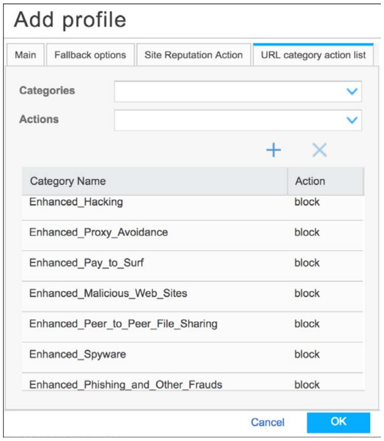
Server Connectivity: ● Log and permit ○ Block

Timeout: ● Log and permit ○ Block

Too many requests: ● Log and permit ○ Block

Figure 7.5 EWF Fallback Options

In the URL category action list tab, select the categories you want to block. As an example, Figure 7.6 adds a few categories that should not be permitted on any regular corporate network:



Category Name	Action
Enhanced_Hacking	block
Enhanced_Proxy_Avoidance	block
Enhanced_Pay_to_Surf	block
Enhanced_Malicious_Web_Sites	block
Enhanced_Peer_to_Peer_File_Sharing	block
Enhanced_Spyware	block
Enhanced_Phishing_and_Other_Frauds	block

Figure 7.6 EWF URL Category List

Click on OK.

This concludes the configuration of the EWF profile.

Content Filtering Overview

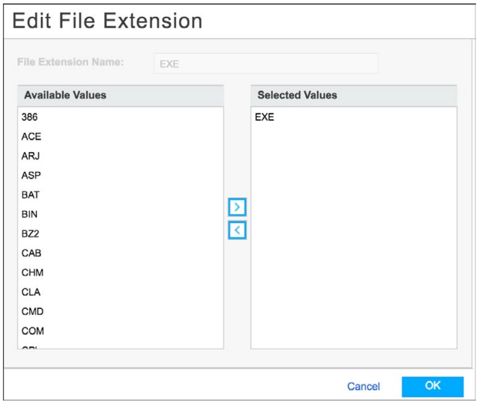
Content Filtering provides basic data loss prevention functionality. It blocks traffic based on MIME type, file extension, and protocol commands. You can also use the content filter module to block ActiveX, Java Applets, and other types of content.

Configuring the Content Filtering Profile

Before setting up the content filtering profile, let's create a custom object so you can block executables in the SRX.

First, go to Configure/Security/UTM/Custom Objects. Select the Filename Extension list tab and click on the + sign.

Create a File Extension profile called *EXE* and select the EXE extension, as you can see in Figure 7.7:



Edit File Extension

File Extension Name: EXE

Available Values

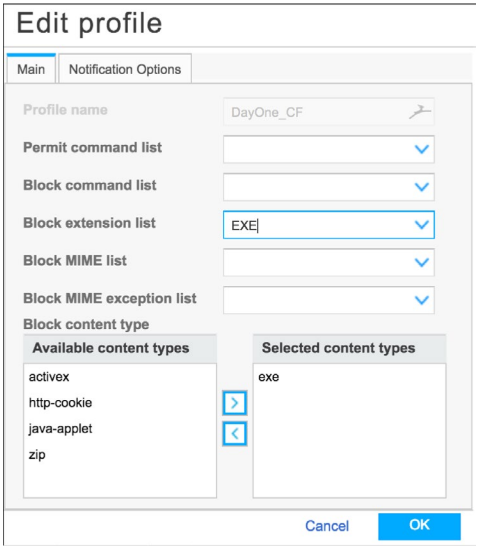
386
ACE
ARJ
ASP
BAT
BIN
BZ2
CAB
CHM
CLA
CMD
COM

Selected Values

EXE

Figure 7.7 *CF Extension Page*

Click OK. Go to the Content Filtering page and click on the + sign. On the Main tab, name the Content Filtering profile according to your preference and on the Block extension list, select the EXE option (the custom profile you just created). Under Block Content Types, select exe:



Edit profile

Profile name: DayOne_CF

Permit command list:

Block command list:

Block extension list: EXE

Block MIME list:

Block MIME exception list:

Block content type

Available content types

activex
http-cookie
java-applet
zip

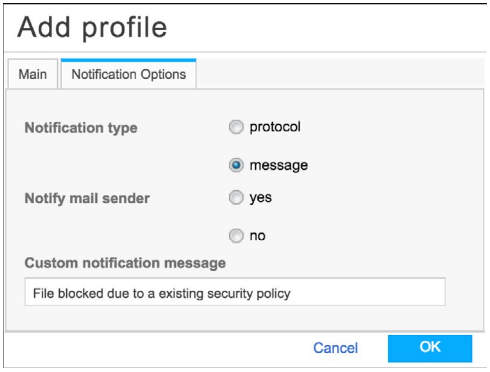
Selected content types

exe

Figure 7.8 *FC Profile Page*

NOTE You can also add a list of commands to block or permit, along with different MIME types, in the Custom Objects page.

On the Notification options tab, create a message that will alert users about the content filtering policy in place:



Add profile

Main | Notification Options

Notification type ○ protocol ● message

Notify mail sender ○ yes ○ no

Custom notification message

File blocked due to a existing security policy

Figure 7.9 *CF Notification Options*

Click OK. This concludes the configuration of the CF profile.

Antispam Overview

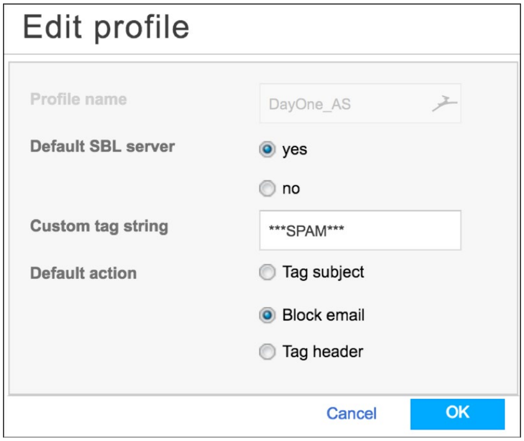
Antispam filtering allows you to tag or block unwanted email traffic by scanning inbound and outbound SMTP email traffic. Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and, optionally, to create your own local whitelists and blacklists for filtering against email messages.

The Antispam service tracks malicious or rogue SMTP servers and email spam accounts and block or tags emails that match the blacklists.

Configuring the Antispam Profile

Follow the GUI path to Configure/Security/UTM/Antspam and click on the + sign to create a new anti-spam profile.

Just add a name to the new profile and define it if you are using the default reputation server and mark the default action of how do you want to handle emails considered to be spam.



Edit profile

Profile name: DayOne_AS

Default SBL server: ● yes ○ no

Custom tag string: ***SPAM***

Default action: ○ Tag subject ● Block email ○ Tag header

Figure 7.10 Antispam Profile Page

Click OK when you're finished. This concludes the configuration of the antispam profile.

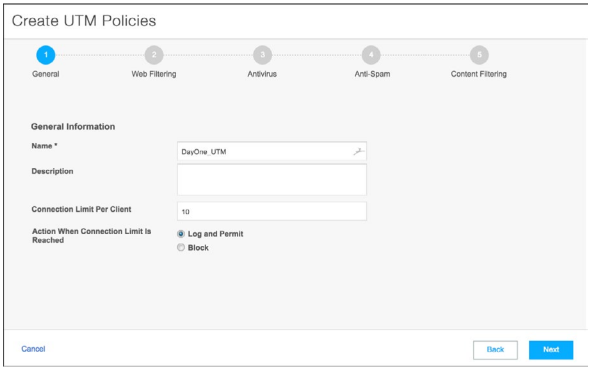
Configuring the UTM Policy and Attaching it to a Security Policy

Now that all the UTM services are configured, you just need to create a UTM policy that includes all the services and attach it to a firewall rule.

Go to Configure/Security/UTM/Policy and click on the + sign.

Click on the Launch Wizard button.

Name your UTM policy and the other parameters according to your preference:



Create UTM Policies

General Information

Name *: DayOne_UTM

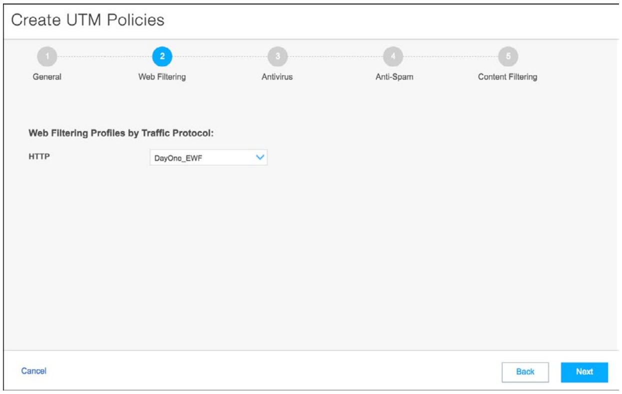
Description:

Connection Limit Per Client: 10

Action When Connection Limit Is Reached: ● Log and Permit ○ Block

Figure 7.11 UTM Policy Wizard

Click Next. In the Web Filtering profile page, select the profile you created earlier:



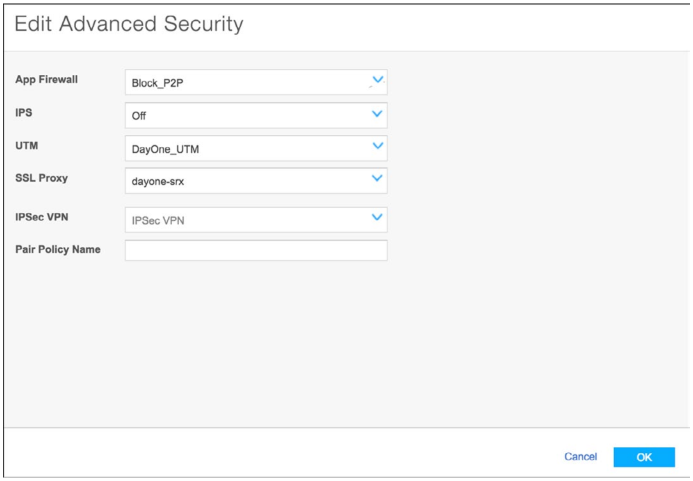
Create UTM Policies

Web Filtering Profiles by Traffic Protocol:

HTTP DayOne_EWF

Figure 7.12 UTM Policy Web Filtering Profile Definition

Do the same for the other profiles and when you're done, click Finish. Go back to your Trust to Internet security policy and add the UTM policy on the Advanced Security pane as shown in 7.13:



Edit Advanced Security

App Firewall Block_P2P

IPS Off

UTM DayOne_UTM

SSL Proxy dayone-srx

IPSec VPN IPSec VPN

Pair Policy Name

Figure 7.13 Adding a UTM Policy to a Security Policy

Enabling the UTM Services and Checking the Status

Finally, you just need to enable the cloud-based UTM services, so they can establish the connectivity with their respective cloud services.

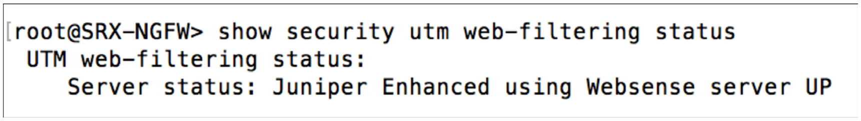
To enable the anti-virus service, go to the Junos CLI, and in configuration mode, use the following command:

```
root@SRX-NGFW# set security utm feature-profile anti-virus type sophos-engine
```

To enable the web filtering service, use this command:

```
root@SRX-NGFW# set security utm feature-profile web-filtering type juniper-enhanced
```

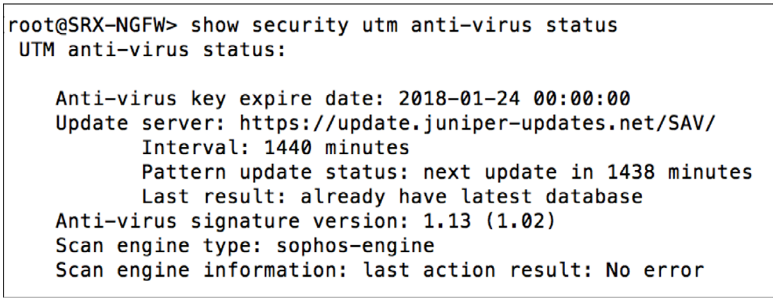
Commit the configuration. You can check the services status for the web filter using the `show security utm web-filtering status` command:



```
[root@SRX-NGFW> show security utm web-filtering status
 UTM web-filtering status:
    Server status: Juniper Enhanced using Websense server UP
```

Figure 7.14 UTM EWF Service Status

And for anti-virus status use the `show security utm anti-virus status` command:



```
root@SRX-NGFW> show security utm anti-virus status
 UTM anti-virus status:

    Anti-virus key expire date: 2018-01-24 00:00:00
    Update server: https://update.juniper-updates.net/SAV/
           Interval: 1440 minutes
           Pattern update status: next update in 1438 minutes
           Last result: already have latest database
    Anti-virus signature version: 1.13 (1.02)
    Scan engine type: sophos-engine
    Scan engine information: last action result: No error
```

Figure 7.15 UTM AV Service Status

NOTE You can also check the UTM services statistics in the J-Web GUI, under the path: Monitor/UTM.

Chapter 8

Intrusion Prevention Systems

An intrusion prevention system (IPS) is a network security technology that examines network traffic flows to detect and prevent exploits. Exploits are usually in the form of a malicious intrusion to a network service that allows attackers to gain control of an application or an operational system. This chapter covers the basics of an IPS and how to enable and configure it in the SRX Series.

Understanding the SRX Intrusion Prevention System

The SRX intrusion prevention systems engine inspects all packets from a given flow looking for exploits and malwares, up to the application layer.

To do this, the IPS engine relies on two methodologies:

- *Protocol Anomalies:* Developed by the Juniper Signature team, it is custom-written code to ensure that traffic behaves to specifications (for example RFC, vendor specifications). A Protocol Anomaly method by definition protects against Zero Day attacks, looking for inputs that are not according to the protocol, service, or application specifications.
- *Signature-Based:* The IPS engine uses stateful signature-based attack objects. The signatures are written to protect systems against vulnerabilities. The IPS engine checks every packet against all loaded signatures looking for a match. If one is found, then the IPS engine will act as configured.

Attack objects can be composed of multiple signatures and protocol anomalies, including logical expressions between signatures for compound matching. This offers greater flexibility when creating signatures as match conditions that can be linked, reducing the chance of false positives.

Let's take a closer look at how it works.

In the following example, it is a simple IPS signature-based attack object that looks for executable files in an HTTP transaction and when matched, triggers a response from the IPS to close the session from the client side:

```
recommended-action close-client;
severity major;
attack-type {
   chain {
      scope transaction;
      expression pattern01 or pattern02;
      member pattern01 {
         attack-type {
            signature {
               context http-header;
               pattern  \[filename\]=.*\.\[exe\];
               direction server-to-client;

      member pattern02 {
         attack-type {
            signature {
               context http-get-url-parsed;
               pattern .*\.\[exe\];
               direction client-to-server;
```

Thinking about logical conditions, the following conditions should happen for this signature to be triggered:

- Condition 1 – HTTP protocol;
- Condition 2 – Client-to-server or server-to-client;
- Condition 3 – HTTP header or GET URL;
- Condition 4 – Filename ending with .exe.

It's important to note that by the very action of inspecting all packets looking for patterns, conditions, and anomalies, IPS systems can affect the network device performance and they need to be used wisely, with laser focus.

The primary use case of an IPS is to protect exposed applications and services from non-trusted networks.

NOTE The SRX Series comes with thousands of pre-defined and validated signatures but administrators can also create their own, if desired or needed.

How the IPS Policy Works

Similar to the firewall security policies, the IPS also has security policies that control the attack detection engine. IPS policy enables selective enforcement of various attack detection and prevention techniques on network traffic passing through the engine.

At first, users can find it strange for the IPS engine to have its own policies apart from the firewall policies, but it makes sense for environments with separated teams that manage firewall and IPS, or devices with users with different roles. For example, an administrator can have permission only to manage firewall policies while other administrators can manage only the IPS piece.

This dual capability allows administrators to write very granular rules to match a section of traffic based on zones, networks, and applications. Administrators can then apply specific attack prevention techniques on that traffic, and take active or passive preventive actions.

Figure 8.1 illustrates the structural view of an SRX IPS policy. It can consist of two types of rulebases – an IPS rulebase and an exempt rulebase:

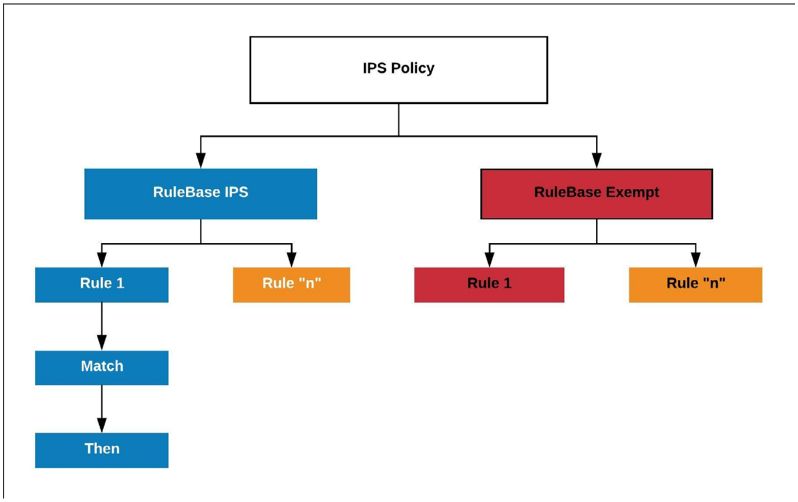


Figure 8.1 *IPS Policy Conditions*

A rulebase is a collection of rules and the SRX Series supports two types of rulebases:

- *IPS rulebase*: Traffic you want to match in a policy and perform inspection upon.
- *Exempt rulebase*: Traffic you want to exclude from the IPS engine because you know they are false positives or because you want to exclude a specific source, destination, or source/destination pair from matching an IPS rule.

Rules contain configuration objects and are similar in structure to security policies because they use configuration objects to create match conditions and resulting actions. Once you create an IPS policy, then you reference it in a security policy, just like you did for AppFW or UTM.

NOTE Although many IPS policies might exist within the configuration, only one IPS policy is active on a SRX device at a given time.

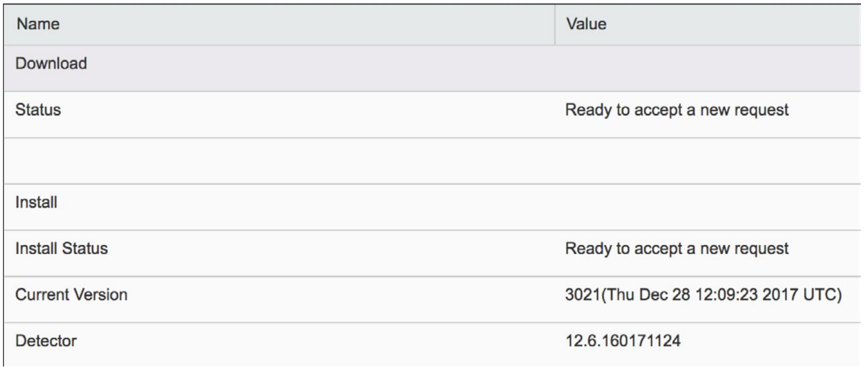
Getting Started with IPS

Based on this book's reference topology in Figure 1.4, let's enable an IPS policy to protect the web server in the DMZ against attacks coming from the Internet.

First, you need to load the signature database and policy templates.

On J-Web, go to Configure/Security/IPS/Signature Update. The steps are exactly the same as those when loading the AppSecure database, so they are not reproduced here – it's a good time to practice your command of the GUI.

After you're done, a screen similar to Figure 8.2 should appear in your IPS Signature Update screen:



Name	Value
Download	
Status	Ready to accept a new request
Install	
Install Status	Ready to accept a new request
Current Version	3021(Thu Dec 28 12:09:23 2017 UTC)
Detector	12.6.160171124

Figure 8.2 IPS Signature Status

Now let's create an IPS policy. When starting with IPS it's a good idea to use Templates. Juniper Networks provides predefined policy templates that administrators can use as a starting point for creating their own policies. Each template is set of rules of a specific rulebase type that you can copy and then update according to your requirements.

Each policy template contains rules that use the default actions associated with the attack objects. You should customize these templates to work on your network by selecting your own source and destination addresses and choosing IPS actions that reflect your security needs. Table 8.1 lists the IPS template types and their descriptions.

Table 8.1 SRX IPS Protection Templates

Template Name	Description
Client-And-Server-Protection	Designed to protect both clients and servers. To be used on high memory devices with 2 GB or more of memory.
Client-And-Server-Protection-1G	Designed to protect both clients and servers. To be used on all devices, including low-memory branch devices.
Client-Protection	Designed to protect clients. To be used on high memory devices with 2 GB or more of memory.
Client-Protection-1G	Designed to protect clients. To be used on all devices, including low-memory branch devices.
DMZ Services	Protects a typical demilitarized zone (DMZ) environment.
DNS Server	Protects Domain Name System (DNS) services.
File Server	Protects file sharing services, such as Network File System (NFS), FTP, and others.
Getting Started	Contains very open rules. Useful in controlled lab environments, but should not be deployed on heavy traffic live networks.
IDP Default	Contains a good blend of security and performance.
Recommended	Contains only the attack objects tagged as recommended by Juniper Networks. All rules have their Actions column set to take the recommended action for each attack object.
Server-Protection	Designed to protect servers. To be used on high memory devices with 2 GB or more of memory.
Server-Protection-1G	Designed to protect servers. To be used on all devices, including low-memory branch devices.
Web Server	Protects HTTP servers from remote attacks.

To download the Templates, go to IPS/Policy, click on the Download button, and Select the Download Template option, shown in Figure 8.3:

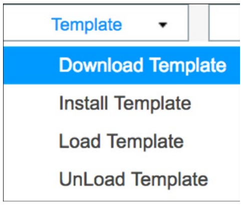
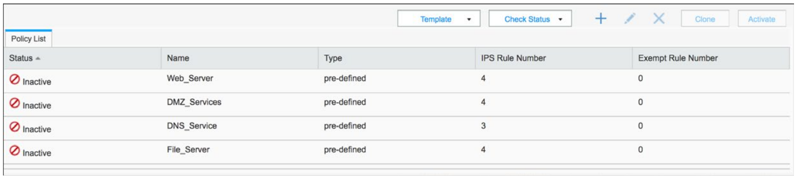


Figure 8.3 Download Template Button

When the download is done, proceed with the Install.

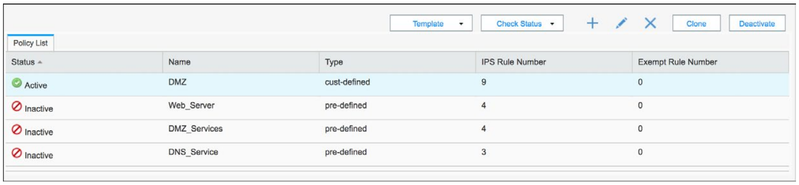
After the installation is concluded, select the Load Template option (it can take a few minutes to load). After loading, your IPS Policy screen should look like Figure 8.4:



Status	Name	Type	IPS Rule Number	Exempt Rule Number
⊘ Inactive	Web_Server	pre-defined	4	0
⊘ Inactive	DMZ_Services	pre-defined	4	0
⊘ Inactive	DNS_Service	pre-defined	3	0
⊘ Inactive	File_Server	pre-defined	4	0

Figure 8.4 IPS Policy List

For a basic installation, let's work with a recommended template. Select it and click on Clone. Name the new template *DMZ*. Select the newly created template and click on Activate in Figure 8.4. You will notice that in Figure 8.5, the new Policy has a green icon and the status has changed to Active:



Status	Name	Type	IPS Rule Number	Exempt Rule Number
✓ Active	DMZ	cust-defined	9	0
⊘ Inactive	Web_Server	pre-defined	4	0
⊘ Inactive	DMZ_Services	pre-defined	4	0
⊘ Inactive	DNS_Service	pre-defined	3	0

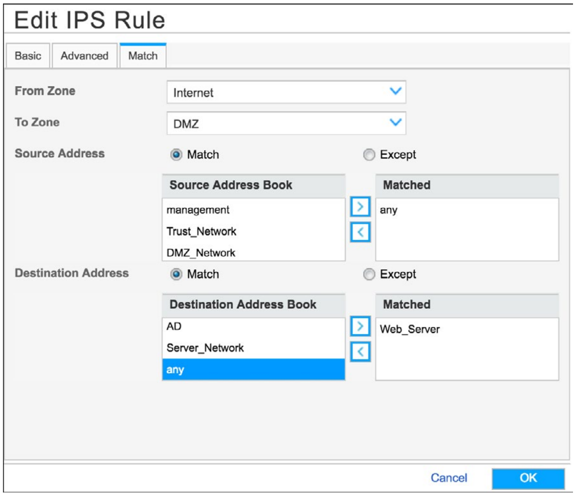
Figure 8.5 Active IPS Policy

Customizing the IPS Rules and Attaching Them to a Security Policy

On Rulebase IPS, remove all the rules except TCP/IP, HTTP, and malware (remember that we only have a web server in our DMZ).

Select each rule, click on Edit, and under the Match tab, configure it with the items here:

- Source Zone: *Internet*
- Destination Zone: *DMZ*
- Source Address: *Any*
- Destination *Address: Web Server* (if you don't have the Web_Server object, create it now)



From Zone: Internet

To Zone: DMZ

Source Address: ● Match ○ Except

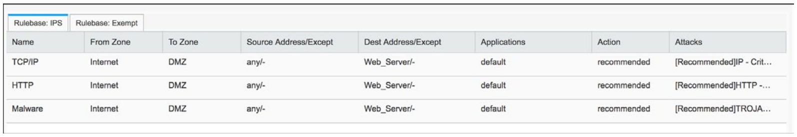
Source Address Book	Matched
management	any
Trust_Network	
DMZ_Network	

Destination Address: ● Match ○ Except

Destination Address Book	Matched
AD	Web_Server
Server_Network	
any	

Figure 8.6 *IPS Rule Configuration*

Your rules should now look like Figure 8.7:

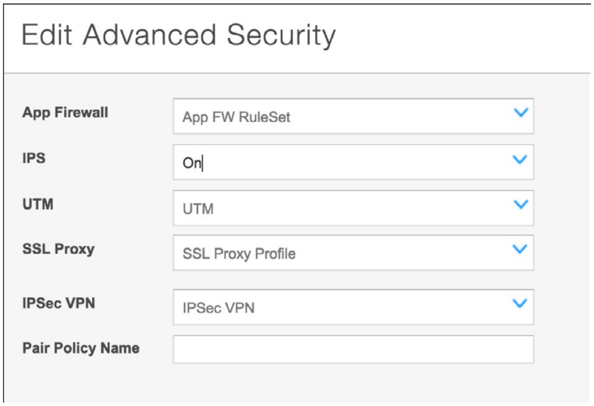


Name	From Zone	To Zone	Source Address/Except	Dest Address/Except	Applications	Action	Attacks
TCP/IP	Internet	DMZ	any/-	Web_Server/-	default	recommended	[Recommended]IP - Crit...
HTTP	Internet	DMZ	any/-	Web_Server/-	default	recommended	[Recommended]HTTP -...
Malware	Internet	DMZ	any/-	Web_Server/-	default	recommended	[Recommended]TROJA...

Figure 8.7 *IPS Policy Rules*

Move on to the Configure/Security/Firewall Policy/Rules page, select your Internet to DMZ policy, and edit it.

On the Advanced Security page, enable the IPS, as shown in Figure 8.8, then save and commit the configuration:



Edit Advanced Security

App Firewall: App FW RuleSet

IPS: On

UTM: UTM

SSL Proxy: SSL Proxy Profile

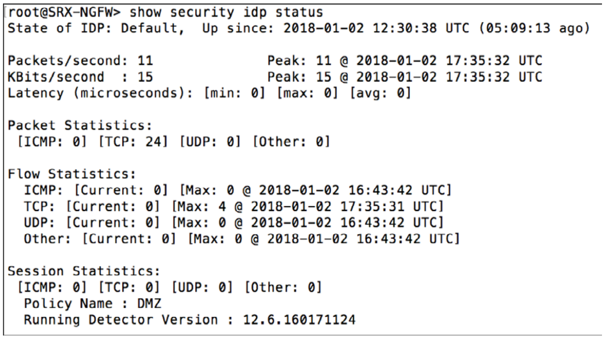
IPSec VPN: IPSec VPN

Pair Policy Name:

Figure 8.8 *Enabling IPS in a Security Policy*

NOTE You created an IPS policy to protect traffic from the Internet against the DMZ, although this book recommends inspecting traffic from all networks against restricted zones. Keep in mind that careful planning and consideration is needed to configure the policies that will keep your network secure, avoid false-positives or false-negatives, and will not affect the overall SRX performance.

You can monitor the IPS status using both the GUI and the CLI, as will be discussed in Monitoring in Chapter 13, but for now, let's check it on the Junos CLI. From operational mode, use the `show security ips status` command as shown in Figure 8.9:



```
root@SRX-NGFW> show security idp status
State of IDP: Default,  Up since: 2018-01-02 12:30:38 UTC (05:09:13 ago)

Packets/second: 11              Peak: 11 @ 2018-01-02 17:35:32 UTC
KBits/second  : 15              Peak: 15 @ 2018-01-02 17:35:32 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 24] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2018-01-02 16:43:42 UTC]
  TCP: [Current: 0] [Max: 4 @ 2018-01-02 17:35:31 UTC]
  UDP: [Current: 0] [Max: 0 @ 2018-01-02 16:43:42 UTC]
  Other: [Current: 0] [Max: 0 @ 2018-01-02 16:43:42 UTC]

Session Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]
  Policy Name : DMZ
  Running Detector Version : 12.6.160171124
```

Figure 8.9 *IPS Status*

As you can see, the IPS is up, it is analyzing packets, and the active IPS Policy is DMZ.

Chapter 9

Denial of Service (DoS) Attack Mitigation

Denial of Service (DoS) attacks are trouble and headaches for network and security engineers, grossly affecting business and critical services worldwide. From our viewpoint, they can be divided into two major groups – *volumetric* or *application* DoS attacks – each with its own characteristics and both needing to be addressed with a slightly different approach.

Volumetric attacks look to flood servers, systems, or networks with traffic in order to overwhelm the victim's resources and make it difficult or impossible for legitimate users to use them.

Application attacks look to overwhelm an application with requests that may or may not be legitimate, with the intent of keeping the target application unable to service valid users.

While it's true that the SRX Series is not a DoS mitigation solution, it has several features designed to protect itself and the network behind it from several types of common DoS attacks.

Understanding SCREENS

The SRX Series provides various detection and defense mechanisms at the zone level that can protect against denial of service attacks, and SCREENS are a set of techniques that help protect the network against certain types of basic attacks and malicious traffic. It also saves precious system resources, because it is evaluated in the very early stages of the traffic processing sequence.

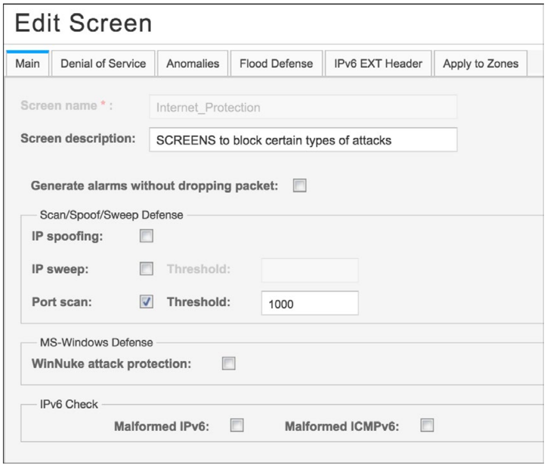
In a nutshell, when SCREENS detect and block an attack, the SRX does not have to perform the follow up, and more intensive, processing.

Configuring a SCREENS Policy and Attaching It to a Zone

In this example, you are going to configure a SCREENS policy to prevent bad traffic from the Internet reaching your internal network.

On J-Web, go to Configure/Security/Objects/Zones/Screens. Click on the SCREENS list tab and click on the + sign to create a new SCREEN.

In the Main tab, give the SCREEN a name, here, *Internet_Protection,* and Enable Port Scan with a threshold of *1000:*



Screen name * : Internet_Protection

Screen description: SCREENS to block certain types of attacks

Generate alarms without dropping packet: □

Scan/Spoof/Sweep Defense

IP spoofing: □

IP sweep: □ Threshold:

Port scan: ☑ Threshold: 1000

MS-Windows Defense

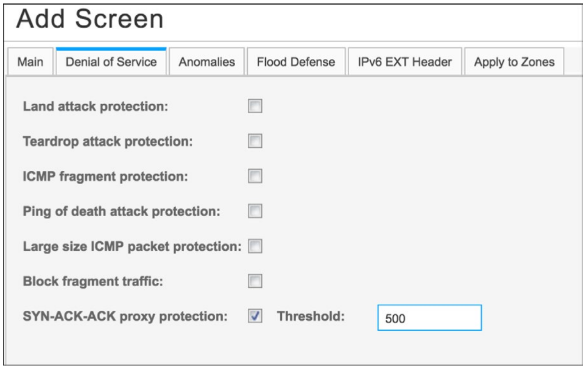
WinNuke attack protection: □

IPv6 Check

Malformed IPv6: □ Malformed ICMPv6: □

Figure 9.1 *SCREEN Configuration*

Next, on the Denial of Service tab, enable the SYN-ACK-ACK proxy protection:



Land attack protection: □

Teardrop attack protection: □

ICMP fragment protection: □

Ping of death attack protection: □

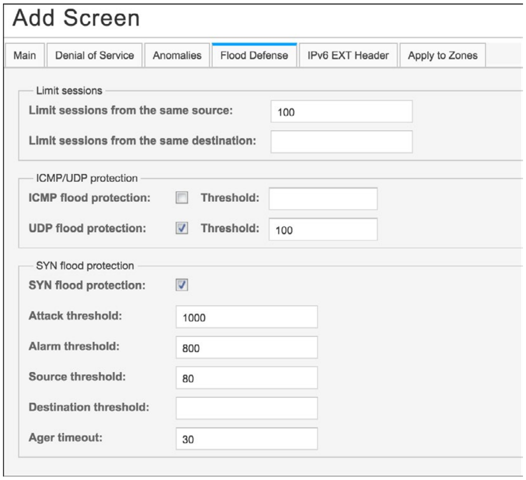
Large size ICMP packet protection: □

Block fragment traffic: □

SYN-ACK-ACK proxy protection: ☑ Threshold: 500

Figure 9.2 *SCREEN (Denial of Service Protection Settings)*

On the Flood Defense tab, limit the sessions from the same source to 100, enable UPD flood protection and set the threshold to 100 packets, and enable the SYN flood protection, setting the attack threshold to 1000, the Alarm threshold to 800, the Source threshold to 80, and the Ager timeout to 30, as shown in Figure 9.3:



Limit sessions

Limit sessions from the same source: 100

Limit sessions from the same destination:

ICMP/UDP protection

ICMP flood protection: □ Threshold:

UDP flood protection: ☑ Threshold: 100

SYN flood protection

SYN flood protection: ☑

Attack threshold: 1000

Alarm threshold: 800

Source threshold: 80

Destination threshold:

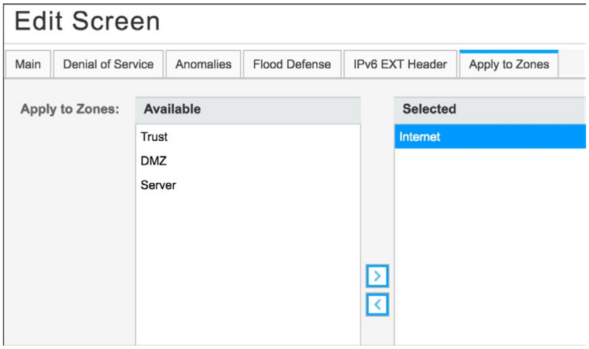
Ager timeout: 30

Figure 9.3 SCREEN Flood Defense Settings

Let's drill down a little on the SYN flood options in Figure 9.3. It's important to understand in more detail as the SYN flood mechanisms are usually the most-used ones:

- *Alarm threshold*: Number of proxied, half-complete, TCP connection requests per second before an alarm logs.
- *Attack threshold*: Number of SYN requests per second required to trigger the SYN proxy response.
- *Source threshold*: Number of SYN packets per second received from a single source.
- *Destination threshold*: Number of SYN requests per second received for a single destination.
- *Ager timeout*: Maximum length of time before a half-completed connection drop from the queue.

Now, moving to Apply to Zones tab, attach the *Internet_Protection* SCREENS to the Internet Zone:



Apply to Zones:

Available: Trust, DMZ, Server

Selected: Internet

Figure 9.4 Assigning the SCREEN to a Zone

Click OK and commit.

Configuring SYN Proxy and Session Table Aging

The SRX has two methods that can be used to proxy a new TCP session and identify if it's legitimate or not:

- *SYN Cookie*: SYN Cookies work by the SRX replying to all initial SYN packets with a SYN/ACK packet that contains the original source, destination, and port numbers as an encrypted hash as the ISN (initial sequence number). The SRX then discards this information and the SYN is not placed into the session table. If the client responds with the proper recalculate ACK, then the session is rebuilt and the SRX allows it.
- *SYN Proxy*: The standard RFC SYN proxy. It inspects sessions to validate if the proper handshake is executed, before allowing the session into the target server.

Let's set up the SYN Proxy mechanism. In the CLI, on configuration mode, use the following command:

```
set security flow syn-flood-protection-mode syn-cookie
```

It's also important to set a session table clean-up mechanism to avoid attacks designed to fill a FW session table. So, let's define the high-watermark – the SRX performs aggressive session aging when the number of sessions in the session table exceeds the high-watermark threshold value – to 90.

While still in configuration mode use:

```
set security flow aging high-watermark 90
```

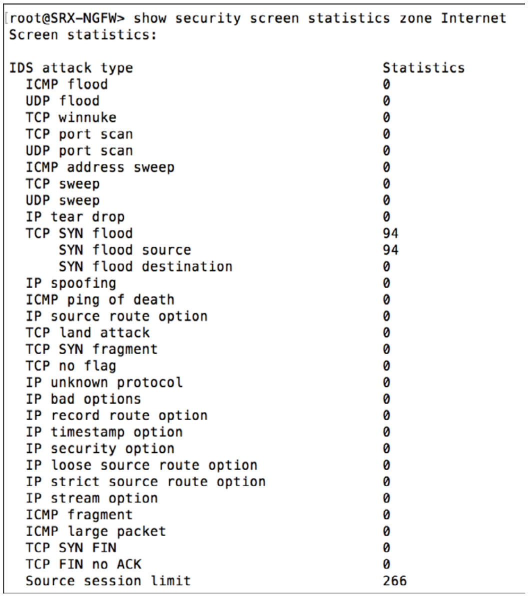
You also need to define the low-watermark – the SRX disables aggressive session aging and returns to normal, when the number of sessions in the session table goes below the low-watermark threshold.

In configuration mode use:

```
set security flow aging low-watermark 70
```

Then commit your configuration.

You can always check the statistics of your SCREEN policy by using the `show security screen statistics zone Internet` command, as shown with output in Figure 9.5:



```
root@SRX-NGFW> show security screen statistics zone Internet
Screen statistics:

IDS attack type                                 Statistics
  ICMP flood                                    0
  UDP flood                                     0
  TCP winnuke                                   0
  TCP port scan                                 0
  UDP port scan                                 0
  ICMP address sweep                            0
  TCP sweep                                     0
  UDP sweep                                     0
  IP tear drop                                  0
  TCP SYN flood                                 94
      SYN flood source                          94
      SYN flood destination                     0
  IP spoofing                                   0
  ICMP ping of death                            0
  IP source route option                        0
  TCP land attack                               0
  TCP SYN fragment                              0
  TCP no flag                                   0
  IP unknown protocol                           0
  IP bad options                                0
  IP record route option                        0
  IP timestamp option                           0
  IP security option                            0
  IP loose source route option                  0
  IP strict source route option                 0
  IP stream option                              0
  ICMP fragment                                 0
  ICMP large packet                             0
  TCP SYN FIN                                   0
  TCP FIN no ACK                                0
  Source session limit                          266
```

Figure 9.5 SCREEN Statistics

Indeed, it’s a useful command to help you tune your configuration.

NOTE It’s very important to tune the SCREENS options to your specific environment. Knowing the characteristics of your protected services (session limits, per example) will help you to build more effective policies.

TIP Also, it’s a good practice, while tuning the configuration, to use the `alarm-without-drop` option. With this option enabled, the SRX will count the packets that trigger a SCREEN policy but it won’t drop them.

Chapter 10

Zero Day Attack Prevention (Anti-APT)

Advanced Persistent Threats (APT) are attacks designed to bypass traditional security mechanisms, such as anti-virus and firewalls. They're extremely hard to detect and once a device is infected, they're also very hard remove.

The *advanced* part of an APT is related to all the sophisticated techniques used by hackers to hide malware from detection mechanisms, and, many times, it also refers to extremely advanced exploit techniques and knowledge about target systems.

The *persistent* part of APT describes the capability that any APT has to remain in an infected network, by using replication techniques and establishing a covert communication channel with a command and control server that is continuously sending commands to the agents and extracting data from the targets.

And of course, the *threat* part indicates the very real risk and impact caused by the attack.

Some defense mechanisms were created to support security professionals in fighting APTs, such as sandboxes, advanced behavior and anomaly detection tools, next generation anti-virus, and others, but many of them still rely on static analysis and monitoring techniques, which simply fuels hackers to develop new and inventive ways to bypass them.

Considering all of the above, Juniper Networks developed a new cloud-based machine learning solution, integrated it with the SRX, and designed it to learn and to adapt to new threat vectors. It's called *Sky Advanced Threat Prevention*, or *Sky ATP*.

Sky ATP Concepts

Sky ATP's identification technology uses a range of techniques to quickly identify a threat and prevent an impending attack. These range from rapid cache lookups to identify known files, to dynamic analysis using unique deception techniques applied in a sandbox environment, tricking malware into activating and self-identifying itself.

Patented machine learning algorithms allow Sky APT to adapt and identify new malware in the ever-changing threat landscape, allowing the solution to identify zero day attacks and eliminate threats before an attacker infiltrates the network. Once a zero-day threat is identified, the malware's signature is recorded in the lookup cache and widely propagated to stop similar attacks in the future.

If the malware is identified from inside the network, like a guest or roaming computer, the SRX can quarantine the infected computer, keeping the malware from spreading into other networks.

Let's take a closer look at how Sky ATP works:

1. A user in a protected zone receives an email with an attachment or downloads a file;
2. The SRX extracts the file and submits it to the Sky Cloud Service for analysis;
3. Sky ATP will initially compare the file against its cache database to verify if it's known malware;
4. If the file is new to Sky ATP, the file will be submitted to multiple AV scan engines for analysis;
5. After the AV Scan phase, if the file is not identified as malware, it will be sent to the Static Analysis engine for sandboxing;
6. Finally, the file is submitted to the Dynamic Engine, which applies machine learning and deception techniques to trick the malware into activating and self-identifying.

The cloud analysis process (see Figure 10.1) can take up to seven minutes, and during that time Sky ATP updates the SRX with information in order to block the malware to be delivered to its intended target (if the file is found to be malware), or the SRX can quarantine the infected computer (in a situation where the computer indicates other behaviors that indicate a compromised machine).

Sky ATP supports HTTP, HTTPS, SMTP, and IMAP protocols.

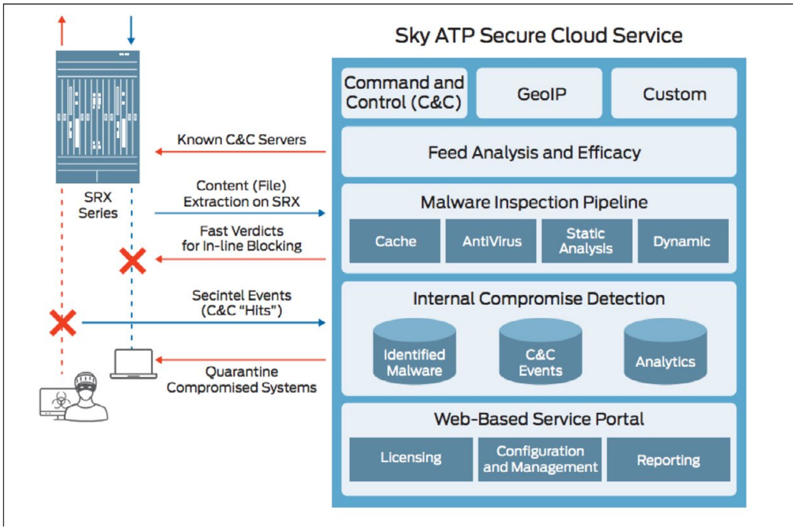

Sky ATP Secure Cloud Service
Command and Control (C&C)
GeoIP
Custom
Feed Analysis and Efficacy
Malware Inspection Pipeline
Cache
AntiVirus
Static Analysis
Dynamic
Internal Compromise Detection
Identified Malware
C&C Events
Analytics
Web-Based Service Portal
Licensing
Configuration and Management
Reporting
SRX Series
Known C&C Servers
Content (File) Extraction on SRX
Fast Verdicts for In-line Blocking
Secintel Events (C&C "Hits")
Quarantine Compromised Systems

Figure 10.1 Sky ATP Workflow

NOTE Juniper also extends its malware detection capabilities to on premise environments through another product, called *Advanced Threat Prevention Appliance*. Juniper can also extend the enforcement capabilities to third-party devices (beyond the SRX Series), by using its *Software Defined Secure Networks (SDSN)* solution. Both topics are beyond the scope of this book, but if you are reading this book, that's a sure indication you need to check the topics out at: https://www.juniper.net/us/en/products-services/security/.

IMPORTANT At the time this book was being written, not all SRX models supported Sky ATP. Please check your specific model documentation for details.

Enrolling the SRX Series Into Sky ATP Cloud Service

As mentioned, Sky ATP uses a cloud-based service to identify advanced malwares. This also applies to Sky ATP management.

First, the user needs to authorize the SRX to access the Sky ATP preferred cloud (AMER, EMEA, or APAC).

NOTE This is a process that must be done in conjunction with your Juniper account representative and requires a valid Sky ATP license. Also, it's important to mention that Sky ATP supports a *premium* license, allowing customers to submit executable files.

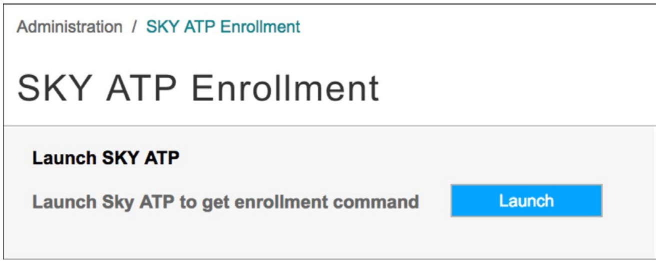
Second, you need to configure the SRX to run in enhanced services mode. This can only be done in the CLI, by issuing the following command in configuration mode:

```
set security forwarding-process enhanced-services-mode
```

WARNING After enabling enhanced mode, a reboot is required. Plan accordingly.

After the on-boarding and enabling enhanced mode are done, access your cloud of choice. In this example, it's the AMER cloud but the steps are identical in all clouds.

Let's get going. On J-Web, follow the path: Administration/Sky ATP Enrollment and click the Launch button shown in Figure 10.2:



Administration / SKY ATP Enrollment

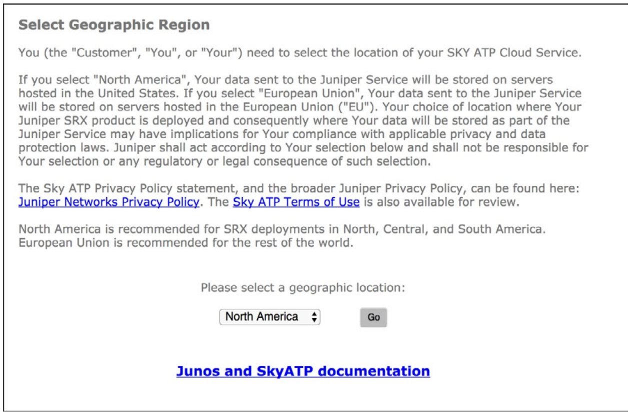
SKY ATP Enrollment

Launch SKY ATP

Launch Sky ATP to get enrollment command

Figure 10.2 Sky ATP Launch Enrollment Button

A browser tab will open with a message similar to Figure 10.3. This is where you choose your cloud of choice, and click on GO:



Select Geographic Region

You (the "Customer", "You", or "Your") need to select the location of your SKY ATP Cloud Service.

If you select "North America", Your data sent to the Juniper Service will be stored on servers hosted in the United States. If you select "European Union", Your data sent to the Juniper Service will be stored on servers hosted in the European Union ("EU"). Your choice of location where Your Juniper SRX product is deployed and consequently where Your data will be stored as part of the Juniper Service may have implications for Your compliance with applicable privacy and data protection laws. Juniper shall act according to Your selection below and shall not be responsible for Your selection or any regulatory or legal consequence of such selection.

The Sky ATP Privacy Policy statement, and the broader Juniper Privacy Policy, can be found here: Juniper Networks Privacy Policy. The Sky ATP Terms of Use is also available for review.

North America is recommended for SRX deployments in North, Central, and South America. European Union is recommended for the rest of the world.

Please select a geographic location:

North America

Junos and SkyATP documentation

Figure 10.3 Select Your Geographic Region

Now, you need to create a Sky ATP domain. On the Sky ATP login screen, click on Create a security realm in the lower left corner of Figure 10.4:

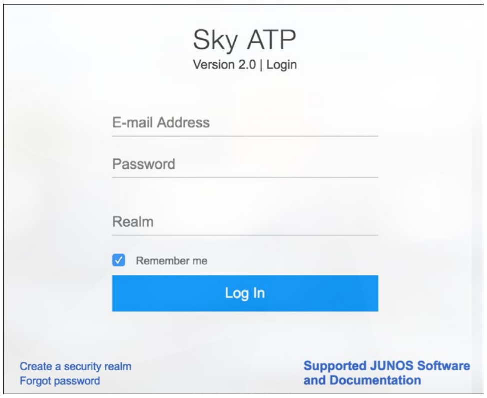
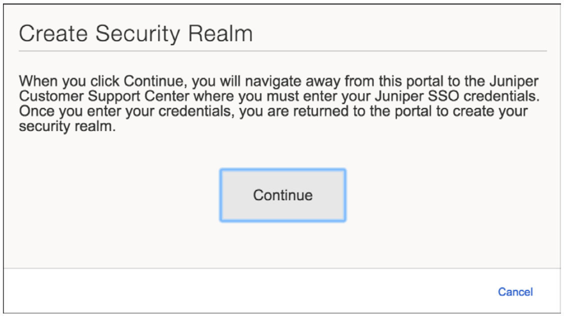


Figure 10.4 *Sky ATP Logon Screen*

The message in Figure 10.5 will appear:



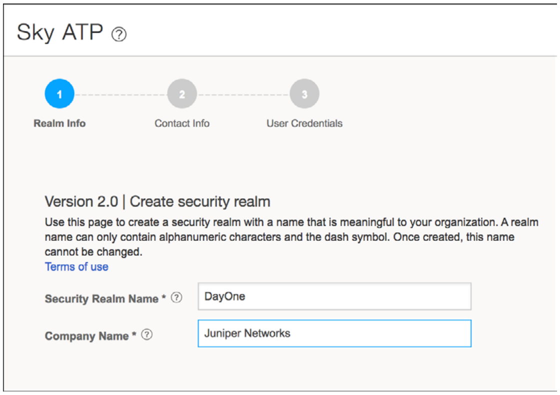
Create Security Realm

When you click Continue, you will navigate away from this portal to the Juniper Customer Support Center where you must enter your Juniper SSO credentials. Once you enter your credentials, you are returned to the portal to create your security realm.

Figure 10.5 *Create Security Realm Warning*

This means you need a valid Juniper credential to be able to continue. If you do not have it, contact your Juniper representative.

After logging in with a valid Juniper account, you will be presented with a wizard that will guide you in the process of setting up a security realm. First the wizard will ask for the security realm information:



Version 2.0 | Create security realm

Use this page to create a security realm with a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed.

Terms of use

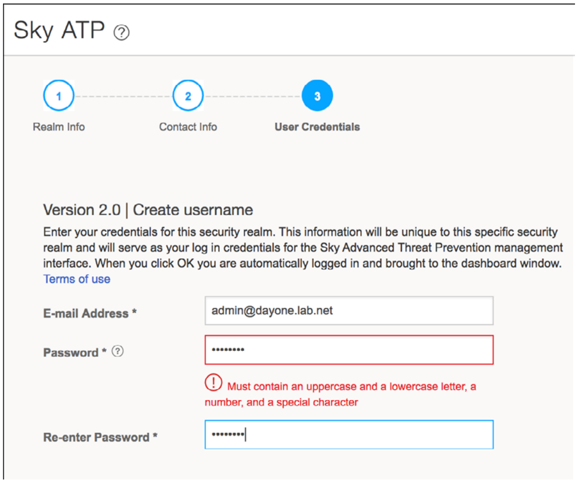
Security Realm Name * DayOne

Company Name * Juniper Networks

Figure 10.6 Security Realm Information

Next is your contact info (not shown here).

And finally, the administrator's, or user's credentials:



Version 2.0 | Create username

Enter your credentials for this security realm. This information will be unique to this specific security realm and will serve as your log in credentials for the Sky Advanced Threat Prevention management interface. When you click OK you are automatically logged in and brought to the dashboard window.

Terms of use

E-mail Address * admin@dayone.lab.net

Password * ••••••••

Must contain an uppercase and a lowercase letter, a number, and a special character

Re-enter Password * ••••••••

Figure 10.7 Create Security Realm Administrator

After you're done, the system will redirect you to the management console. The Sky ATP GUI is very similar to J-Web (and Security Director) as they all use the same framework and workflows. The SKY ATP GUI is divided into the five tabs shown in Figure 10.8:

- Dashboard
- Monitor – Events and Malware related information
- Devices – Enroll, Disenroll, and Device status
- Configure – Policies and Profiles
- Administration

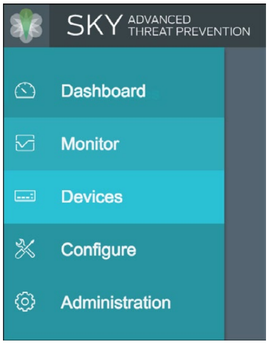
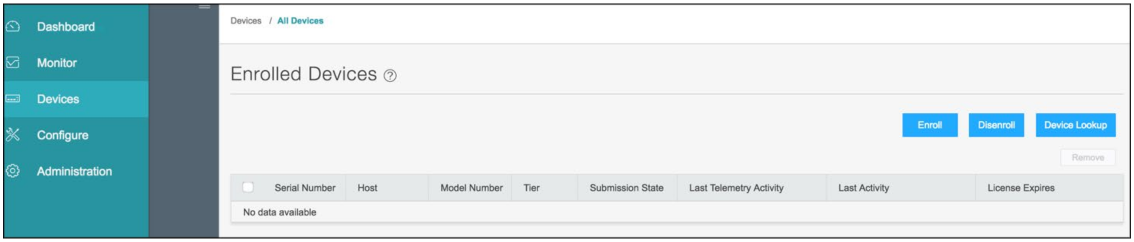


Figure 10.8 Sky ATP GUI Management Panels

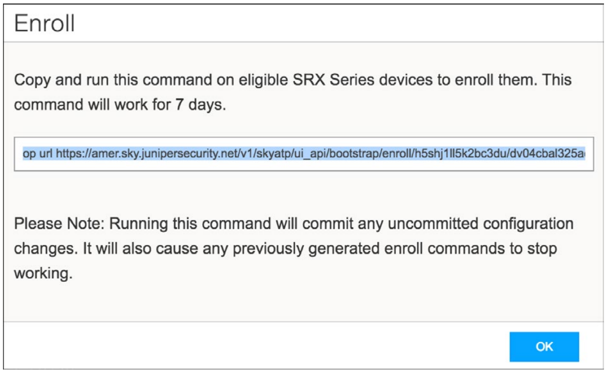
You need to enroll the SRX into Sky ATP. Click on Devices. As you can see in Figure 10.9, there are no devices enrolled yet. Click on Enroll:



☐	Serial Number	Host	Model Number	Tier	Submission State	Last Telemetry Activity	Last Activity	License Expires
No data available								

Figure 10.9 Sky ATP Devices Management Screen

An enrollment screen will appear (each SRX will have its own script generated automatically) with a message explaining that the script needs to be executed on the SRX. Copy the whole line as shown in Figure 10.10:



Enroll

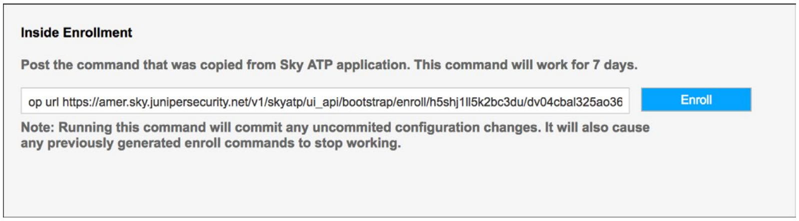
Copy and run this command on eligible SRX Series devices to enroll them. This command will work for 7 days.

```
op url https://amer.sky.junipersecurity.net/v1/skyatp/ui_api/bootstrap/enroll/h5shj1ll5k2bc3du/dv04cbal325a
```

Please Note: Running this command will commit any uncommitted configuration changes. It will also cause any previously generated enroll commands to stop working.

Figure 10.10 Copying the Enroll Script on SKY ATP GUI

Access the SRX J-Web GUI again and go to Administration/Sky ATP Enrollment. Paste the command, and click the Enroll button as shown in Figure 10.11:



Inside Enrollment

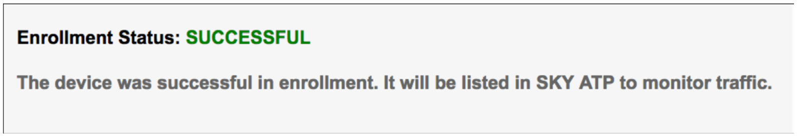
Post the command that was copied from Sky ATP application. This command will work for 7 days.

```
op url https://amer.sky.junipersecurity.net/v1/skyatp/ui_api/bootstrap/enroll/h5shj1ll5k2bc3du/dv04cbal325ao36
```

Note: Running this command will commit any uncommited configuration changes. It will also cause any previously generated enroll commands to stop working.

Figure 10.11 Executing the Enroll Script on SRX J-Web

The enrollment process takes several minutes to conclude. Once it's done, the following message will appear:

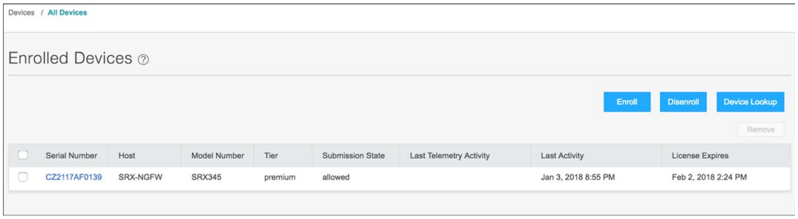


Enrollment Status: SUCCESSFUL

The device was successful in enrollment. It will be listed in SKY ATP to monitor traffic.

Figure 10.12 Enrollment Status

You should now be able to find the SRX Series in the Sky ATP management console, as in Figure 10.13:



Enrolled Devices

□	Serial Number	Host	Model Number	Tier	Submission State	Last Telemetry Activity	Last Activity	License Expires
□	CZ2117AF0139	SRX-NGFW	SRX345	premium	allowed		Jan 3, 2018 8:55 PM	Feb 2, 2018 2:24 PM

Figure 10.13 Device Discovered on SKY ATP Cloud

Configuring Sky ATP Threat Prevention Profile

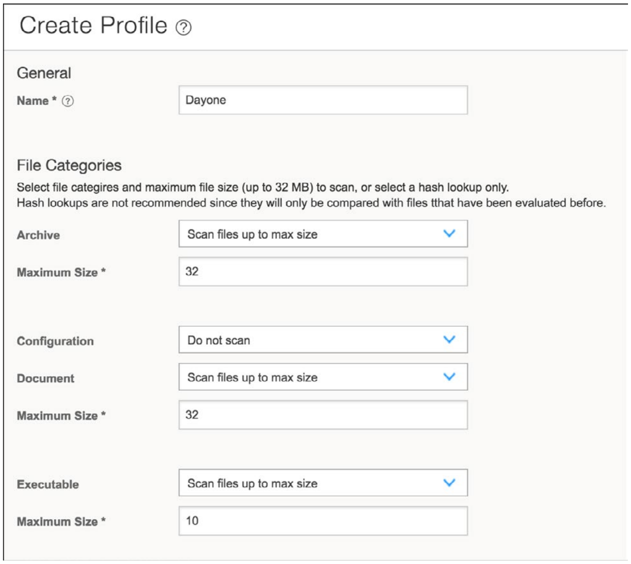
Once the SRX is enrolled into the Sky ATP cloud service, you need to define a threat prevention profile. A threat prevention profile allows administrators to define which files to send to the cloud for inspection, to create a whitelist or blacklist of IPs and URLs, and to define what threat level is required for a device to be quarantined. Table 10.1 lists the file types supported by Sky ATP:

Table 10.1 Sky ATP Supported File Types

Category	Description	Included File Types
Active media	Flash and Silverlight applications	.swf, .xap, .xbap
Archive	Archive files	.zip, .rar, .tar, .gzip
Code	Source code	.c, .cc, .cpp, .cxx, .h, .htt, .java
Config	Configuration files	.inf, .ini, .lnk, .reg, .plist
Document	All document types except PDFs	.chm, .doc, .docx, .dotx, .hta, .html, .pot, .ppa, .pps, .ppt, .pptsm, .pptx, .ps, .rtf, .rtf, .txt, .xlsx, .xml, .xsl, .xslt
Emerging threat	A special category that includes known threat source file types	n/a
Executable	Executable binaries	.bin, .com, .dat, .exe, .msi, .msm, .mst
Java	Java applications, archives, and libraries	.class, .ear, .jar, .war
Library	Dynamic and static libraries and kernel modules	.a, .dll, .kext, .ko, .o, .so, ocx
Mobile	Mobile applications for iOS and Android	.apk, .ipa
OS package	OS specific update applications	.deb, .dmg
Script	Scripting files	.bat, .js, .pl, .ps1, .py, .sct .sh, .tcl, .vbs, plsm, pyc, pyo
Portable document	PDF, e-mail, and MBOX files	.email, .mbox, .pdf, .pdfa

To configure the threat prevention policy, go back to the Sky ATP Web UI, and then go to Configure/File Inspection profile. Click on the + sign.

Give the profile a name (in the example shown in Figure 10.14, it's *DayOne)*. For each supported file category, define if you want to disable scanning, scan up to the maximum size (32 MB max), or to only submit the file hash:



Create Profile

General

Name *: Dayone

File Categories

Select file categires and maximum file size (up to 32 MB) to scan, or select a hash lookup only.
Hash lookups are not recommended since they will only be compared with files tthat have been evaluated before.

Archive: Scan files up to max size

Maximum Size *: 32

Configuration: Do not scan

Document: Scan files up to max size

Maximum Size *: 32

Executable: Scan files up to max size

Maximum Size *: 10

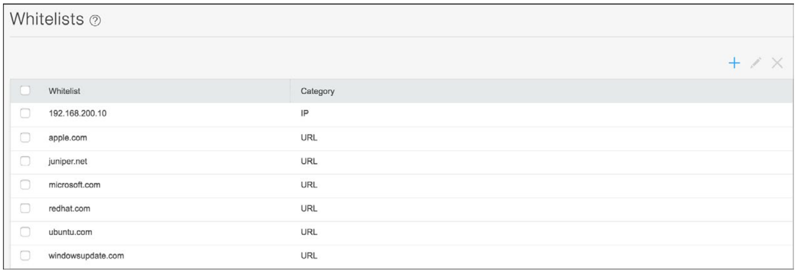
Figure 10.14 *File Inspection Profile*

NOTE It's important to remember that malwares are, by nature, very small in size. The majority of them are smaller than 1MB, and the largest go up to 10MB. This is because once a user hits an infected site or command-and-control server, the attacker wants to send as many malwares as possible, expecting that at least one will succeed in infecting a computer. This demands that malware be smaller in size, to avoid blocking or drawing too much attention to itself (from the user or from the network administrators). In this context, we can consider that 32MB is a very large file size and works in almost any environment.

Whitelists

Now let's create a whitelist (in other words, source URLs or IPs that we *don't* want to submit files to Sky ATP when receiving). Maneuver to Configure/Whitelists.

Add Trusted servers and URLs whose received files you don't want to inspect. In Figure 10.15, the DMZ Web Server was added and some trusted domains:

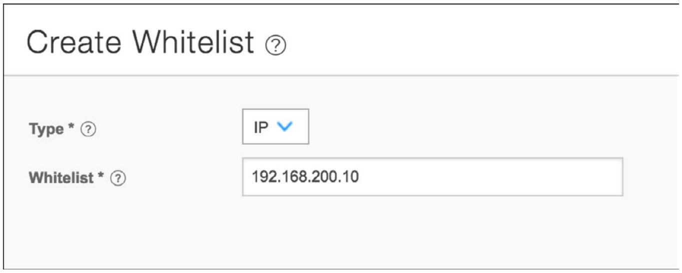


Whitelists ?

□	Whitelist	Category
□	192.168.200.10	IP
□	apple.com	URL
□	juniper.net	URL
□	microsoft.com	URL
□	redhat.com	URL
□	ubuntu.com	URL
□	windowsupdate.com	URL

Figure 10.15 Whitelists

To add an IP or URL, simply click on the + sign:



Create Whitelist ?

Type * ? IP

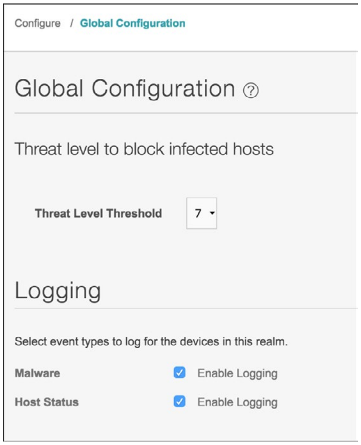
Whitelist * ? 192.168.200.10

Figure 10.16 Adding a Whitelist Object

Global Threat Level

We need to set up a global threat level. This defines when Sky ATP needs to instruct the SRX, or a SDSN infrastructure, to quarantine a computer that reaches the defined threat level.

On the Sky ATP GUI, go to Configure/Global Configure. You can accept the default value or modify it to another value. Also, enable malware and host status logging:



Configure / Global Configuration

Global Configuration

Threat level to block infected hosts

Threat Level Threshold 7

Logging

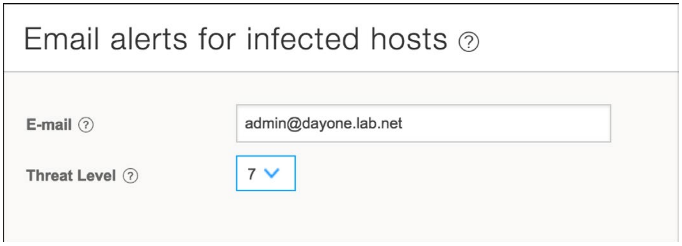
Select event types to log for the devices in this realm.

Malware ☑ Enable Logging

Host Status ☑ Enable Logging

Figure 10.17 Global Threat Configuration

On the same page, add an email to be notified when an infected host is found. This book recommends adding an alias, so administrative groups can be notified, rather than just one individual. You can also define the threat level that will trigger an email notification:



Email alerts for infected hosts

E-mail: admin@dayone.lab.net

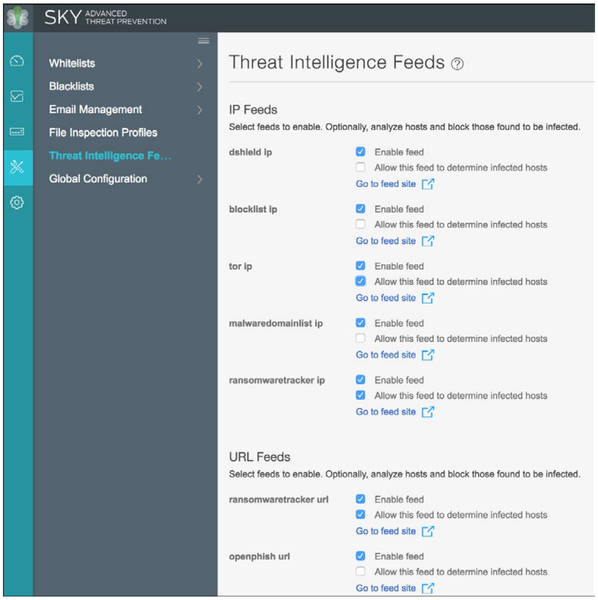
Threat Level: 7

Figure 10.18 Email Notification

Configuring Sky ATP Intelligence Threat Feeds

Sky ATP also offers threat feeds that allow dynamic blocking of threats, based on several categories, such as command-and-control servers, malware distribution sites, phishing sites, bad reputation IPs, and others. You can also configure GeoIP feeds that will block traffic based on country code information.

To configure threat intelligence feeds on the Sky ATP Console, go to Configure/ Threat Intelligence Feeds. As shown in Figure 10.19, enable the important categories to your environment (to see details for each category, click on *Go to feed site*):



Threat Intelligence Feeds

IP Feeds

Select feeds to enable. Optionally, analyze hosts and block those found to be infected.

dshield ip
☑ Enable feed
☐ Allow this feed to determine infected hosts
Go to feed site

blocklist ip
☑ Enable feed
☐ Allow this feed to determine infected hosts
Go to feed site

tor ip
☑ Enable feed
☑ Allow this feed to determine infected hosts
Go to feed site

malwaredomainlist ip
☑ Enable feed
☐ Allow this feed to determine infected hosts
Go to feed site

ransomwaretracker ip
☑ Enable feed
☑ Allow this feed to determine infected hosts
Go to feed site

URL Feeds

Select feeds to enable. Optionally, analyze hosts and block those found to be infected.

ransomwaretracker url
☑ Enable feed
☑ Allow this feed to determine infected hosts
Go to feed site

openphish url
☑ Enable feed
☐ Allow this feed to determine infected hosts
Go to feed site

Figure 10.19 Threat Intelligence Feeds

Configuring Sky ATP Threat Prevention Policy and Attaching It to a Security Policy

Sky ATP Threat Prevention policy is configured at the SRX level. It instructs the firewall on what threat prevention policy it should use. However, Sky ATP Threat Prevention Policy was not available yet on J-Web at the time this book was being written, so let's do it on the CLI.

NOTE Junos Space Security Director allows Sky ATP to be managed on premise, through the Policy Enforcer module.

To configure the Sky ATP Threat Prevention Policy in the CLI, go into configuration mode.

First, you need to create a Sky ATP Threat Prevention Policy, name it, and define the block threshold. The following command does all that (named *dayone*):

```
set services advanced-anti-malware policy dayone verdict-threshold 7
```

Next, you need to associate the threat prevention profile created earlier with the Sky ATP Threat Prevention Policy. Use the following command:

```
set services advanced-anti-malware policy dayone http inspection-profile Dayone
```

It's useful to configure the policy to block any file if its returned verdict is greater than or equal to 7, and then create a log entry. To configure use this set command:

```
set services advanced-anti-malware policy dayone http action block notification log
```

When there is an error condition you can configure the policy to allow files to be downloaded, or block them and create a log entry. Here are the configurations:

```
set services advanced-anti-malware policy dayone fallback-options action permit

set services advanced-anti-malware policy dayone fallback-options notification log
```

Let's configure the system to create a log entry when attempting to download a file from a site listed in the blacklist or whitelist files:

```
set services advanced-anti-malware policy dayone blacklist-notification log

set services advanced-anti-malware policy dayone whitelist-notification log
```

You need to attach the Sky ATP Threat Prevention Policy to a security policy.

First let's modify your Trust Zone to Internet Zone security policy (we're calling it *All_Trust_Internet* in this book). You can easily search for it in operational mode with this show command:

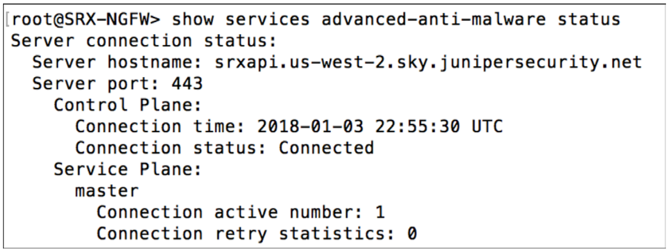
```
show configuration security policies from zone Trust to zone Internet
```

Once you define your security policy, attach the Sky ATP Threat Prevention Policy to it. The command should be like this:

```
set security policies from zone Trust to zone Internet policy All_Trust_Internet then action permit
application-services advanced-anti-malware-policy dayone
```

Commit your configuration. You can check with a show command, with the command results showing in Figure 10.20:

```
show services advanced-anti-malware status
```



```
root@SRX-NGFW> show services advanced-anti-malware status
Server connection status:
  Server hostname: srxapi.us-west-2.sky.junipersecurity.net
  Server port: 443
    Control Plane:
      Connection time: 2018-01-03 22:55:30 UTC
      Connection status: Connected
    Service Plane:
      master
        Connection active number: 1
        Connection retry statistics: 0
```

Figure 10.20 Sky ATP Service Status

Configuring Sky ATP Threat Intelligence Policy and Attaching It to a Security Policy

To create a Threat Intel feed profile and attach it to a security policy, configure the SRX Threat Intel profile. In this configuration example, the profile name is *feed_profile* and threat levels 5 and above are blocked:

```
set services security-intelligence profile feed_profile category CC and set services security-
intelligence profile feed_profile rule 1 match threat-level [5 6 7 8 9 10]
```

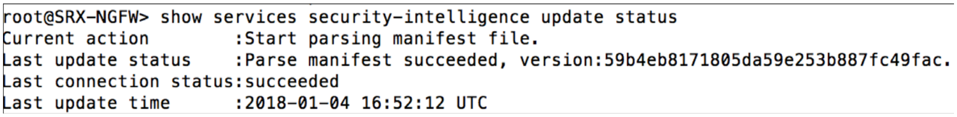
Configure the profile to drop connections above or equal to the threshold level and log them:

```
set services security-intelligence profile feed_profile rule 1 then action block drop and set services
security-intelligence profile feed_profile rule 1 then log
```

Configure the default rule to permit traffic:

```
set services security-intelligence profile feed_profile default-rule then action permit
```

Verify your profile using the `show services security-intelligence` command. Your output should look similar to Figure 10.21:



```
root@SRX-NGFW> show services security-intelligence update status
Current action        :Start parsing manifest file.
Last update status    :Parse manifest succeeded, version:59b4eb8171805da59e253b887fc49fac.
Last connection status:succeeded
Last update time      :2018-01-04 16:52:12 UTC
```

Figure 10.21 Threat Feed Service Status

You also need to create a profile for infected computers so the SRX can quarantine them when instructed to do so by Sky ATP. Configure the SRX Infected Hosts profile. In this example, the profile name is *ih_profile* and threat levels 5 and above are blocked:

```
set services security-intelligence profile ih-profile category Infected-Hosts and
set services security-intelligence profile ih-profile rule 1 match threat-level [5 6 7 8 9 10]
```

Configure the profile to drop connections above or equal to the threshold level and log them:

```
set services security-intelligence profile ih-profile rule 1 then action block drop and set services
security-intelligence profile ih-profile rule 1 then log
```

Next, configure your threat intel policy to point to the profile created above. In this example, the policy name is *dayone:*

```
set services security-intelligence policy dayone CC feed_profile and set services security-intelligence
policy dayone Infected-Hosts ih-profile
```

Configure the security policy to include the Security-Intelligence *dayone* policy. Use the same Trust to Internet policy:

```
set security policies from-zone Trust to-zone Internet policy All_Trust_Internet then permit
application-services security-intelligence-policy dayone
```

Commit the changes.

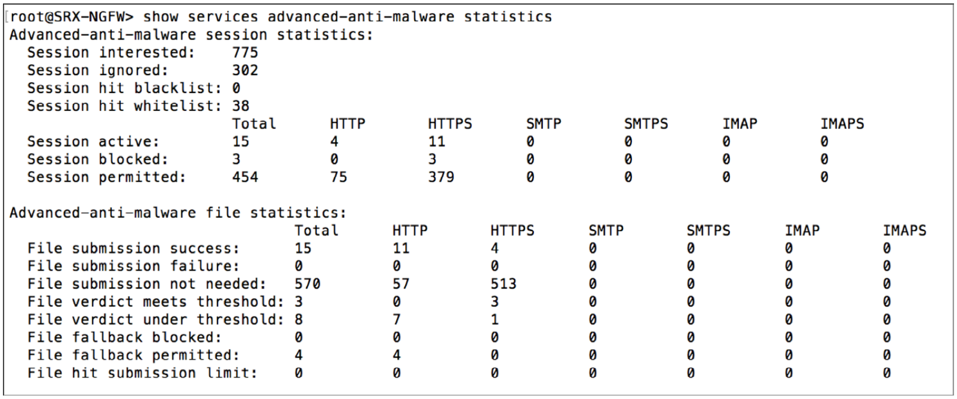
Monitoring Sky ATP and Responding to Threats

As mentioned, Sky ATP monitors and inspects email attachments and downloads to detect and block zero day threats and it also dynamically blocks communication with malware distribution and command-and-control servers, among other threats.

Once Sky ATP is active, administrators will have visibility into threats they could not see before, and this will eventually lead to the task of responding to those threats.

Let's examine and tweak how Sky ATP allows administrators to monitor these threats and respond to them.

First, you can always check for statistics in the CLI. In operational mode, use the `show services advanced-anti-malware statistics` command shown in Figure 10.22:



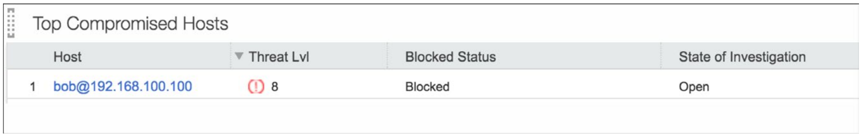
```
[root@SRX-NGFW> show services advanced-anti-malware statistics
Advanced-anti-malware session statistics:
  Session interested:    775
  Session ignored:       302
  Session hit blacklist: 0
  Session hit whitelist: 38
                         Total      HTTP       HTTPS      SMTP       SMTPS      IMAP       IMAPS
  Session active:        15         4          11         0          0          0          0
  Session blocked:       3          0          3          0          0          0          0
  Session permitted:     454        75         379        0          0          0          0

Advanced-anti-malware file statistics:
                                Total      HTTP       HTTPS      SMTP       SMTPS      IMAP       IMAPS
  File submission success:      15         11         4          0          0          0          0
  File submission failure:      0          0          0          0          0          0          0
  File submission not needed:   570        57         513        0          0          0          0
  File verdict meets threshold: 3          0          3          0          0          0          0
  File verdict under threshold: 8          7          1          0          0          0          0
  File fallback blocked:        0          0          0          0          0          0          0
  File fallback permitted:      4          4          0          0          0          0          0
  File hit submission limit:    0          0          0          0          0          0          0
```

Figure 10.22 Sky ATP Statistics

As you can see, Sky ATP is doing its job, looking for malwares in sessions. You can also see that some files already meet threshold and were blocked. Let's drill down on what happened.

Okay, let's log in to the Sky ATP GUI. In the Dashboard, right on the Top Compromised Hosts widget, you can see that the user *bob* on the device with IP address 192.168.100.100 (the Trusted network), hit a malware with a Threat Level of 8. The machine was quarantined due to its triggering of the Global Threat level:



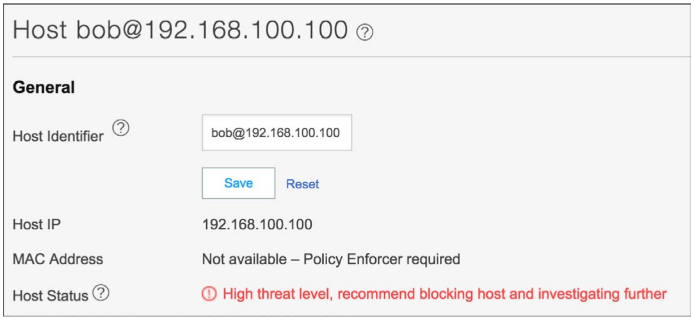
Top Compromised Hosts

	Host	▼ Threat Lvl	Blocked Status	State of Investigation
1	bob@192.168.100.100	ⓘ 8	Blocked	Open

Figure 10.23 *Infected Hosts Widget*

Because of that, the device is quarantined and there's an urgent need to investigate this further. Click on the Host link *bob@192.168.100.100*.

You are taken to the Hosts page, and you can see right away that there's a high threat level associated with this host, and the Investigate Status is open. You can also see that the actual policy recommended a blocking of the host:



Host bob@192.168.100.100 ?

General

Host Identifier ? bob@192.168.100.100

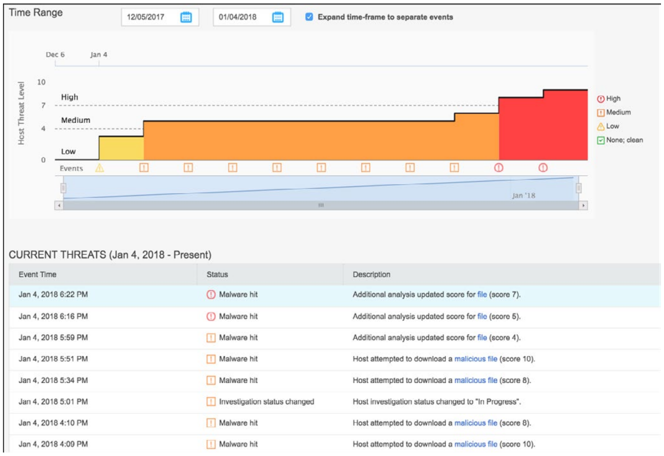
Host IP 192.168.100.100

MAC Address Not available – Policy Enforcer required

Host Status ? ⓘ High threat level, recommend blocking host and investigating further

Figure 10.24 *Infected Hosts Widget*

Scrolling down the Hosts page, you can see that this host also tried to download a lot of other malwares recently:



Time Range 12/05/2017 01/04/2018 ☑ Expand time-frame to separate events

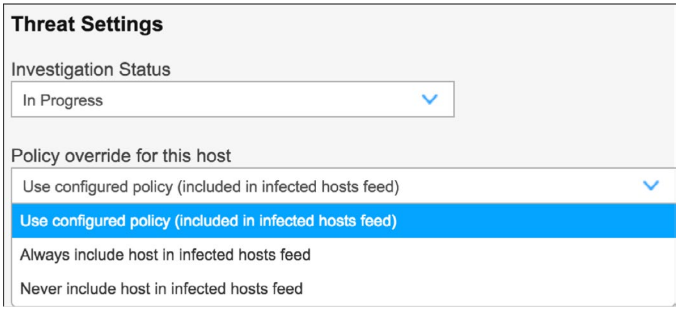
CURRENT THREATS (Jan 4, 2018 - Present)

Event Time	Status	Description
Jan 4, 2018 6:22 PM	Malware hit	Additional analysis updated score for file (score 7).
Jan 4, 2018 6:16 PM	Malware hit	Additional analysis updated score for file (score 5).
Jan 4, 2018 5:59 PM	Malware hit	Additional analysis updated score for file (score 4).
Jan 4, 2018 5:51 PM	Malware hit	Host attempted to download a malicious file (score 10).
Jan 4, 2018 5:34 PM	Malware hit	Host attempted to download a malicious file (score 8).
Jan 4, 2018 5:01 PM	Investigation status changed	Host investigation status changed to "In Progress".
Jan 4, 2018 4:10 PM	Malware hit	Host attempted to download a malicious file (score 8).
Jan 4, 2018 4:09 PM	Malware hit	Host attempted to download a malicious file (score 10).

Figure 10.25 Malware Hits

Before you continue your investigation, it's important to highlight a few things. In Threat Settings, let's change the Investigation Status to In Progress.

NOTE You can decide to override the actual policy by choosing the *Always include host in infected hosts feed; Use configured policy; or Never Include host in infected hosts feed* options. After the investigation is done, you can return it to the original option, if you want.



Threat Settings

Investigation Status: In Progress

Policy override for this host: Use configured policy (included in infected hosts feed)

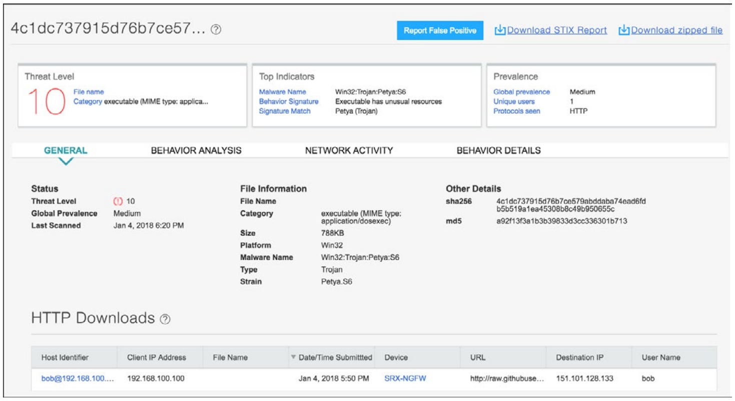
Use configured policy (included in infected hosts feed)
Always include host in infected hosts feed
Never include host in infected hosts feed

Figure 10.26 Policy Override

Now, let's investigate *bob* and his malware download attempts by clicking on the malicious file links shown in Figure 10.26.

You can see in Figure 10.27 the malware name, its category, how many times Sky ATP saw this malware before, unique users that tried to download it, protocol vector used, and number of download attempts among other facts. You can also download the file for your own analysis and report this as a false positive and download the STIX report (in the upper right corner of Figure 10.27).

WARNING Make sure that if you download the file for internal analysis, that it is done in a safe and isolated environment.



4c1dc737915d76b7ce57...

Threat Level
10 File name
Category executable (MIME type: applica...

Top Indicators

Malware Name	Win32:Trojan:Petya:S6
Behavior Signature	Executable has unusual resources
Signature Match	Petya (Trojan)

Prevalence

Global prevalence	Medium
Unique users	1
Protocols seen	HTTP

Status

Threat Level	(!) 10
Global Prevalence	Medium
Last Scanned	Jan 4, 2018 6:20 PM

File Information

File Name	
Category	executable (MIME type: application/dosexec)
Size	788KB
Platform	Win32
Malware Name	Win32:Trojan:Petya:S6
Type	Trojan
Strain	Petya.S6

Other Details

sha256	4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c
md5	a92f13f3a1b3b39833d3cc336301b713

HTTP Downloads

Host Identifier	Client IP Address	File Name	Date/Time Submittted	Device	URL	Destination IP	User Name
bob@192.168.100....	192.168.100.100		Jan 4, 2018 5:50 PM	SRX-NGFW	http://raw.githubuse...	151.101.128.133	bob

Figure 10.27 General Malware Details

Let's check what the machine learning can tell us about this file by clicking on Behavior Analysis. Figure 10.28 displays all the behaviors found during the Sky ATP analysis and how much they affected the verdict value:

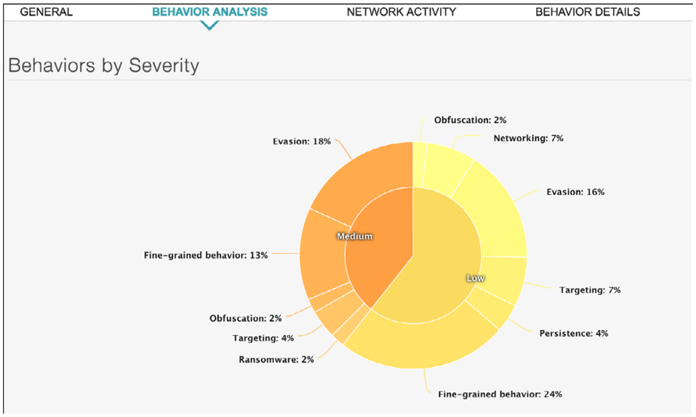
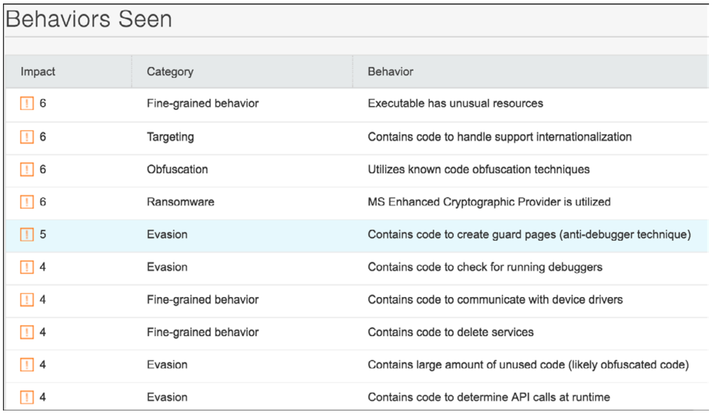


Figure 10.28 Behavior Analysis

You can also see the list of techniques the malware used to avoid detection in Figure 10.29:

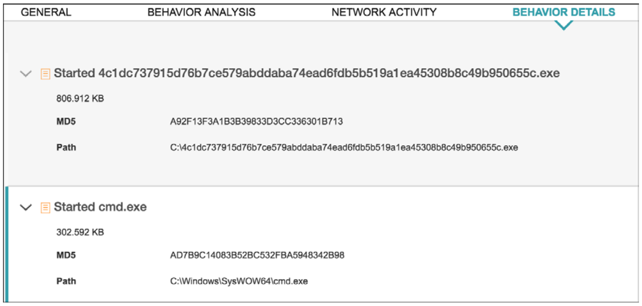


Behaviors Seen

Impact	Category	Behavior
! 6	Fine-grained behavior	Executable has unusual resources
! 6	Targeting	Contains code to handle support internationalization
! 6	Obfuscation	Utilizes known code obfuscation techniques
! 6	Ransomware	MS Enhanced Cryptographic Provider is utilized
! 5	Evasion	Contains code to create guard pages (anti-debugger technique)
! 4	Evasion	Contains code to check for running debuggers
! 4	Fine-grained behavior	Contains code to communicate with device drivers
! 4	Fine-grained behavior	Contains code to delete services
! 4	Evasion	Contains large amount of unused code (likely obfuscated code)
! 4	Evasion	Contains code to determine API calls at runtime

Figure 10.29 *Behavior Analysis (cont.)*

If you click on Behavior Details, in Figure 10.28's Behavior Details tab, the trail of files and registry keys infected will be documented such as those in Figure 10.30:



Started 4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c.exe

806.912 KB

MD5	A92F13F3A1B3B39833D3CC336301B713
Path	C:\4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c.exe

Started cmd.exe

302.592 KB

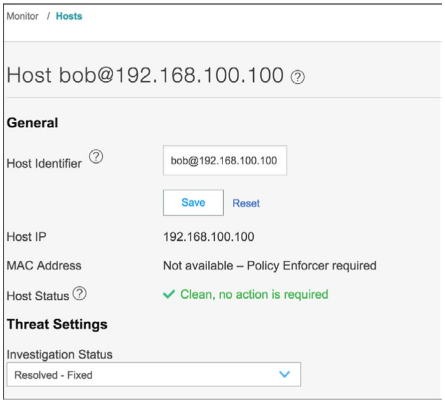
MD5	AD7B9C14083B52BC532FBA5948342B98
Path	C:\Windows\SysWOW64\cmd.exe

Figure 10.30 *Behavior Details*

It is clear that Sky ATP blocked the download of a very dangerous *trojan* with modern evasion detection techniques. The quarantine action seems like a very assertive measure because, at this moment, you don't know what triggered the download (another malware, a botnet, a phishing link, an unaware user trying to download an infected file by mistake, etc.).

In addition, you need to consider the possibility that the computer in question could have been infected while it was out of the corporate network and an onsite analysis seems appropriate.

After the security team solves the incident, the administrator can unblock the quarantined computer in the Sky ATP GUI. Go to Monitor/Hosts and under Investigation Status, at the bottom of Figure 10.31, select *Fixed – Resolved:*


Monitor / Hosts

Host bob@192.168.100.100

General

Host Identifier: bob@192.168.100.100

Host IP: 192.168.100.100

MAC Address: Not available – Policy Enforcer required

Host Status: ✓ Clean, no action is required

Threat Settings

Investigation Status: Resolved - Fixed

Figure 10.31 *Threat Status Change*

Now Bob and his computer can be allowed onto the network again without the risk of infecting the whole infrastructure.

Chapter 11

Virtual Private Networks

A virtual private network (VPN) extends private networks across a public transport network, such as the Internet. Yet it enables users to send and receive data and access applications and resources as if their devices were directly connected to the private network.

Applications and services running across a VPN may therefore benefit from the functionality, security, and management of the private network.

VPNs also extend clouds in a secure way, allowing virtual machines in a private cloud to communicate with counterparts deployed in a public cloud infrastructure, including tasks such as automation and orchestration.

Remote access VPNs also allow remote works to access internal resources easily and securely.

The SRX offers a complete set of VPN functionalities, helping customers to establish static site-to-site VPN tunnels, full mesh dynamic VPN environments, and remote access SSL VPNs, among others.

This chapter helps you set up route-based site-to-site VPNs and Remote Access SSL VPNs.

Understanding Route Based Site-to-Site IPsec VPNs

Let's extend our book's reference topology and include another network (let's call it a branch network) as illustrated in Figure 11.1. This additional private network connects to the Internet using a firewall (in this case, another SRX, but other devices from different vendors can establish IPsec tunnels with the SRX without issues).

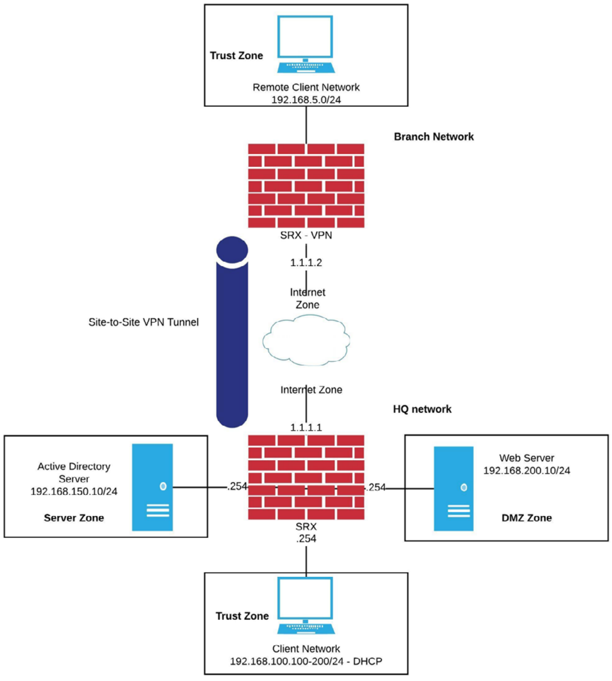


Figure 11.1 Site-to-Site VPN Topology

Initially, both private networks are completely locked down from each other, separated by the Internet (as you know, private networks cannot be routed over a public network).

So, how can you establish communication between branch and HQ, allowing remote users to share files and access resources and services in the HQ? The most common answer is IPsec.

IPsec is a framework of open standards for helping to ensure private, secure communications over IP networks through the use of cryptographic security services. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. Because IPsec is integrated at the Internet layer (Layer 3), it provides security for almost all protocols in the TCP/IP suite, and because IPsec is applied transparently to applications, there is no need to configure separate security for each application that uses TCP/IP.

This makes IPsec one of the most adopted solutions to provide secure communications between networks.

The SRX supports several VPN technologies:

- Policy-based VPN
- Route-based VPN
- Group VPN
- Auto VPN
- Auto Discovery VPN
- Remote Access IPsec VPN
- Remote Access SSL VPN

This offers extreme flexibility to support a large range of environments with basic or complex requirements. The most common VPN deployments are policy- and route-based IPsec VPNs. Let's see what the differences are between these two modes listed in Table 11.1.

Table 11.1 Policy-Based vs Route-Based VPNs

Policy-Based VPNs	Route-Based VPNs
In policy-based VPNs, a tunnel is treated as an object that, together with source, destination, application, and action, constitutes a tunnel policy that permits VPN traffic.	In route-based VPNs, a policy does not specifically reference a VPN tunnel.
A tunnel policy specifically references a VPN tunnel by name.	A route determines which traffic is sent through the tunnel based on a destination IP address.
The number of policy-based VPN tunnels that you can create is limited by the number of tunnels that the device supports.	The number of route-based VPN tunnels that you create is limited by the number of st0 interfaces (for point-to-point VPNs) or the number of tunnels that the device supports, whichever is lower.
With a policy-based VPN, although you can create numerous tunnel policies referencing the same VPN tunnel, each tunnel policy pair creates an individual IPsec SA with the remote peer. Each SA counts as an individual VPN tunnel.	Because the route, not the policy, determines which traffic goes through the tunnel, multiple policies can be supported with a single SA or VPN.
In a policy-based VPN, the action must be permitted and must include a tunnel.	In a route-based VPN, the regulation of traffic is not coupled to the means of its delivery.

The exchange of dynamic routing information is not supported in policy-based VPNs.	Route-based VPNs support the exchange of dynamic routing information through VPN tunnels. You can enable an instance of a dynamic routing protocol, such as OSPF, on an st0 interface that is bound to a VPN tunnel.
If you need more granularity than a route can provide to specify the traffic sent to a tunnel, using a policy-based VPN with security policies is the best choice.	Route-based VPNs use routes to specify the traffic sent to a tunnel; a policy does not specifically reference a VPN tunnel.
With a policy-based VPN tunnel, you can consider a tunnel as an element in the construction of a policy.	When the security device does a route lookup to find the interface through which it must send traffic to reach an address, it finds a route through a secure tunnel (st0) interface. With a route-based VPN tunnel, you can consider a tunnel as a means for delivering traffic, and can consider the policy as a method for either permitting or denying the delivery of that traffic.

Okay, so now let's establish a route-based IPsec VPN between the branch and HQ firewalls to enable both remote private networks to communicate.

Configuring a Route Based Site-to-Site IPsec VPN

Establishing a VPN between peers requires some planning in advance between firewall administrators. Some key points need to be discussed and defined before starting the configuration, such as:

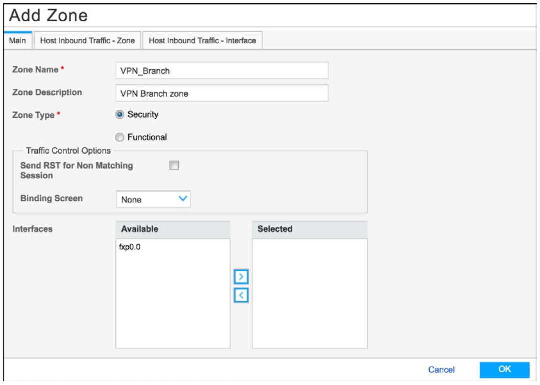
- Security algorithms and keys.
- Protocol mode, either transport or tunnel. SRX devices always use tunnel mode.
- Key-management method, either manual key or AutoKey IKE.
- For inbound traffic, the SRX looks up the SA by using the following:
  - Destination IP address.
  - Security protocol, either AH or ESP
- For outbound VPN traffic, the policy invokes the SA associated with the VPN tunnel and some items need to be defined:
  - Interface tunnel IP address
  - Traffic selectors

Now that all this is sorted out, it's time to start configuring the VPN gateways!

HQ SRX Configuration

On route-based VPNs, traffic is forwarded through the tunnel based on routing decisions, and as such, you need to have an internal tunnel to which you can point the VPN routes. It's also important to attach this interface to a dedicated security zone so you can enforce the proper security policies.

Begin in the J-Web GUI and navigate to Configuration/Security/Objects/Zones/Screens. Then create a new zone called *VPN*_Branch, as shown in Figure 11.2:



Add Zone

Main | Host Inbound Traffic - Zone | Host Inbound Traffic - Interface

Zone Name * VPN_Branch

Zone Description VPN Branch zone

Zone Type * ● Security ○ Functional

Traffic Control Options

Send RST for Non Matching Session □

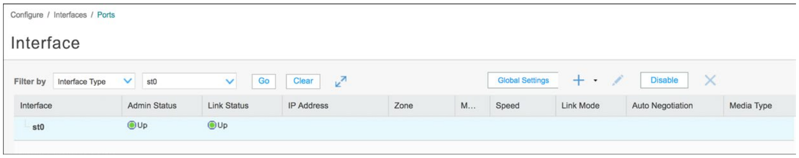
Binding Screen None

Interfaces

Available	Selected
fxp0.0	

Figure 11.2 *Adding a New Security Zone for VPN Branch Traffic*

Navigate to Configuration/Interfaces/Ports and select the st0 interface and then click Go:



Configure / Interfaces / Ports

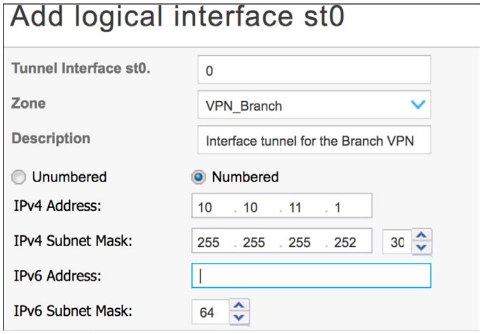
Interface

Filter by Interface Type st0

Interface	Admin Status	Link Status	IP Address	Zone	M...	Speed	Link Mode	Auto Negotiation	Media Type
st0	Up	Up							

Figure 11.3 *Adding a New st0 Logical Interface*

Click on the + sign and select *Logical Interface*. The Add logical interface settings appear, as shown in Figure 11.4. Configure it, changing the field values to reflect your own environment:



Add logical interface st0

Tunnel Interface st0. 0

Zone VPN_Branch

Description Interface tunnel for the Branch VPN

○ Unumbered ● Numbered

IPv4 Address: 10 . 10 . 11 . 1

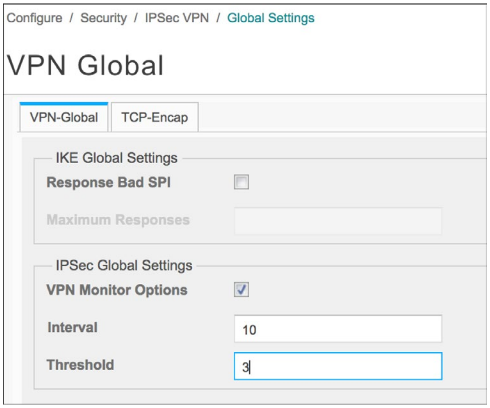
IPv4 Subnet Mask: 255 . 255 . 255 . 252 30

IPv6 Address:

IPv6 Subnet Mask: 64

Figure 11.4 Logical Interface Configuration

After completing the logical interface settings, navigate to Configuration/Security/IPsec VPN. In the Global Settings section, enable the VPN Monitor Options. Use the values listed in Figure 11.5 as a reference for your own environment:



Configure / Security / IPSec VPN / Global Settings

VPN Global

IKE Global Settings

Response Bad SPI □

Maximum Responses

IPSec Global Settings

VPN Monitor Options ☑

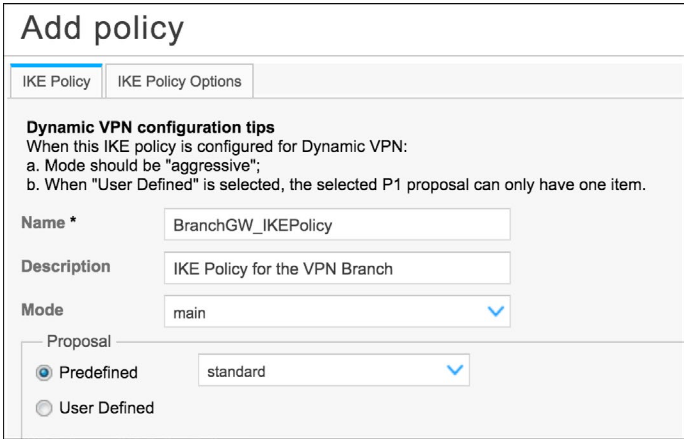
Interval 10

Threshold 3

Figure 11.5 VPN Global Settings

Save your settings, and now let's start configuring the IKE (Phase 1) options. Navigate to IPsec/IKE (Phase 1), and add a new policy.

As shown in Figure 11.6, name the policy, here, *BranchGW_IKEPolicy*, and define the VPN Mode as *main*. In the Proposal fields, let's use *Predefined* and *standard*:



Add policy

Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN:
a. Mode should be "aggressive";
b. When "User Defined" is selected, the selected P1 proposal can only have one item.

Name * BranchGW_IKEPolicy

Description IKE Policy for the VPN Branch

Mode main

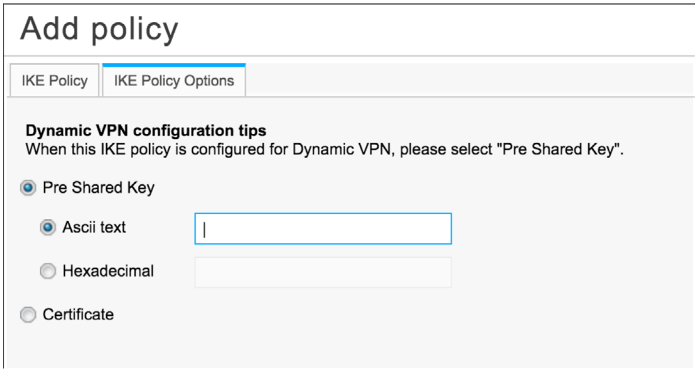
Proposal

● Predefined standard

○ User Defined

Figure 11.6 *IKE Policy Basic Settings*

On the IKE Policy Options tab in Figure 11.7, let's use a Pre Shared Key (certificates are also supported). Type your Pre Shared Key and click OK:



Add policy

Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN, please select "Pre Shared Key".

● Pre Shared Key

● Ascii text |

○ Hexadecimal

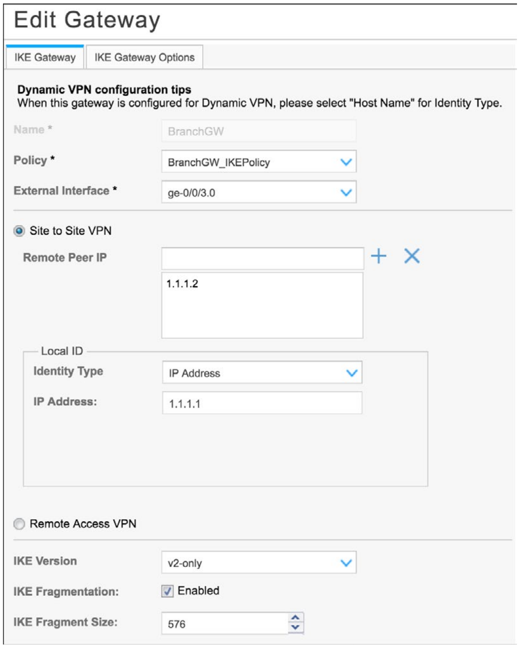
○ Certificate

Figure 11.7 *IKE Policy Options*

Let's configure the IKE gateway. Navigate to IPsec/IKE to edit the gateway.

In Figure 11.8, select the IKE Gateway tab, and fill in the fields. Name it as *BranchGW* and use the policy you just created in the last step. For the external interface, select the interface that is reachable for the remote VPN gateway (in our case, it's the Internet-connected interface, ge-0/0/3.0).

We need to set up the remote and local ID peers. Use the Remote Peer IP (1.1.1.2) and for the Local ID, let's use the IP Address as the identity type and the interface address (1.1.1.1). Select IKE version v2 as the IKE version and enable IKE Fragmentation:


Edit Gateway

IKE Gateway | IKE Gateway Options

Dynamic VPN configuration tips
When this gateway is configured for Dynamic VPN, please select "Host Name" for Identity Type.

Name *: BranchGW
Policy *: BranchGW_IKEPolicy
External Interface *: ge-0/0/3.0

● Site to Site VPN

Remote Peer IP: 1.1.1.2

Local ID
Identity Type: IP Address
IP Address: 1.1.1.1

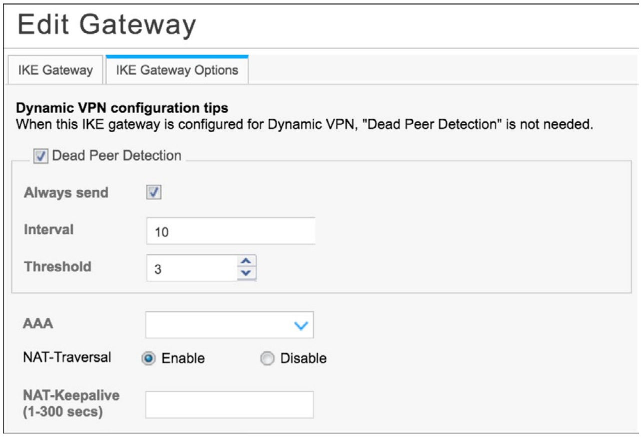
○ Remote Access VPN

IKE Version: v2-only
IKE Fragmentation: ☑ Enabled
IKE Fragment Size: 576

Figure 11.8 IKE Gateway Basic Settings

NOTE Compared with IKEv1, IKEv2 simplifies the security association (SA) negotiation process. IKEv2 uses two exchanges (a total of four messages) to create an IKE SA and a pair of IPsec SAs. To create multiple pairs of IPsec SAs, only one additional exchange is needed for each additional pair of SAs, but before selecting IKEv2, check to see if the remote VPN gateway supports it.

On the IKE Gateway Options tab, enable Dead Peer Detection. Use the values in Figure 11.9 as a reference for your own lab or environment:



Edit Gateway

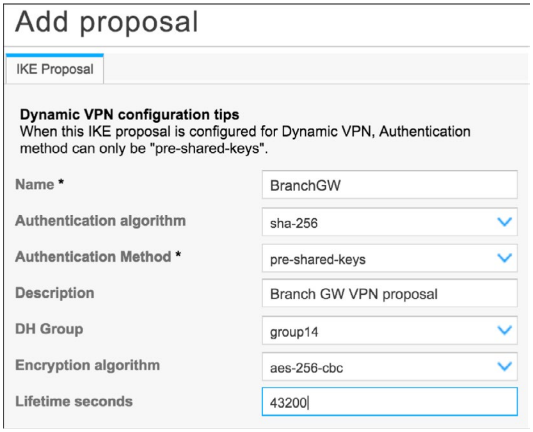
Dynamic VPN configuration tips
When this IKE gateway is configured for Dynamic VPN, "Dead Peer Detection" is not needed.

☑ Dead Peer Detection

Always send	☑
Interval	10
Threshold	3
AAA	
NAT-Traversal	● Enable ○ Disable
NAT-Keepalive (1-300 secs)	

Figure 11.9 IKE Gateway Options

Click OK and click on IKE Proposal. Name the proposal *BranchGW*, select the Authentication Algorithm as *sha-256*, Authentication Method as *pre-shared-keys, and* add a description for the IKE proposal. For the Diffie Helman Group, select *group14*. Select *aes-256-cbc* as the Encryption algorithm and for lifetime seconds, use *43200:*



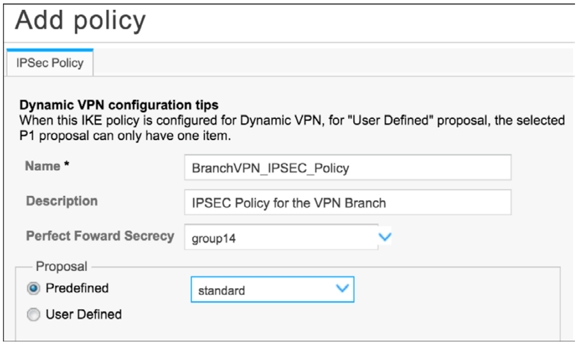
Add proposal

Dynamic VPN configuration tips
When this IKE proposal is configured for Dynamic VPN, Authentication method can only be "pre-shared-keys".

Name *	BranchGW
Authentication algorithm	sha-256
Authentication Method *	pre-shared-keys
Description	Branch GW VPN proposal
DH Group	group14
Encryption algorithm	aes-256-cbc
Lifetime seconds	43200

Figure 11.10 IKE Proposal

Click OK and go to IPsec (Phase 2). Select IPsec Policy. Name the new policy as *BranchVPN_IPsec_Policy*, add a Description, and select *group14* for the Perfect Forward Secrecy (PFS). For a proposal, let's use the pre-defined *standard:*



Add policy

IPSec Policy

Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN, for "User Defined" proposal, the selected P1 proposal can only have one item.

Name * BranchVPN_IPSEC_Policy

Description IPSEC Policy for the VPN Branch

Perfect Foward Secrecy group14

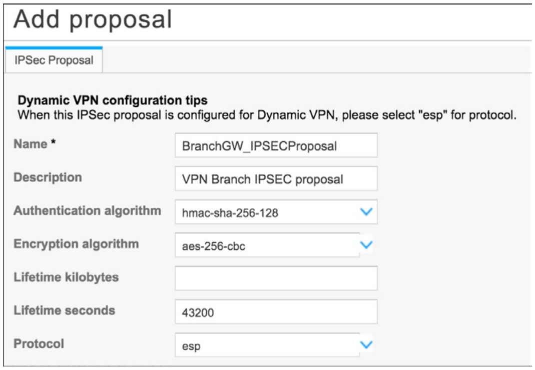
Proposal

● Predefined standard

○ User Defined

Figure 11.11 *IPsec Policy*

Click OK. Now let's create the IPsec (Phase 2) proposal. Add the IPsec (Phase 2) proposal, name it *BranchGW_IPsecProposal*, add a description for authentication algorithm, select *hmac-sha-256-128*, for the encryption algorithm, use aes-256-cbc. Lifetime, use *43200* and protocol, select *esp*:



Add proposal

IPSec Proposal

Dynamic VPN configuration tips
When this IPSec proposal is configured for Dynamic VPN, please select "esp" for protocol.

Name * BranchGW_IPSECProposal

Description VPN Branch IPSEC proposal

Authentication algorithm hmac-sha-256-128

Encryption algorithm aes-256-cbc

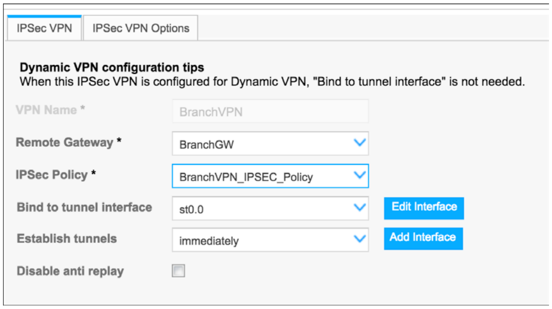
Lifetime kilobytes

Lifetime seconds 43200

Protocol esp

Figure 11.12 *IPsec (Phase 2) Proposal*

Click OK. Select the VPN tab. Define the Remote Gateway as *BranchGW* (defined in the IKE Gateway step). Use the IPsec Policy defined earlier. Select the tunnel interface you created for this VPN and for Establish Tunnels, select the *immediately* option:



IPSec VPN | IPSec VPN Options

Dynamic VPN configuration tips
When this IPSec VPN is configured for Dynamic VPN, "Bind to tunnel interface" is not needed.

VPN Name *	BranchVPN
Remote Gateway *	BranchGW
IPSec Policy *	BranchVPN_IPSEC_Policy
Bind to tunnel interface	st0.0
Establish tunnels	immediately
Disable anti replay	□

Figure 11.13 IPsec VPN

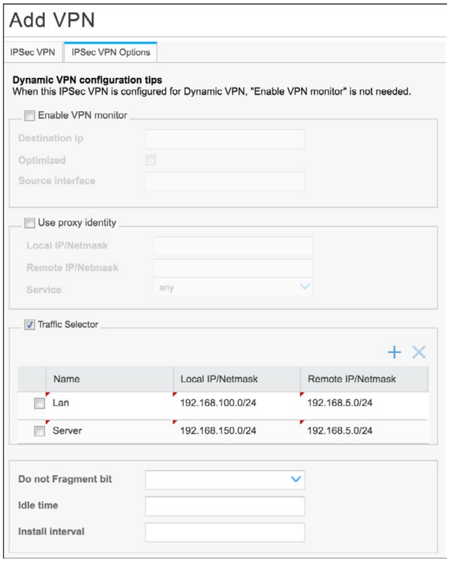
For the IPsec VPN Options tab, shown in Figure 11.13, enable the Traffic Selector option and add a traffic selector for each network pair you want to participate in this VPN. (At the start of this chapter, you and the other administrator discussed and traded connection information.)

In this book's environment, the following traffic selectors are necessary:

LAN: Local Network (192.168.100.0/24) -> Remote Network (192.168.5.0/24)

SERVER: Local Network (192.168.150.0/24) -> Remote Network (192.168.5.0/24)

DMZ: Local Network (192.168.200.0/24) -> Remote Network (192.168.5.0/24)



Add VPN

IPSec VPN | IPSec VPN Options

Dynamic VPN configuration tips
When this IPSec VPN is configured for Dynamic VPN, "Enable VPN monitor" is not needed.

□ Enable VPN monitor

Destination ip	
Optimized	□
Source Interface	

□ Use proxy identity

Local IP/Netmask	
Remote IP/Netmask	
Service	any

☑ Traffic Selector

	Name	Local IP/Netmask	Remote IP/Netmask
□	Lan	192.168.100.0/24	192.168.5.0/24
□	Server	192.168.150.0/24	192.168.5.0/24

Do not Fragment bit	
Idle time	
Install interval	

Figure 11.14 IPsec VPN Options

NOTE A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. With this feature, you can define a traffic selector within a specific route-based VPN, which can result in multiple Phase 2 IPsec SAs. Only traffic that conforms to a traffic selector is permitted through the associated SA. Traffic selectors automatically install routes to the matching SA; this process is known as *auto route insertion* (ARI).

WARNING Do not confuse a traffic selector with a security policy. You still need to configure the proper security policies to allow traffic.

The IPsec VPN configuration is concluded but we still need to add the security policies and enable the IKE service.

As discussed in Chapter 3, interfaces and zones only allow traffic that is specifically allowed in their direction. As a result, you need to go back to Zone settings, select the Internet interface (ge-0/0/3), and enable the IKE service under it.

In the J-Web GUI, navigate to Configuration/Security/Objects/Zones/Screens. Select the Internet Zone and add the IKE service into your Host Inbound Traffic settings as shown in Figure 11.15:

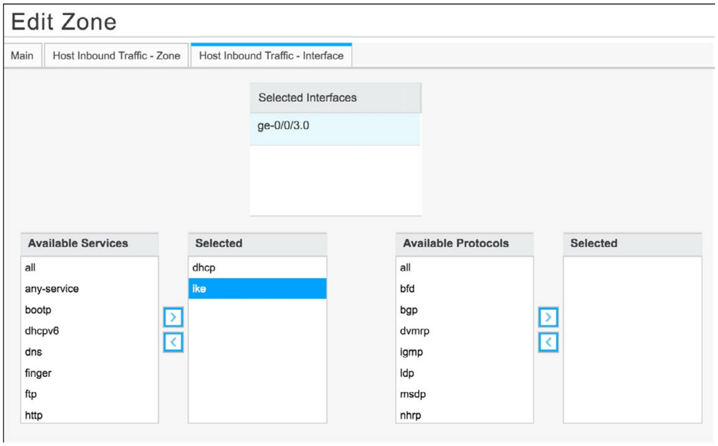


Figure 11.15 Enabling IKE Service in the Internet Zone Interface

Let's add the security policies.

The policies need to be configured according to your lab or environment. As a reference, the following security policies enable the VPN traffic between the Branch and HQ:

- Zone VPN Branch to Zone Trust
  - Source Address -> Remote Branch Network (192.168.5.0/24)
  - Destination Address -> Trust Network (192.168.100.0/24)
  - Services -> *any*
  - Action-> *permit*
- Zone Trust to Zone VPN Branch
  - Source Address -> Trust Network (192.168.100.0/24)
  - Destination Address -> Remote Branch Network (192.168.5.0/24)
  - Services -> *any*
  - Action-> *permit*
- Zone VPN Branch to Zone Server
  - Source Address -> Remote Branch Network (192.168.5.0/24)
  - Destination Address -> Server Network (192.168.150.0/24)
  - Services -> *any*
  - Action-> *permit, log*
- Zone VPN Branch to Zone DMZ
  - Source Address -> Remote Branch Network (192.168.5.0/24)
  - Destination Address -> DMZ Network (192.168.200.0/24)
  - Services -> *http/https*
  - Action-> *permit, log*

To diminish problems, it's important to configure a maximum segment size in order for the VPN traffic to be lower than the interface MTU.

This is a value that will change from network to network, but a good starting point is configuring it to a value of *1350*. This value can accommodate the IPsec header overhead and avoid fragmentation, and by consequence, packet loss and performance problems.

To configure the VPN maximum segment size (MSS), go to the CLI and in configuration mode, issue the following `set security flow tcp-mss IPsec-vpn mss 1350` command.

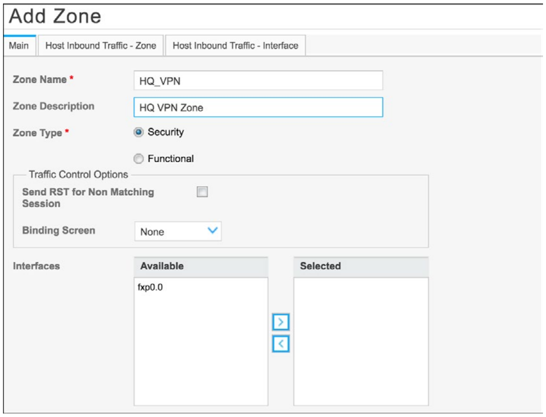
Commit the configuration. And that concludes the HQ VPN gateway configuration.

Normally, the other VPN GW is managed by a different entity or team, but sometimes both gateways are under the same management team. This is our case, so we need to configure the remote branch SRX as well.

The configuration steps are the same, so follow along through the necessary steps, and we'll illustrate them along the way, but won't go into details. You should know exactly what is happening.

Branch SRX Configuration

In the J-Web GUI, add a new security zone to control the VPN traffic coming from HQ:



Add Zone

Main | Host Inbound Traffic - Zone | Host Inbound Traffic - Interface

Zone Name *: HQ_VPN

Zone Description: HQ VPN Zone

Zone Type *: ● Security ○ Functional

Traffic Control Options

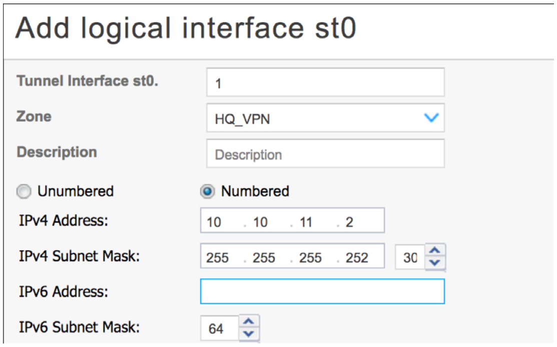
Send RST for Non Matching Session: □

Binding Screen: None

Interfaces: Available: fxp0.0 | Selected:

Figure 11.16 *Configuring the HQ_VPN Zone*

Add an interface tunnel and attach it to the security zone HQ_VPN:



Add logical interface st0

Tunnel Interface st0.: 1

Zone: HQ_VPN

Description: Description

○ Unnumbered ● Numbered

IPv4 Address: 10 . 10 . 11 . 2

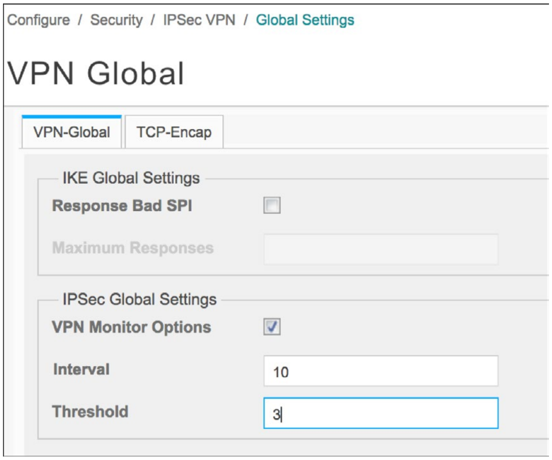
IPv4 Subnet Mask: 255 . 255 . 255 . 252 30

IPv6 Address:

IPv6 Subnet Mask: 64

Figure 11.17 *Adding an Interface Tunnel for HQ VPN*

Define the VPN Global settings:



Configure / Security / IPSec VPN / Global Settings

VPN Global

IKE Global Settings

Response Bad SPI □

Maximum Responses

IPSec Global Settings

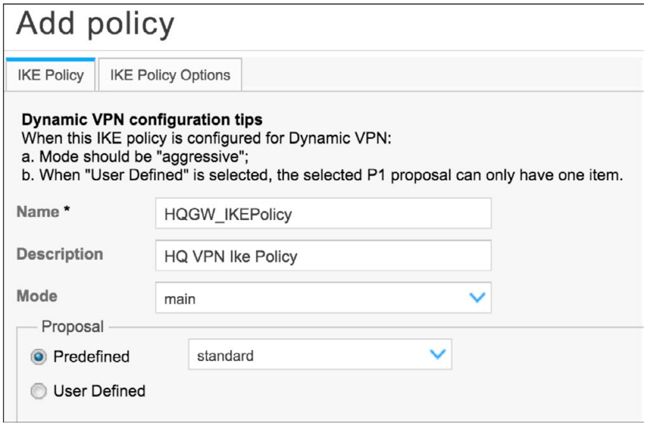
VPN Monitor Options ☑

Interval 10

Threshold 3

Figure 11.18 Configuring VPN Global Settings

Add an IKE policy:



Add policy

Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN:
a. Mode should be "aggressive";
b. When "User Defined" is selected, the selected P1 proposal can only have one item.

Name * HQGW_IKEPolicy

Description HQ VPN Ike Policy

Mode main

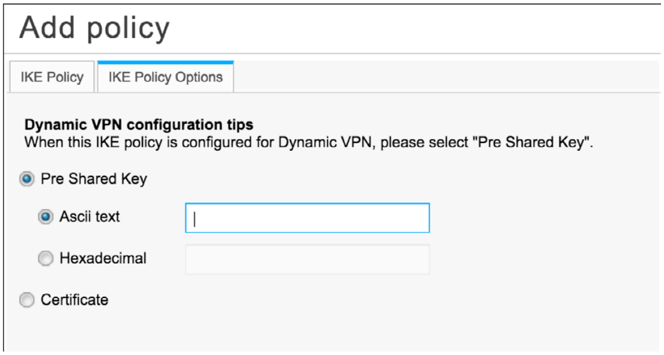
Proposal

● Predefined standard

○ User Defined

Figure 11.19 Adding an IKE Policy

Configure the Pre Shared Key (same as the HQ SRX):



Add policy

IKE Policy | IKE Policy Options

Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN, please select "Pre Shared Key".

● Pre Shared Key

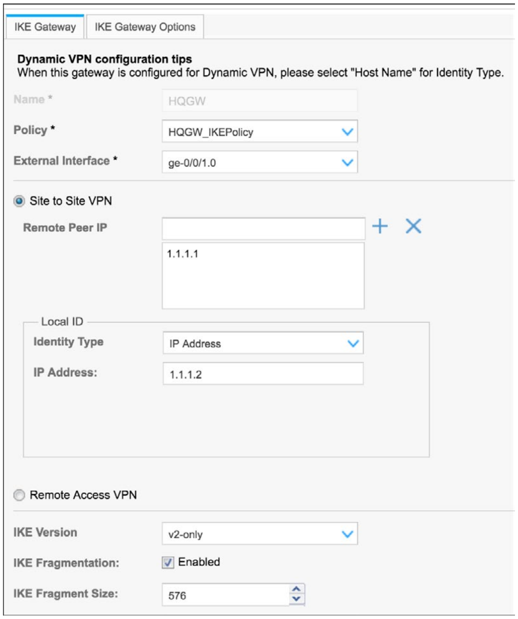
● Ascii text |

○ Hexadecimal

○ Certificate

Figure 11.20 *IKE Policy Options*

Configure the IKE Gateway:



IKE Gateway | IKE Gateway Options

Dynamic VPN configuration tips
When this gateway is configured for Dynamic VPN, please select "Host Name" for Identity Type.

Name * HQGW

Policy * HQGW_IKEPolicy

External Interface * ge-0/0/1.0

● Site to Site VPN

Remote Peer IP + ✕
1.1.1.1

Local ID
Identity Type IP Address
IP Address: 1.1.1.2

○ Remote Access VPN

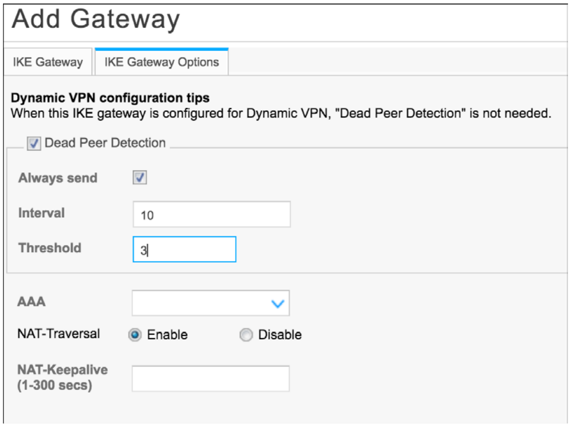
IKE Version v2-only

IKE Fragmentation: ☑ Enabled

IKE Fragment Size: 576

Figure 11.21 *IKE Gateway Settings*

Set up the IKE Gateway Options:



Add Gateway

Dynamic VPN configuration tips
When this IKE gateway is configured for Dynamic VPN, "Dead Peer Detection" is not needed.

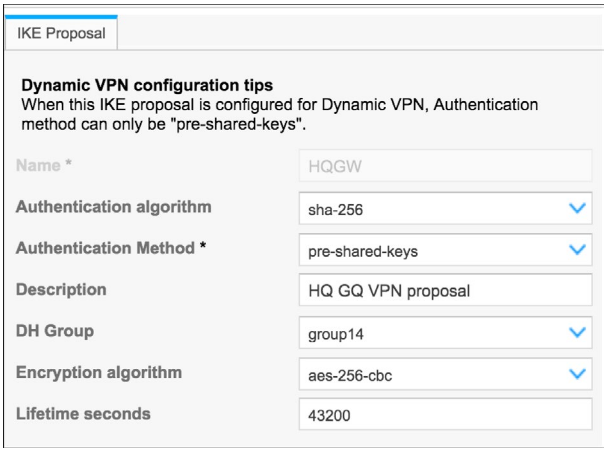
☑ Dead Peer Detection

Always send	☑
Interval	10
Threshold	3

AAA		
NAT-Traversal	● Enable	○ Disable
NAT-Keepalive (1-300 secs)		

Figure 11.22 *IKE Gateway Options*

Define the IKE Proposal:

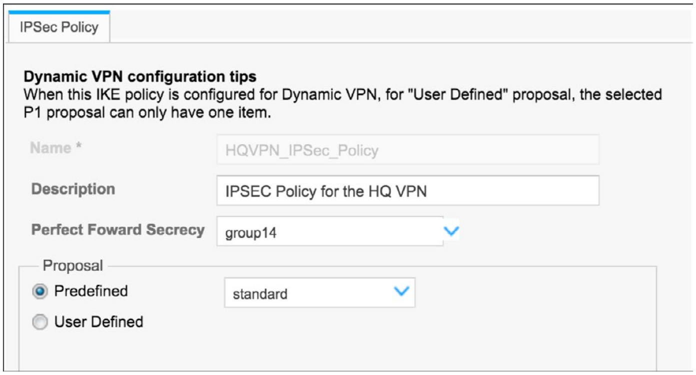


Dynamic VPN configuration tips
When this IKE proposal is configured for Dynamic VPN, Authentication method can only be "pre-shared-keys".

Name *	HQGW
Authentication algorithm	sha-256
Authentication Method *	pre-shared-keys
Description	HQ GQ VPN proposal
DH Group	group14
Encryption algorithm	aes-256-cbc
Lifetime seconds	43200

Figure 11.23 *IKE Proposal*

Configure the IPsec Policy:



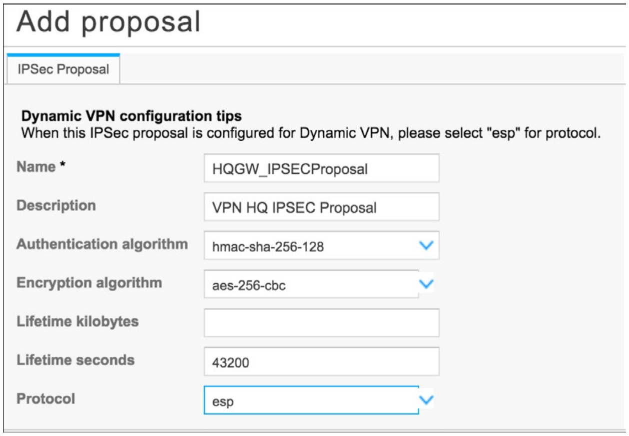
Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN, for "User Defined" proposal, the selected P1 proposal can only have one item.

Name *	HQVPN_IPSec_Policy
Description	IPSEC Policy for the HQ VPN
Perfect Foward Secrecy	group14

Proposal
- ● Predefined: standard
- ○ User Defined

Figure 11.24 IPsec Policy

Configure the IPsec Proposal:

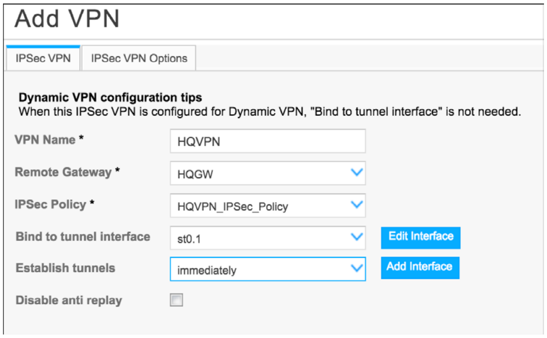


Dynamic VPN configuration tips
When this IPSec proposal is configured for Dynamic VPN, please select "esp" for protocol.

Name *	HQGW_IPSECProposal
Description	VPN HQ IPSEC Proposal
Authentication algorithm	hmac-sha-256-128
Encryption algorithm	aes-256-cbc
Lifetime kilobytes	
Lifetime seconds	43200
Protocol	esp

Figure 11.25 IPsec Proposal

Configure the IPsec VPN:



Add VPN

IPSec VPN | IPSec VPN Options

Dynamic VPN configuration tips
When this IPSec VPN is configured for Dynamic VPN, "Bind to tunnel interface" is not needed.

VPN Name *	HQVPN
Remote Gateway *	HQGW
IPSec Policy *	HQVPN_IPSec_Policy
Bind to tunnel interface	st0.1
Establish tunnels	immediately
Disable anti replay	□

Figure 11.26 IPsec VPN Settings

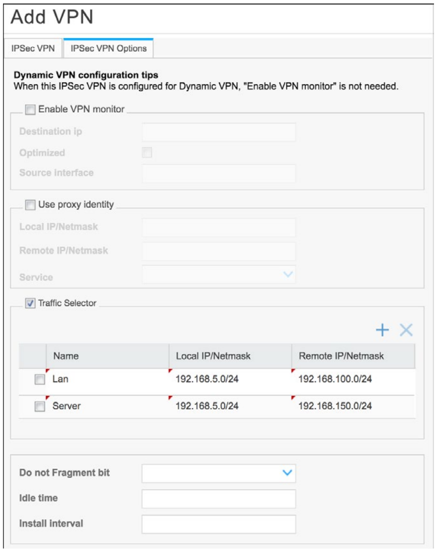
Configure the IPsec VPN Options. Enable the Traffic Selector option and add a traffic selector for each network pair you want to participate in this VPN.

In this book’s environment, the following traffic selectors are necessary:

LAN – Local Network *(192.168.5.0/24)* -> Remote Network *(192.168.100.0/24)*

SERVER - Local Network *(192.168.5.0/24)* -> Remote Network *(192.168.150.0/24)*

DMZ - Local Network *(192.168.5.0/24)* -> Remote Network *(192.168.200.0/24)*



Add VPN

IPSec VPN | IPSec VPN Options

Dynamic VPN configuration tips
When this IPSec VPN is configured for Dynamic VPN, "Enable VPN monitor" is not needed.

□ Enable VPN monitor
Destination ip
Optimized □
Source Interface

□ Use proxy identity
Local IP/Netmask
Remote IP/Netmask
Service

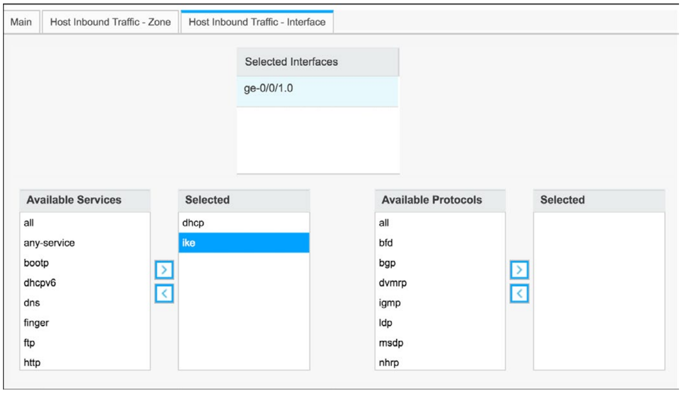
☑ Traffic Selector

	Name	Local IP/Netmask	Remote IP/Netmask
□	Lan	192.168.5.0/24	192.168.100.0/24
□	Server	192.168.5.0/24	192.168.150.0/24

Do not Fragment bit
Idle time
Install Interval

Figure 11.27 IPsec VPN Options

Enable the IKE service in the proper zone or interface (in this case the interface *ge-0/0/1*, that belongs to the *Untrust* zone).



Selected Interfaces
ge-0/0/1.0

Selected
dhcp
ike

Selected

Figure 11.28 *Enabling IKE Service in the Proper Zone/Interface*

Add the security policies. The policies need to be configured according to your environment. As a reference, we added the following security policies to enable the VPN traffic between the HQ and the Branch:

- Zone Trust to Zone VPN HQ
  - Source Address -> Trust Network *(192.168.5.0/24)*
  - Destination Address -> Trust HQ Network *(192.168.100.0/24)*, Server Network *(192.168.150.0/24)*, DMZ Network *(192.168.200.0/24)*
  - Services -> *any*
  - Action-> *permit*
- Zone VPN HQ to Zone Trust
  - Source Address -> Trust HQ Network *(192.168.100.0/24)*
  - Destination Address -> Trust Network (192.168.5.0/24)
  - Services -> any
  - Action-> permit

Go to the CLI and configure the TCP MSS by issuing this command:

```
set security flow tcp-mss IPsec-vpn mss 1350
```

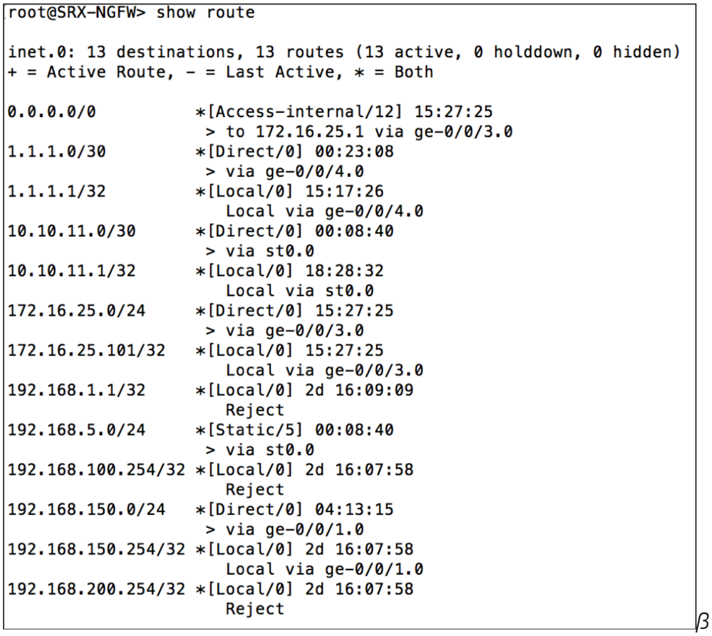
Commit the change. And that concludes the Branch VPN SRX configuration.

Monitoring a Site-to-Site IPsec VPN

The SRX offers both CLI and GUI methods to monitor the state of a VPN. Let's take a look at a few commands.

First, it's always important to check if the traffic selectors are correct. To monitor the routes in the CLI, enter show routes while in operational mode.

As you can see in Figure 11.29, there are routes in the HQ-FW towards the 192.168.5.0/24 network, pointing to the st0.0 interface, meaning that the VPN routing is correct:



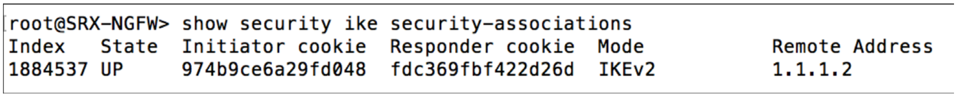
```
root@SRX-NGFW> show route

inet.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Access-internal/12] 15:27:25
                    > to 172.16.25.1 via ge-0/0/3.0
1.1.1.0/30         *[Direct/0] 00:23:08
                    > via ge-0/0/4.0
1.1.1.1/32         *[Local/0] 15:17:26
                      Local via ge-0/0/4.0
10.10.11.0/30      *[Direct/0] 00:08:40
                    > via st0.0
10.10.11.1/32      *[Local/0] 18:28:32
                      Local via st0.0
172.16.25.0/24     *[Direct/0] 15:27:25
                    > via ge-0/0/3.0
172.16.25.101/32   *[Local/0] 15:27:25
                      Local via ge-0/0/3.0
192.168.1.1/32     *[Local/0] 2d 16:09:09
                      Reject
192.168.5.0/24     *[Static/5] 00:08:40
                    > via st0.0
192.168.100.254/32 *[Local/0] 2d 16:07:58
                      Reject
192.168.150.0/24   *[Direct/0] 04:13:15
                    > via ge-0/0/1.0
192.168.150.254/32 *[Local/0] 2d 16:07:58
                      Local via ge-0/0/1.0
192.168.200.254/32 *[Local/0] 2d 16:07:58
                      Reject
```

Figure 11.29 Visualizing the Routing Table

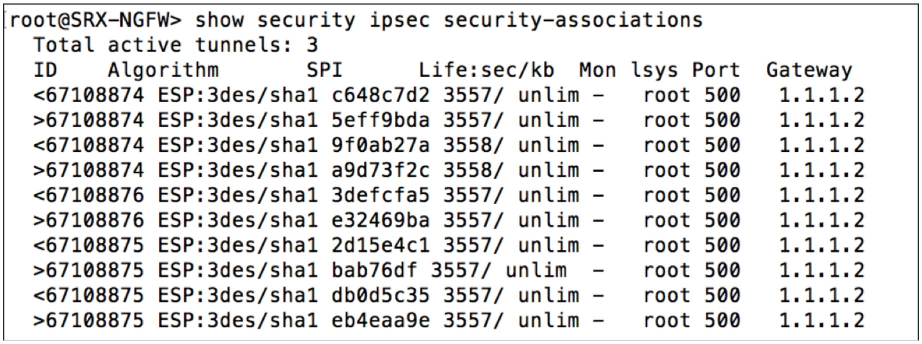
You can also monitor the VPN status. Let's check the status of the Phase 1. On the CLI, in operational mode, enter the show security ike security-associations command. You can see in Figure 11.30 that Phase 1 is UP:



```
root@SRX-NGFW> show security ike security-associations
Index    State  Initiator cookie  Responder cookie  Mode           Remote Address
1884537  UP     974b9ce6a29fd048  fdc369fbf422d26d  IKEv2          1.1.1.2
```

Figure 11.30 Visualizing Phase 1 Status

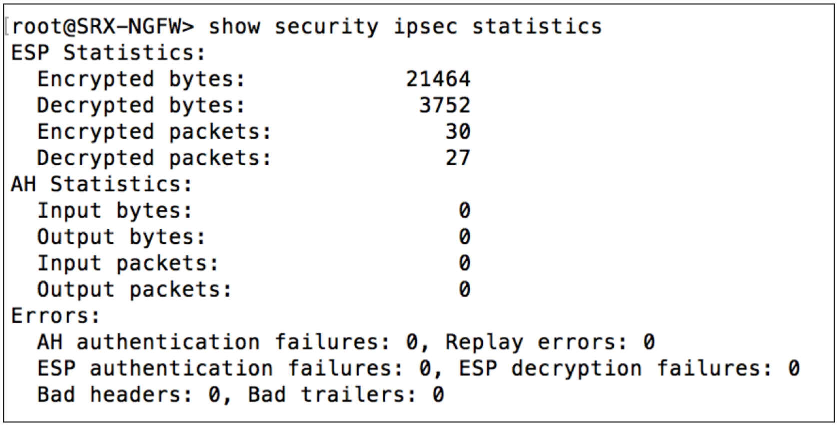
You can also check for IPsec Phase 2 information. On the CLI, in operational mode, enter the `show security ipse security-associations` command. The output in Figure 11.31 shows that there are three active tunnels:



```
root@SRX-NGFW> show security ipsec security-associations
  Total active tunnels: 3
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <67108874 ESP:3des/sha1 c648c7d2 3557/ unlim -   root 500   1.1.1.2
  >67108874 ESP:3des/sha1 5eff9bda 3557/ unlim -   root 500   1.1.1.2
  <67108874 ESP:3des/sha1 9f0ab27a 3558/ unlim -   root 500   1.1.1.2
  >67108874 ESP:3des/sha1 a9d73f2c 3558/ unlim -   root 500   1.1.1.2
  <67108876 ESP:3des/sha1 3defcfa5 3557/ unlim -   root 500   1.1.1.2
  >67108876 ESP:3des/sha1 e32469ba 3557/ unlim -   root 500   1.1.1.2
  <67108875 ESP:3des/sha1 2d15e4c1 3557/ unlim -   root 500   1.1.1.2
  >67108875 ESP:3des/sha1 bab76df 3557/ unlim  -   root 500   1.1.1.2
  <67108875 ESP:3des/sha1 db0d5c35 3557/ unlim -   root 500   1.1.1.2
  >67108875 ESP:3des/sha1 eb4eaa9e 3557/ unlim -   root 500   1.1.1.2
```

Figure 11.31 *Visualizing Phase 2 Status*

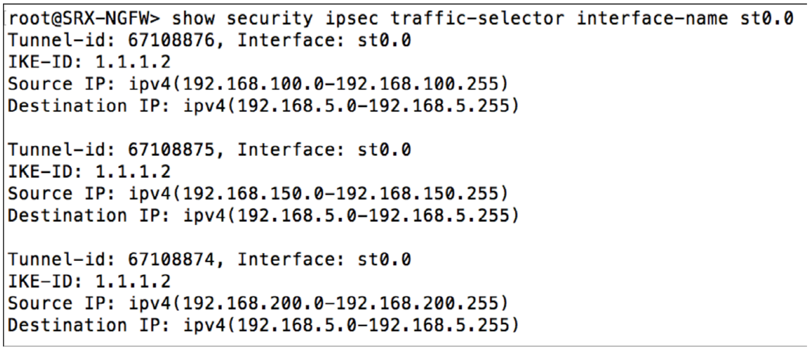
Let's take a look at the IPsec statistics. On the CLI, in operational mode, enter the `show security IPsec statistics` command. Notice that in Figure 11.32 there are no errors or failures, and that the encrypted/decrypted counters show that there is traffic in both directions:



```
root@SRX-NGFW> show security ipsec statistics
ESP Statistics:
  Encrypted bytes:            21464
  Decrypted bytes:             3752
  Encrypted packets:             30
  Decrypted packets:             27
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

Figure 11.32 *Visualizing IPsec Statistics*

You can also check the traffic selectors available for a specific interface tunnel. On the CLI, in operational mode, enter the `show security IPsec traffic-selector interface name st0.0` command. Notice that in Figure 11.33 there are three traffic selectors configured and each one is pointing to a specific tunnel:



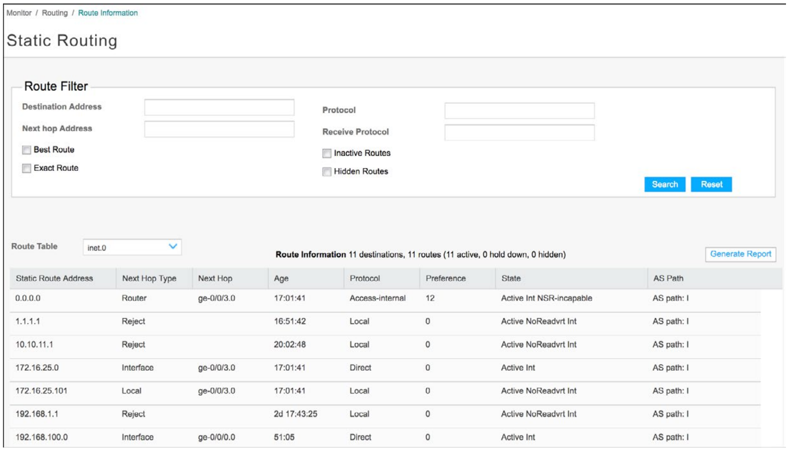
```
root@SRX-NGFW> show security ipsec traffic-selector interface-name st0.0
Tunnel-id: 67108876, Interface: st0.0
IKE-ID: 1.1.1.2
Source IP: ipv4(192.168.100.0-192.168.100.255)
Destination IP: ipv4(192.168.5.0-192.168.5.255)

Tunnel-id: 67108875, Interface: st0.0
IKE-ID: 1.1.1.2
Source IP: ipv4(192.168.150.0-192.168.150.255)
Destination IP: ipv4(192.168.5.0-192.168.5.255)

Tunnel-id: 67108874, Interface: st0.0
IKE-ID: 1.1.1.2
Source IP: ipv4(192.168.200.0-192.168.200.255)
Destination IP: ipv4(192.168.5.0-192.168.5.255)
```

Figure 11.33 Traffic Selector information

You can also obtain most of this information in the GUI, as displayed in the next four figures, Figures 11.34 – 11.37:

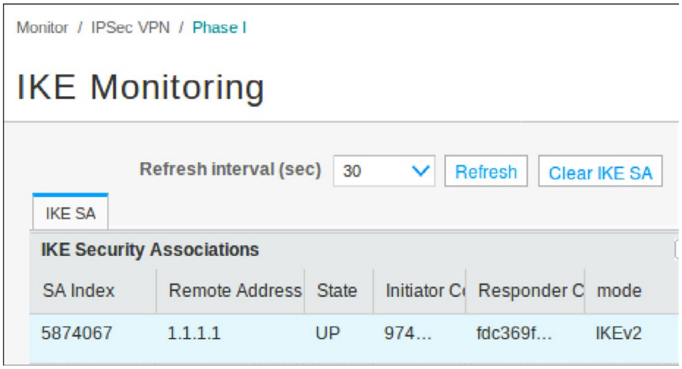


Route Information 11 destinations, 11 routes (11 active, 0 hold down, 0 hidden)

Static Route Address	Next Hop Type	Next Hop	Age	Protocol	Preference	State	AS Path
0.0.0.0	Router	ge-0/0/3.0	17:01:41	Access-internal	12	Active Int NSR-incapable	AS path: I
1.1.1.1	Reject		16:51:42	Local	0	Active NoReadvrt Int	AS path: I
10.10.11.1	Reject		20:02:48	Local	0	Active NoReadvrt Int	AS path: I
172.16.25.0	Interface	ge-0/0/3.0	17:01:41	Direct	0	Active Int	AS path: I
172.16.25.101	Local	ge-0/0/3.0	17:01:41	Local	0	Active NoReadvrt Int	AS path: I
192.168.1.1	Reject		2d 17:43:25	Local	0	Active NoReadvrt Int	AS path: I
192.168.100.0	Interface	ge-0/0/0.0	51:05	Direct	0	Active Int	AS path: I

Figure 11.34 Routing Information

You can monitor the status of both Phase 1 and 2 in Monitor/IPsec VPN as shown in Figures 11.35, 11.36, and 11.37:



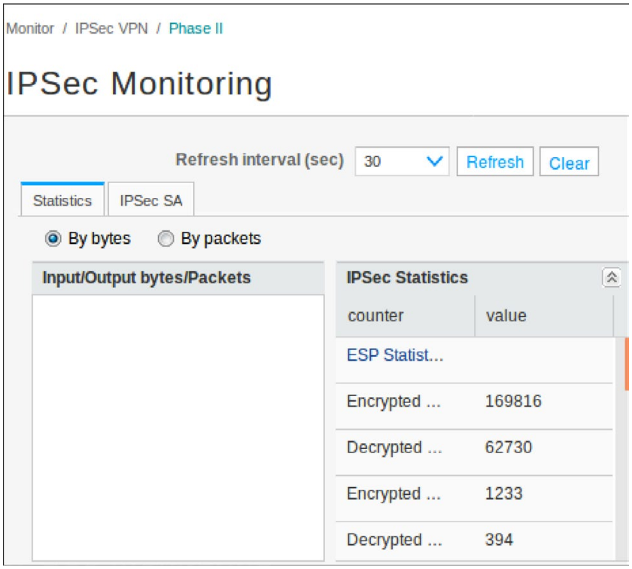
IKE Monitoring

Refresh interval (sec) 30

IKE Security Associations

SA Index	Remote Address	State	Initiator C	Responder C	mode
5874067	1.1.1.1	UP	974...	fdc369f...	IKEv2

Figure 11.35 *IKE Monitoring*



IPSec Monitoring

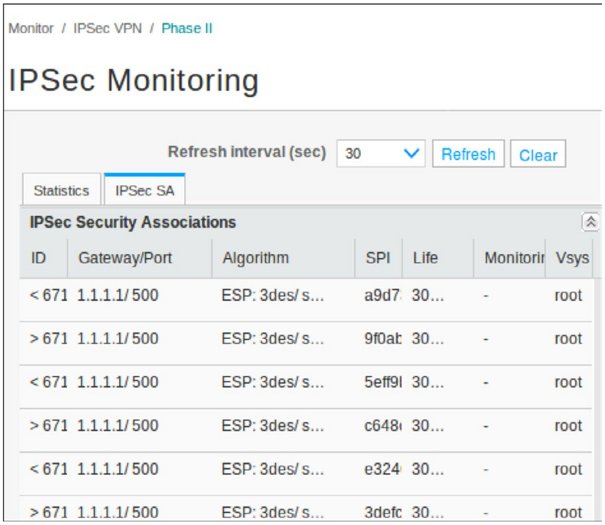
Refresh interval (sec) 30

● By bytes ○ By packets

IPSec Statistics

counter	value
ESP Statist...	
Encrypted ...	169816
Decrypted ...	62730
Encrypted ...	1233
Decrypted ...	394

Figure 11.36 *IPsec Monitoring*



IPSec Monitoring

IPSec Security Associations

ID	Gateway/Port	Algorithm	SPI	Life	Monitorir	Vsys
< 671	1.1.1.1/ 500	ESP: 3des/ s...	a9d7	30...	-	root
> 671	1.1.1.1/ 500	ESP: 3des/ s...	9f0ab	30...	-	root
< 671	1.1.1.1/ 500	ESP: 3des/ s...	5eff9l	30...	-	root
> 671	1.1.1.1/ 500	ESP: 3des/ s...	c648	30...	-	root
< 671	1.1.1.1/ 500	ESP: 3des/ s...	e324	30...	-	root
> 671	1.1.1.1/ 500	ESP: 3des/ s...	3defc	30...	-	root

Figure 11.37 IPsec Tunnel Monitoring

MORE? Junos Space Security Director offers an enterprise level VPN monitoring solution that helps teams to visualize and identity VPN performance and issues. See https://www.juniper.net/us/en/products-services/security/security-director/.

Understanding SSL Remote Access VPN

In many public hotspot environments, IPsec traffic is blocked while TCP connections over port 443 are normally allowed.

For these environments, the SRX Series can support IPsec messages encapsulated within a TCP connection. This implementation is compatible with the third-party, Juniper NCP Exclusive Remote Access Client.

Users running NCP Exclusive Remote Access Client software can establish SSL connections with SRX Series to exchange encapsulated IPsec traffic.

The patented NCP VPN Path Finder technology is a new remote access technology that removes a major constraint in communication within IPsec VPNs by allowing data connections from unknown networks, whose firewall settings deny IPsec communication, and only allowing Internet access to web browsers.

The NCP's Secure Client automatically recognizes when the VPN gateway is not available via IPsec. When this is the case, the client software automatically switches to a modified mode (emulates HTTPS) and sets up an end-to-site tunnel to the main network.

With this technology, highly secure VPN connections based on IPsec are possible even in hotel and public hotspot networks with restricted security access settings or in certain mobile communication networks.

The advantage of this solution over traditional SSL-based VPNs is that the administrator maintains the corporate security policy based on IPsec.

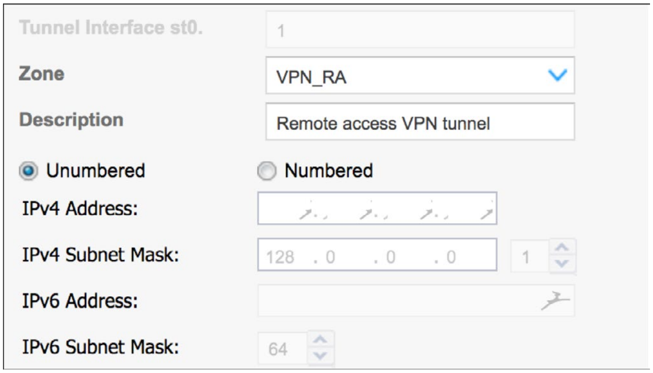
MORE? NCP Exclusive Remote Access Client software is available for download at https://www.ncp-e.com/ncp-exclusive-remote-access-client and in selected App Stores.

Configuring SSL Remote Access VPN for Local Authentication

As you should now know, the SRX Series supports several authentication mechanisms, such as local database, remote authentication, and certificate-based authentication. In this next tutorial, let's configure the Remote Access clients to authenticate themselves against the SRX local database.

SRX Configuration

In the J-Web GUI, configure a new security zone. Let's name it *VPN_RA*. Now create a new logical tunnel interface, st0.1, as in Figure 11.38:



Tunnel Interface st0. 1

Zone VPN_RA

Description Remote access VPN tunnel

● Unumbered ○ Numbered

IPv4 Address:

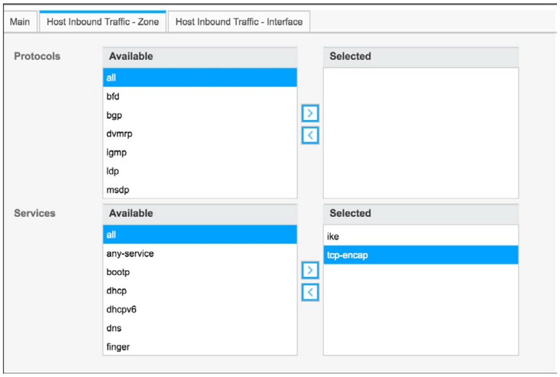
IPv4 Subnet Mask: 128 . 0 . 0 . 0 1

IPv6 Address:

IPv6 Subnet Mask: 64

Figure 11.38 *Adding a Second Logical Tunnel Interface*

In the Internet Zone or interface (where your clients will connect), open at least both IKE and TCP-ENCAP services, (you may need other services and protocols in your environment) as in Figure 11.39:



Protocols

Available: all, bfd, bgp, dvmrp, igmp, ldp, msdp

Selected:

Services

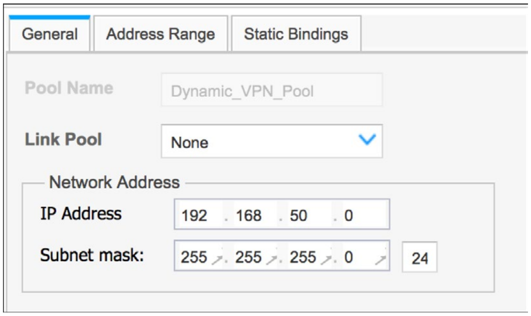
Available: all, any-service, bootp, dhcp, dhcpv6, dns, finger

Selected: ike, tcp-encap

Figure 11.39 Enabling TCP-ENCAP Service in the Internet Zone

WARNING You cannot add both HTTPS web-management and TCP-ENCAP services in the same interface or zone. In case you absolutely need to have both enabled over the same interface, change the HTTPS management port to another value.

Navigate to Configure/Network/DHCP Server and add another Address Pool for the Dynamic VPN clients. Figure 11.40 is using 192.168.50.0/24 as a network range:



Pool Name: Dynamic_VPN_Pool

Link Pool: None

IP Address: 192 . 168 . 50 . 0

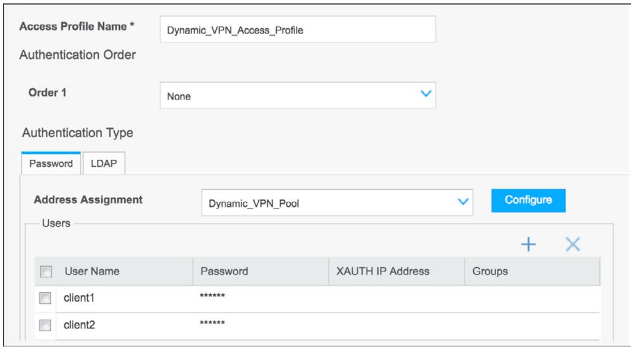
Subnet mask: 255 . 255 . 255 . 0 24

Figure 11.40 Remote VPN Clients Address Pool

You need to create an Access Profile to define how users are authenticated and the address pool they will use. Go to Configure/Authentication/Access Profiles and create a new one as shown in Figure 11.41, using the values below:

- Access Profile Name: *Dynamic_VPN_Access_Profile*
- Authentication Type: *Password*

- Create the VPN users and passwords for your own environment
- Address Assignment: *Dynamic_VPN_Pool* (the address pool just created)



Access Profile Name * Dynamic_VPN_Access_Profile

Authentication Order

Order 1 None

Authentication Type

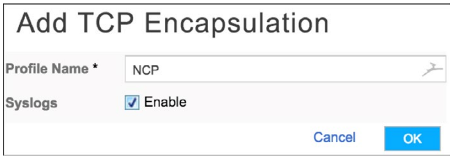
Address Assignment Dynamic_VPN_Pool

Users

□	User Name	Password	XAUTH IP Address	Groups
□	client1	******		
□	client2	******		

Figure 11.41 Remote VPN Access Profile

Now let's define the VPN parameters. Navigate to Configure/Security/IPsec VPN/Global Settings/ TCP-Encapsulation (NCP Path Finder technology). Add a new TCP Encapsulation with a profile name (here NCP) and with Syslogs *enabled*:



Add TCP Encapsulation

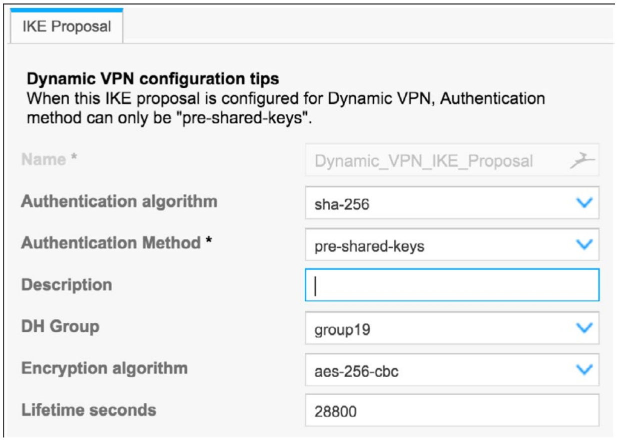
Profile Name * NCP

Syslogs ☑ Enable

Figure 11.42 TCP Encapsulation

On Configure/Security/IPsec VPN/IKE, create a new IKE Proposal for the Remote Access VPN using the following field information for Figure 11.43:

- Authentication algorithm: *sha256*
- Authentication method: *pre-shared-keys*
- Diffie Hellman Group: *group19*
- Encryption algorithm: *aes-256-cbc*
- Lifetime: *28800*



IKE Proposal

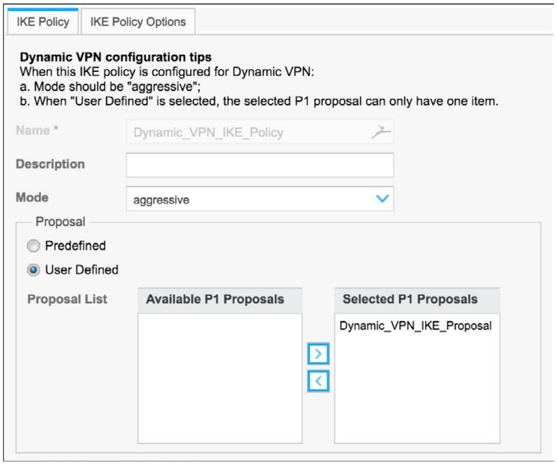
Dynamic VPN configuration tips
When this IKE proposal is configured for Dynamic VPN, Authentication method can only be "pre-shared-keys".

Name *	Dynamic_VPN_IKE_Proposal
Authentication algorithm	sha-256
Authentication Method *	pre-shared-keys
Description	
DH Group	group19
Encryption algorithm	aes-256-cbc
Lifetime seconds	28800

Figure 11.43 Remote VPN IKE Proposal Settings

Now create a new IKE Policy for the Remote Access VPN using the following field information in Figure 11.44:

- Connection Mode: *aggressive*
- Proposal: User Defined: *Dynamic_VPN_IKE_Proposal* (the one created in the preceding step)



IKE Policy | IKE Policy Options

Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN:
a. Mode should be "aggressive";
b. When "User Defined" is selected, the selected P1 proposal can only have one item.

Name *	Dynamic_VPN_IKE_Policy
Description	
Mode	aggressive

Proposal

○ Predefined
● User Defined

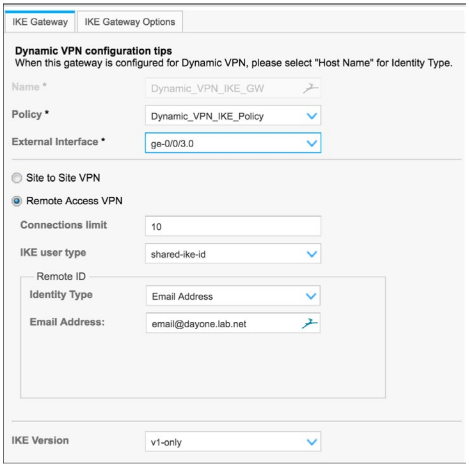
Proposal List

Available P1 Proposals	Selected P1 Proposals
	Dynamic_VPN_IKE_Proposal

Figure 11.44 Remote VPN IKE Policy Settings

In the IKE Policy Options tab create an ASCII-text pre-shared key. Go to IKE Gateway and configure it, as below:

- Policy: *Dynamic_VPN_IKE_Policy* (the policy we created in the step above)
- External interface: *ge-0/0/3.0* (or another interface you have defined)
- Remote Access VPN Mode
  - Connections limit: *10*
  - IKE user type: *shared-ike-id*
  - Identity type: *Email address*
  - Email Address: *email@dayone.lab.net* (use an equivalent for your domain)
- IKE Version: *v1-only*



Dynamic VPN configuration tips
When this gateway is configured for Dynamic VPN, please select "Host Name" for Identity Type.

Name * Dynamic_VPN_IKE_GW
Policy * Dynamic_VPN_IKE_Policy
External Interface * ge-0/0/3.0

○ Site to Site VPN
● Remote Access VPN

Connections limit 10
IKE user type shared-ike-id

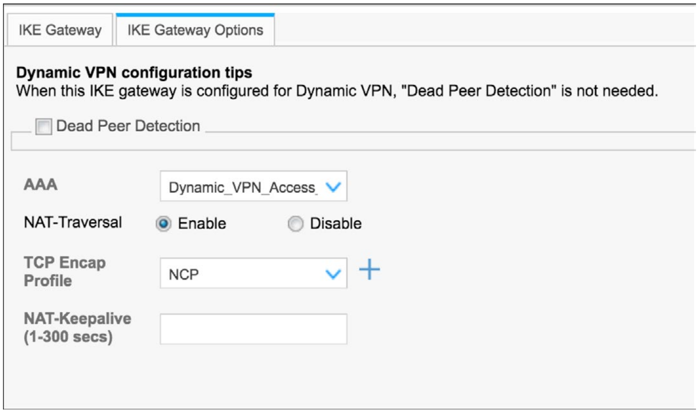
Remote ID
Identity Type Email Address
Email Address: email@dayone.lab.net

IKE Version v1-only

Figure 11.45 Remote VPN IKE Gateway Settings

In the IKE Gateway Options tab shown in Figure 11.46, define the following:

- AAA: *Dynamic_VPN_Access*
- *TCP Encap Profile: NCP*



Dynamic VPN configuration tips
When this IKE gateway is configured for Dynamic VPN, "Dead Peer Detection" is not needed.

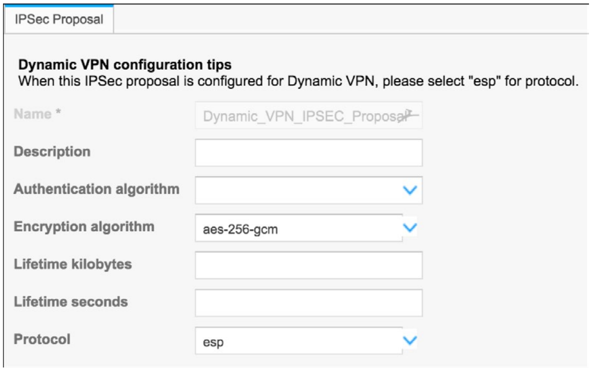
☐ Dead Peer Detection

AAA	Dynamic_VPN_Access
NAT-Traversal	● Enable ○ Disable
TCP Encap Profile	NCP
NAT-Keepalive (1-300 secs)	

Figure 11.46 *Remote VPN IKE Gateway Options*

Now let's configure the IPsec options. Navigate to Configure/Security/IPsec VPN/IPsec, and create a new IPsec Proposal as in Figure 11.47, and populate the fields with the following:

- Name: *Dynamic_VPN_IPsec_Proposal*
- Encryption algorithm: *aes-256-gcm*
- Protocol: *esp*



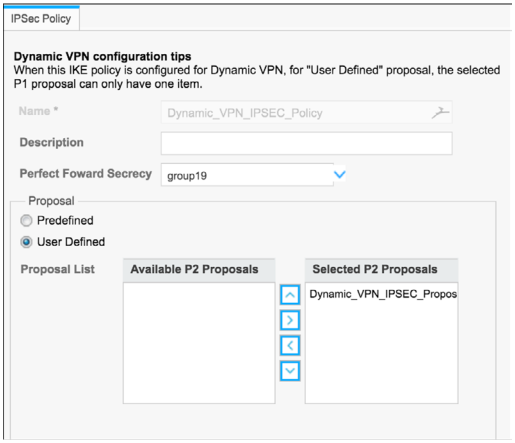
Dynamic VPN configuration tips
When this IPSec proposal is configured for Dynamic VPN, please select "esp" for protocol.

Name *	Dynamic_VPN_IPSEC_Proposal
Description	
Authentication algorithm	
Encryption algorithm	aes-256-gcm
Lifetime kilobytes	
Lifetime seconds	
Protocol	esp

Figure 11.47 *Remote VPN IPsec Proposal*

Now let's add a new IPsec Policy:

- Name: *Dynamic_VPN_IPsec_Policy*
- Perfect Forward Secrec: *group19*
- Proposal: *Dynamic_VPN_IPsec_Proposal*



IPSec Policy

Dynamic VPN configuration tips
When this IKE policy is configured for Dynamic VPN, for "User Defined" proposal, the selected P1 proposal can only have one item.

Name *: Dynamic_VPN_IPSEC_Policy

Description:

Perfect Foward Secrecy: group19

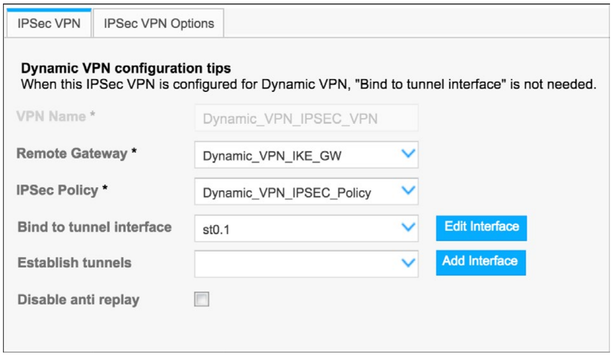
Proposal
○ Predefined
● User Defined

Proposal List
Available P2 Proposals:
Selected P2 Proposals: Dynamic_VPN_IPSEC_Propos

Figure 11.48 Remote VPN IPsec Policy

And add a new IPsec VPN:

- Remote Gateway: *Dynamic_VPN_IKE_GW*
- IPsec Policy: *Dynamic_VPN_IPsec_Policy*
- Bind to tunnel interface – *st0.1*



IPSec VPN | IPSec VPN Options

Dynamic VPN configuration tips
When this IPSec VPN is configured for Dynamic VPN, "Bind to tunnel interface" is not needed.

VPN Name *: Dynamic_VPN_IPSEC_VPN

Remote Gateway *: Dynamic_VPN_IKE_GW

IPSec Policy *: Dynamic_VPN_IPSEC_Policy

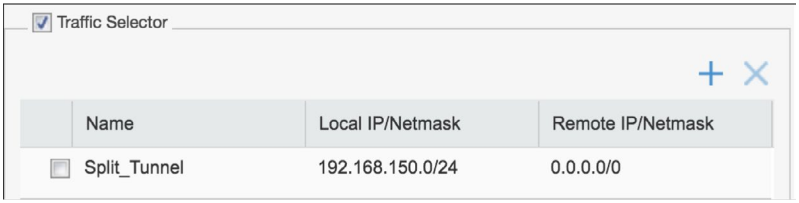
Bind to tunnel interface: st0.1 Edit Interface

Establish tunnels: Add Interface

Disable anti replay: □

Figure 11.49 Remote VPN IPsec VPN

Click in the IPsec VPN Options tab, and then define a new traffic selector: Split_Tunnel; Local Network: (*192.168.150.0/24); and* Remote Network: (*0.0.0.0/0*):



☑ Traffic Selector

	Name	Local IP/Netmask	Remote IP/Netmask
□	Split_Tunnel	192.168.150.0/24	0.0.0.0/0

Figure 11.50 Remote VPN Traffic Selector

NOTE You are adding a traffic selector only for the server network. Add others as you see fit. If you decide to not add a traffic selector, then the VPN client will be dedicated (no split tunneling).

You need to add a security policy to allow traffic from the Remote Access VPN to the Server Network. So let's create the following security policy, Zone VPN RA to Zone Server, with the following attributes:

- Source Address -> Remote Access Network: *192.168.50.0/24*
- Destination Address -> Server Network: *192.168.150.0/24*
- Services: *any*
- Action: *permit, log*

This concludes the SRX configuration.

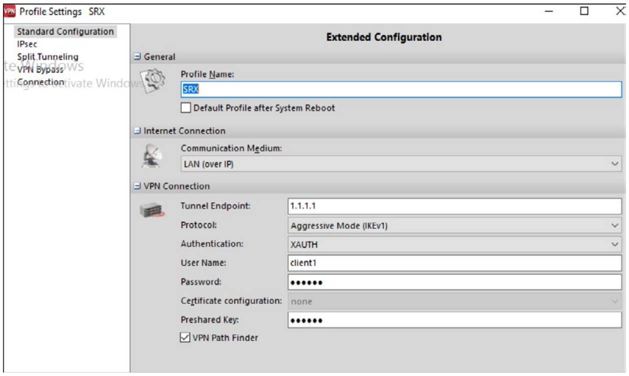
NCP VPN Client Configuration

For the NCP VPN client, we're using Windows OS but the steps are the same for other VPN clients as well.

After downloading and installing the VPN client application, open the client and click on Configuration/Profiles. Create a new profile with the following information as shown in Figure 11.51:

- Profile Name: *SRX*
- Tunnel Endpoint: *1.1.1.1* (change it accordingly for your environment – FQDN are also valid)
- Protocol: *Aggressive* (IKEv1)

- Username/password: *the user/password you created in the SRX*
- Pre-shared key: *use the pre-shared key you created in the SRX*



Extended Configuration

General

Profile Name: SRX

☐ Default Profile after System Reboot

Internet Connection

Communication Medium: LAN (over IP)

VPN Connection

Tunnel Endpoint: 1.1.1.1

Protocol: Aggressive Mode (IKEv1)

Authentication: XAUTH

User Name: client1

Password: ••••••

Certificate configuration: none

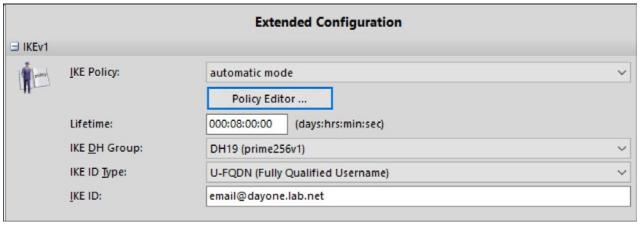
Preshared Key: ••••••

☑ VPN Path Finder

Figure 11.51 NCP Client Profile Standard Configuration

Click on IPsec in the left column. For IKEv1, configure the following parameters:

- IKE DH Group*: DH19*
- IKE ID Type*: U-FQDN*
- IKE ID: email@dayone.lab.net (use the value you configured on your IKE GW settings)



Extended Configuration

IKEv1

IKE Policy: automatic mode

Lifetime: 000:08:00:00 (days:hrs:min:sec)

IKE DH Group: DH19 (prime256v1)

IKE ID Type: U-FQDN (Fully Qualified Username)

IKE ID: email@dayone.lab.net

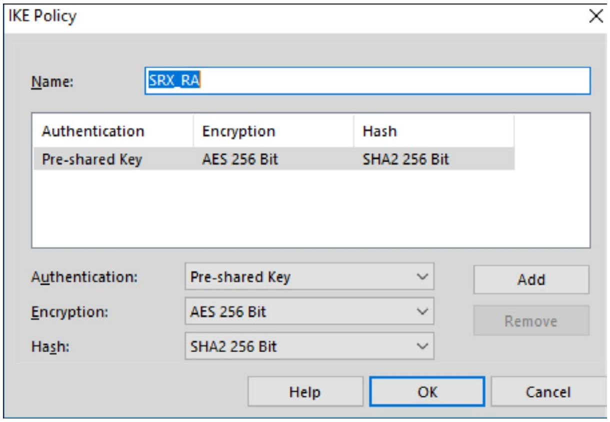
Figure 11.52 NCP Client Profile IKEv1 Configuration

Click on the Policy Editor button in Figure 11.52:

In Figure 11.53, remove any default options and create a new one. Let's name it *SRX_RA* and use the following values:

- Authentication: *Pre-shared key*
- Encryption: *AES 256 Bit*
- Hash: *SHA2 256 Bit*

Click OK:



Name: SRX_RA

Authentication	Encryption	Hash
Pre-shared Key	AES 256 Bit	SHA2 256 Bit

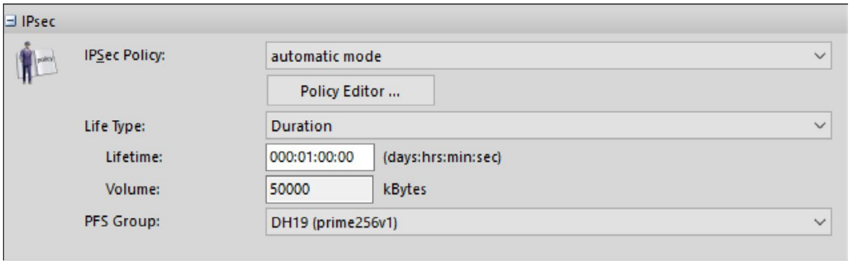
Authentication: Pre-shared Key

Encryption: AES 256 Bit

Hash: SHA2 256 Bit

Figure 11.53 NCP Client Profile IKE Policy Editor

Click on IPsec in the left column and for PFS Group choose DH19 as in Figure 11.54:



IPSec Policy: automatic mode

Life Type: Duration

Lifetime: 000:01:00:00 (days:hrs:min:sec)

Volume: 50000 kBytes

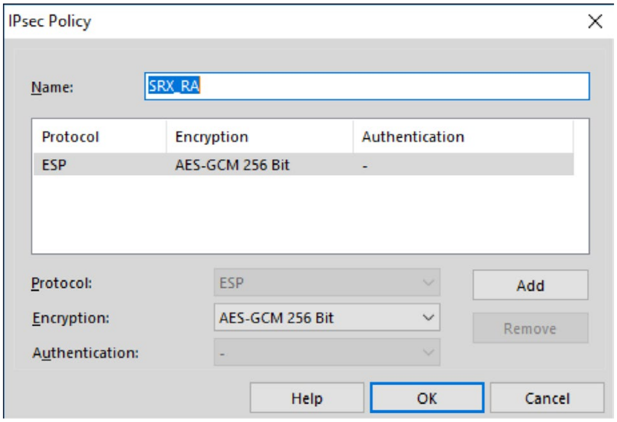
PFS Group: DH19 (prime256v1)

Figure 11.54 NCP Client Profile IPsec Configuration

Click on the Policy Editor button.

Remove the default options and create a new one as in Figure 11.55, named: *SRX_RA*. Use the following values:

- Protocol: *ESP*
- Encryption: *AES-GCM 256 bit*



Name: SRX_RA

Protocol	Encryption	Authentication
ESP	AES-GCM 256 Bit	-

Protocol: ESP

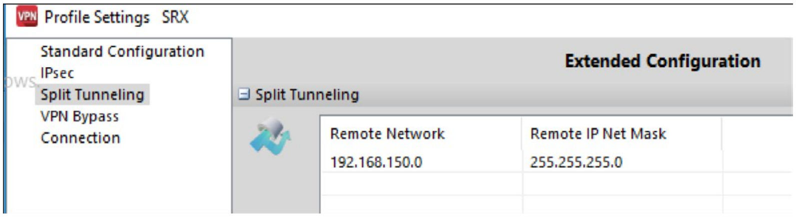
Encryption: AES-GCM 256 Bit

Authentication: -

Figure 11.55 NCP Client Profile IPsec Policy Editor

Go back to the main window, click on Split Tunneling in the left hand column, and configure a traffic selector for the server network with the following data:

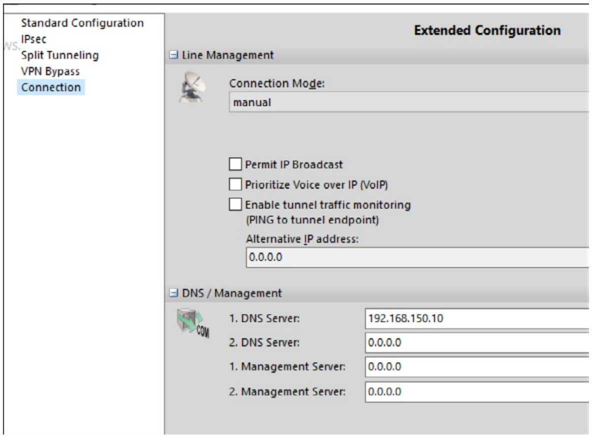
- Remote Network: *192.168.150.0*
- Network IP Net Mask: *255.255.255.0*



Remote Network	Remote IP Net Mask
192.168.150.0	255.255.255.0

Figure 11.56 NCP Client Profile Split Tunneling Options

In the main window, click on Connection, and add the DNS Server (*192.168.150.10* in this book's lab) as shown in Figure 11.57:



Connection Mode: manual

□ Permit IP Broadcast

□ Prioritize Voice over IP (VoIP)

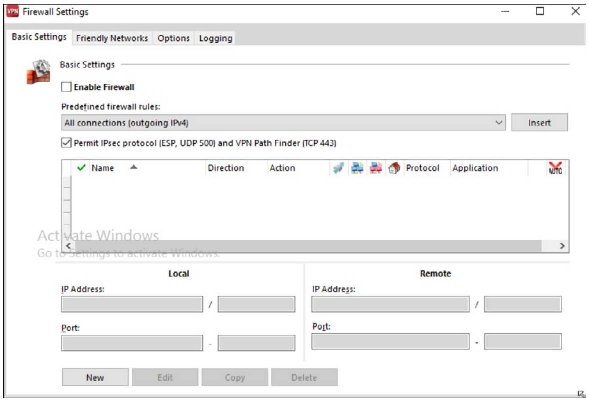
□ Enable tunnel traffic monitoring (PING to tunnel endpoint)

Alternative IP address: 0.0.0.0

1. DNS Server: 192.168.150.10
2. DNS Server: 0.0.0.0
1. Management Server: 0.0.0.0
2. Management Server: 0.0.0.0

Figure 11.57 NCP Client Profile Connection Options

Save the configuration and then click on Configuration/Firewall. If the firewall is enabled, make sure that the *Permit IPsec protocol* option is enabled as shown in Figure 11.58:



□ Enable Firewall

Predefined firewall rules: All connections (outgoing IPv4)

☑ Permit IPsec protocol (ESP, UDP 500) and VPN Path Finder (TCP 443)

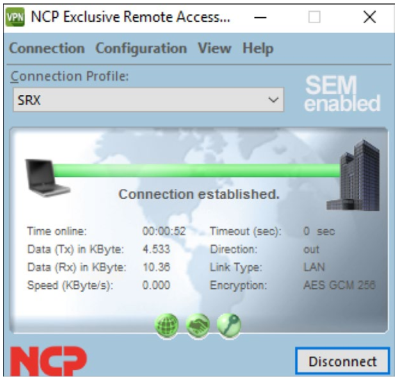
IP Address: /

Port: -

Figure 11.58 NCP Client Firewall Options

Save the configuration.

On the NCP client main screen, click on Connect and the connection should establish, as in Figure 11.59:


NCP Exclusive Remote Access...
Connection Configuration View Help
SEM enabled
NCP
Disconnect

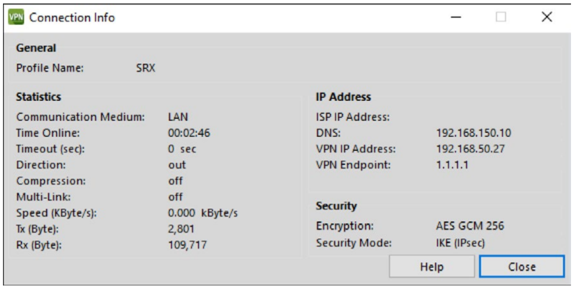
Connection Profile: SRX

Connection established.

Time online: 00:00:52
Data (Tx) in KByte: 4.533
Data (Rx) in KByte: 10.36
Speed (KByte/s): 0.000
Timeout (sec): 0 sec
Direction: out
Link Type: LAN
Encryption: AES GCM 256

Figure 11.59 *NCP Client VPN Established*

You can check the VPN details by clicking on Connection/Connection info, as shown in Figure 11.60:



General
Profile Name: SRX

Statistics
Communication Medium: LAN
Time Online: 00:02:46
Timeout (sec): 0 sec
Direction: out
Compression: off
Multi-Link: off
Speed (KByte/s): 0.000 kByte/s
Tx (Byte): 2,801
Rx (Byte): 109,717

IP Address
ISP IP Address:
DNS: 192.168.150.10
VPN IP Address: 192.168.50.27
VPN Endpoint: 1.1.1.1

Security
Encryption: AES GCM 256
Security Mode: IKE (IPsec)

Figure 11.60 *NCP Client VPN Connection Details*

This process will allow you to run the VPN client for 30 days, after which the client licenses need to be installed. Client licenses are loaded in the NCP Management Console, which also offers a centralized way to configure both VPN and firewall policies for multiple clients.

NOTE The NCP Server Management configuration is beyond the scope of this book.

Chapter 12

Logging and Reporting

The SRX Series allows a user to store events locally and to forward events to an external location, such as Junos Space Security Director, Juniper Security Analytics, or other third-party solutions. You can store logs locally and forward them to an external solution simultaneously.

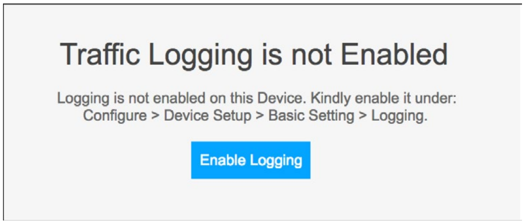
Having on-box log visibility helps teams that cannot have a large-scale solution, such as Junos Space Security Director, to easily monitor and troubleshoot security events and have visibility over the Layer 7 traffic.

This chapter explores how to enable on-box logging and reporting and how to visualize and sort through events.

Configuring On-box Logging and Reporting

So far, you have enabled logging in a few security policies, but as you haven't logged local (on-box) or forwarding (external destinations) yet, you actually haven't logged any data just yet.

To enable on-box logging, go to the J-Web GUI and navigate to Monitor/Events/All events. The message in Figure 12.1 will be displayed:



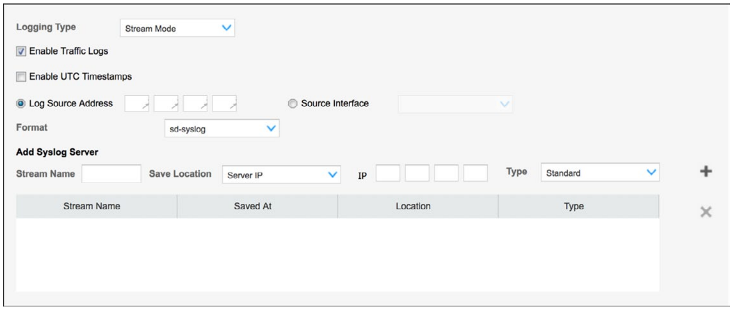
Traffic Logging is not Enabled

Logging is not enabled on this Device. Kindly enable it under: Configure > Device Setup > Basic Setting > Logging.

Figure 12.1 *Traffic Logging Warning*

Click on the Enable Logging button. You will be taken to the logging configuration screen. To configure on-box logging, configure the following parameters:

- Logging Type: *Stream Mode*
- Enable the Traffic Logs option
- Format: *sd-syslog*



Logging Type: Stream Mode

☑ Enable Traffic Logs

□ Enable UTC Timestamps

● Log Source Address ○ Source Interface

Format: sd-syslog

Add Syslog Server

Stream Name: Save Location: Server IP IP Type: Standard

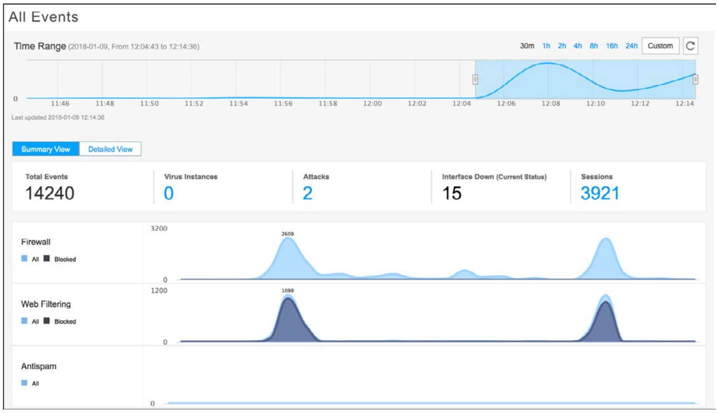
Stream Name	Saved At	Location	Type

Figure 12.2 *Log Configuration*

Click OK. A warning message will be displayed stating that no external syslog is configured. Just ignore it and commit your configuration.

Event Search

Now let's go back to Monitor/Events/All Events. As you can see in Figure 12.3, there are events being logged in the SRX:



All Events

Time Range (2018-01-09, From 12:04:43 to 12:14:36)

Last updated 2018-01-09 12:14:36

Total Events	Virus Instances	Attacks	Interface Down (Current Status)	Sessions
14240	0	2	15	3921

Figure 12.3 *Security Events Panel*

Let’s look into these in more detail. In the left panel, you can see that events are classified according to their criteria (Figure 12.4). This means you can look at all events, or click on the pre-defined views and have them pre-sorted for you:

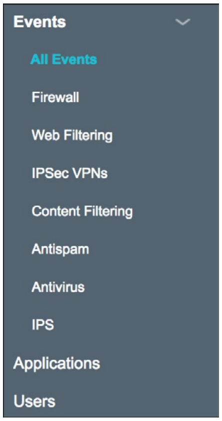
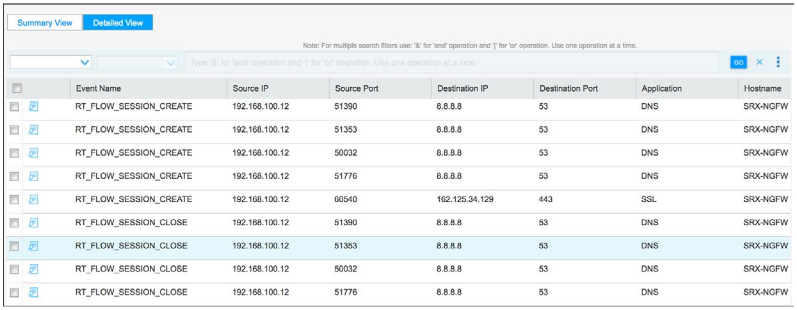


Figure 12.4 Security Events Panel

In the All Events Panel, click the Detailed View button. And, as shown in Figure 12.5, the security events are displayed with more details:



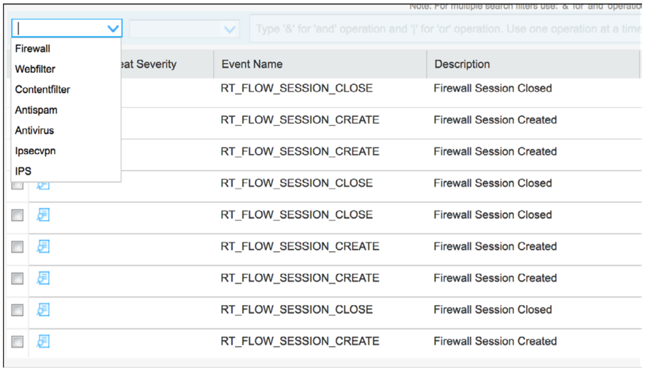
Note: For multiple search filters use: '&' for 'and' operation and '|' for 'or' operation. Use one operation at a time.

Type '&' for 'and' operation and '|' for 'or' operation. Use one operation at a time.

□	Event Name	Source IP	Source Port	Destination IP	Destination Port	Application	Hostname
□	RT_FLOW_SESSION_CREATE	192.168.100.12	51390	8.8.8.8	53	DNS	SRX-NGFW
□	RT_FLOW_SESSION_CREATE	192.168.100.12	51353	8.8.8.8	53	DNS	SRX-NGFW
□	RT_FLOW_SESSION_CREATE	192.168.100.12	50032	8.8.8.8	53	DNS	SRX-NGFW
□	RT_FLOW_SESSION_CREATE	192.168.100.12	51776	8.8.8.8	53	DNS	SRX-NGFW
□	RT_FLOW_SESSION_CREATE	192.168.100.12	60540	162.125.34.129	443	SSL	SRX-NGFW
□	RT_FLOW_SESSION_CLOSE	192.168.100.12	51390	8.8.8.8	53	DNS	SRX-NGFW
□	RT_FLOW_SESSION_CLOSE	192.168.100.12	51353	8.8.8.8	53	DNS	SRX-NGFW
□	RT_FLOW_SESSION_CLOSE	192.168.100.12	50032	8.8.8.8	53	DNS	SRX-NGFW
□	RT_FLOW_SESSION_CLOSE	192.168.100.12	51776	8.8.8.8	53	DNS	SRX-NGFW

Figure 12.5 Detailed View

Let's query a specific event. On the left side, click on the query fields and select IPS, as shown in Figure 12.6:



Note: For multiple search filters use: '&' for 'and' operatio

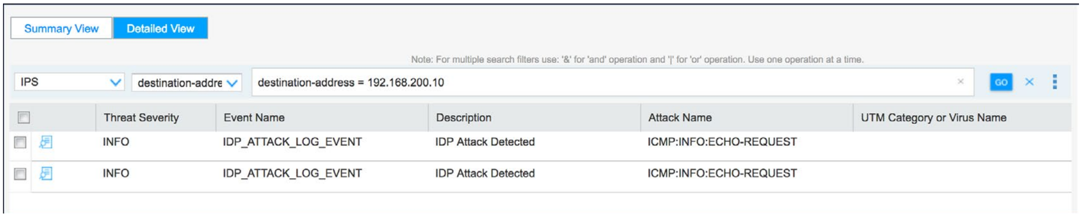
Type '&' for 'and' operation and '|' for 'or' operation. Use one operation at a time

at Severity	Event Name	Description
	RT_FLOW_SESSION_CLOSE	Firewall Session Closed
	RT_FLOW_SESSION_CREATE	Firewall Session Created
	RT_FLOW_SESSION_CREATE	Firewall Session Created
	RT_FLOW_SESSION_CLOSE	Firewall Session Closed
	RT_FLOW_SESSION_CLOSE	Firewall Session Closed
	RT_FLOW_SESSION_CREATE	Firewall Session Created
	RT_FLOW_SESSION_CREATE	Firewall Session Created
	RT_FLOW_SESSION_CLOSE	Firewall Session Closed
	RT_FLOW_SESSION_CREATE	Firewall Session Created

Figure 12.6 Search Options

You can refine your search by adding a destination IP address and then clicking in the Go button, as shown in Figure 12.7. In this book's lab, we're adding the IP 192.168.200.10 (the lab's web server).

TIP You can also concatenate more search items by using the operators (&&) or the pipe (|).



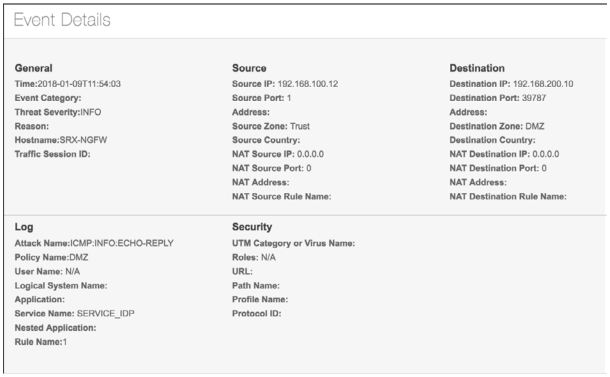
Note: For multiple search filters use: '&' for 'and' operation and '|' for 'or' operation. Use one operation at a time.

IPS | destination-addre | destination-address = 192.168.200.10

	Threat Severity	Event Name	Description	Attack Name	UTM Category or Virus Name
□	INFO	IDP_ATTACK_LOG_EVENT	IDP Attack Detected	ICMP:INFO:ECHO-REQUEST	
□	INFO	IDP_ATTACK_LOG_EVENT	IDP Attack Detected	ICMP:INFO:ECHO-REQUEST	

Figure 12.7 Search Parameters

Click on one of the events and look for details as shown in Figure 12.8. You can have all the parsed information about the event:



Event Details

General
Time:2018-01-09T11:54:03
Event Category:
Threat Severity:INFO
Reason:
Hostname:SRX-NGFW
Traffic Session ID:

Source
Source IP: 192.168.100.12
Source Port: 1
Address:
Source Zone: Trust
Source Country:
NAT Source IP: 0.0.0.0
NAT Source Port: 0
NAT Address:
NAT Source Rule Name:

Destination
Destination IP: 192.168.200.10
Destination Port: 39787
Address:
Destination Zone: DMZ
Destination Country:
NAT Destination IP: 0.0.0.0
NAT Destination Port: 0
NAT Address:
NAT Destination Rule Name:

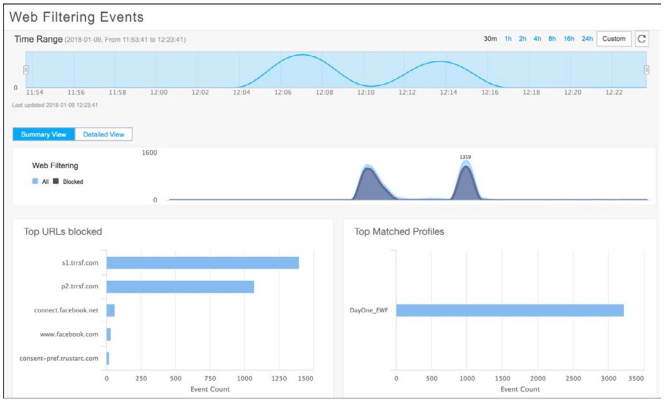
Log
Attack Name:ICMP:INFO:ECHO-REPLY
Policy Name:DMZ
User Name: N/A
Logical System Name:
Application:
Service Name: SERVICE_IDP
Nested Application:
Rule Name:1

Security
UTM Category or Virus Name:
Roles: N/A
URL:
Path Name:
Profile Name:
Protocol ID:

Figure 12.8 Event Details

Drill down into one of the security event categories.

Click on Events /Web Filtering. You are presented with a dashboard with information related to the specific category you are looking at. The same applies for all the other categories:



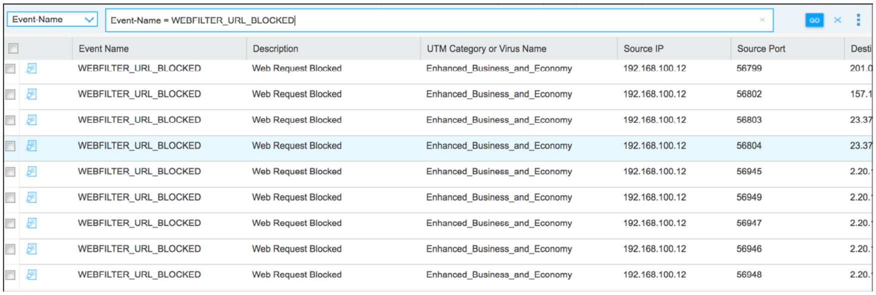
Web Filtering Events

Time Range (2018-01-09, From 11:53:41 to 12:23:41)

Last updated 2018-01-09 12:23:41

Figure 12.9 Web Filtering Dashboard

Click on Detailed View, and you will be presented with only web filter-related events, as you can see in Figure 12.10. You can now search specific event filters:



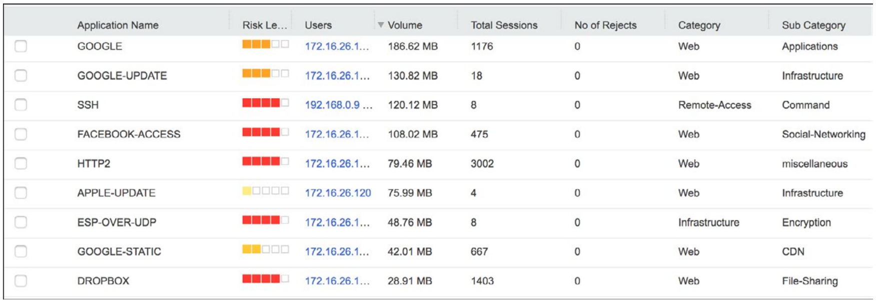
□		Event Name	Description	UTM Category or Virus Name	Source IP	Source Port	Desti
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56799	201.0
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56802	157.1
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56803	23.37
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56804	23.37
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56945	2.20.
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56949	2.20.
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56947	2.20.
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56946	2.20.
□		WEBFILTER_URL_BLOCKED	Web Request Blocked	Enhanced_Business_and_Economy	192.168.100.12	56948	2.20.

Figure 12.10 Web Filtering Events

Application and User Visibility

Additional interesting features are the Application and User Visibility panels. They allow administrators a quick view of what applications are consuming the network and the top user IPs.

Click on the Monitor/Applications panel. You can select among bubble or grid view. In Figure 12.11 you can see the grid view:

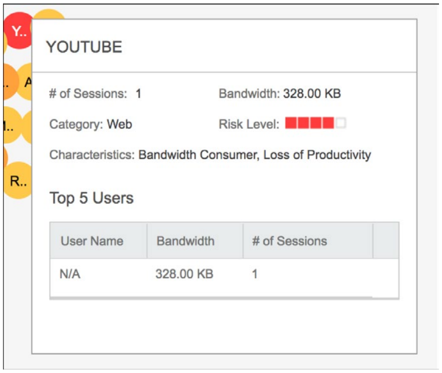


	Application Name	Risk Le...	Users	Volume	Total Sessions	No of Rejects	Category	Sub Category
□	GOOGLE	■■■□□	172.16.26.1...	186.62 MB	1176	0	Web	Applications
□	GOOGLE-UPDATE	■■■□□	172.16.26.1...	130.82 MB	18	0	Web	Infrastructure
□	SSH	■■■■□	192.168.0.9 ...	120.12 MB	8	0	Remote-Access	Command
□	FACEBOOK-ACCESS	■■■■□	172.16.26.1...	108.02 MB	475	0	Web	Social-Networking
□	HTTP2	■■■■□	172.16.26.1...	79.46 MB	3002	0	Web	miscellaneous
□	APPLE-UPDATE	■□□□□	172.16.26.120	75.99 MB	4	0	Web	Infrastructure
□	ESP-OVER-UDP	■■■■□	172.16.26.1...	48.76 MB	8	0	Infrastructure	Encryption
□	GOOGLE-STATIC	■■□□□	172.16.26.1...	42.01 MB	667	0	Web	CDN
□	DROPBOX	■■■■□	172.16.26.1...	28.91 MB	1403	0	Web	File-Sharing

Figure 12.11 Application Visibility

The grid view allows you to identify applications, volume used, sessions related, AppFW drops, and users' IPs using the application.

In bubble view, rolling your mouse over an application also allows you to view the same information, as in Figure 12.12:



YOUTUBE

# of Sessions: 1

Bandwidth: 328.00 KB

Category: Web

Risk Level: 🟥🟥🟥🟥□

Characteristics: Bandwidth Consumer, Loss of Productivity

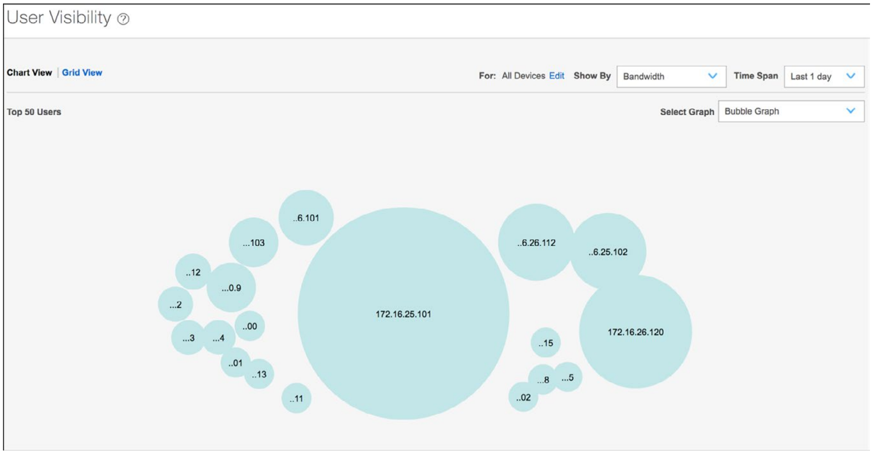
Top 5 Users

User Name	Bandwidth	# of Sessions
N/A	328.00 KB	1

Figure 12.12 Application Usage Details

Now, click on the Monitor/Users panel.

You have the same view, but in Figure 12.13, it's from the user/IP perspective. You can see which users or which IP addresses are consuming bandwidth or sessions, and view which applications are used by those users and IPs:



User Visibility

Chart View | Grid View

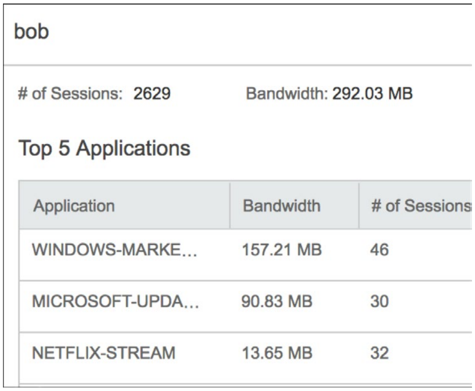
For: All Devices Edit Show By Bandwidth Time Span Last 1 day

Top 50 Users

Select Graph Bubble Graph

Figure 12.13 User Visibility

If you select a specific IP or username, such as bob in Figure 12.14, then you will be able to visualize the applications most used, and the bandwidth or sessions consumed:



bob

# of Sessions: 2629 Bandwidth: 292.03 MB

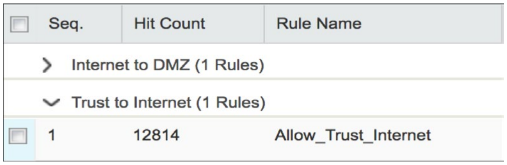
Top 5 Applications

Application	Bandwidth	# of Sessions
WINDOWS-MARKE...	157.21 MB	46
MICROSOFT-UPDA...	90.83 MB	30
NETFLIX-STREAM	13.65 MB	32

Figure 12.14 User Visibility Details

Firewall Hit Counters

Another interesting information source available to you is the Hit Counter. Selecting a firewall rule will present you with the Hit Count column. It displays the number of session hits of a given policy such as in Figure 12.15:



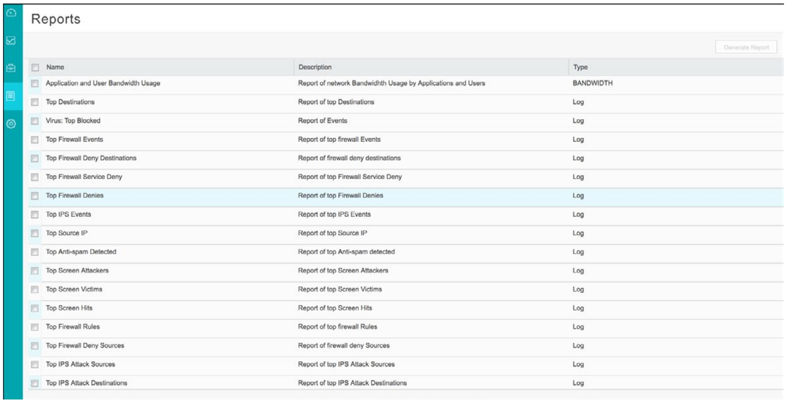
□	Seq.	Hit Count	Rule Name
	› Internet to DMZ (1 Rules)		
	⌄ Trust to Internet (1 Rules)		
□	1	12814	Allow_Trust_Internet

Figure 12.15 Firewall Hit Counters

Reports

The SRX Series allows you to generate pre-defined reports and offers some basic customization options.

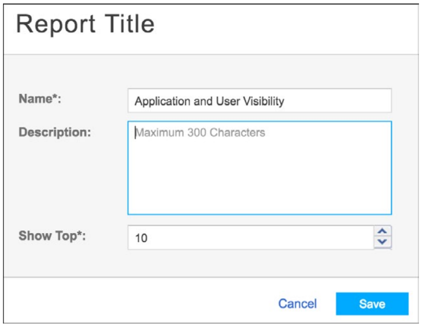
Click on Reports, and a list of available reports will appear:



□ Name	Description	Type
□ Application and User Bandwidth Usage	Report of network Bandwidhth Usage by Applications and Users	BANDWIDTH
□ Top Destinations	Report of top Destinations	Log
□ Virus: Top Blocked	Report of Events	Log
□ Top Firewall Events	Report of top firewall Events	Log
□ Top Firewall Deny Destinations	Report of firewall deny destinations	Log
□ Top Firewall Service Deny	Report of top Firewall Service Deny	Log
□ Top Firewall Denies	Report of top Firewall Denies	Log
□ Top IPS Events	Report of top IPS Events	Log
□ Top Source IP	Report of top Source IP	Log
□ Top Anti-spam Detected	Report of top Anti-spam detected	Log
□ Top Screen Attackers	Report of top Screen Attackers	Log
□ Top Screen Victims	Report of top Screen Victims	Log
□ Top Screen Hits	Report of top Screen Hits	Log
□ Top Firewall Rules	Report of top firewall Rules	Log
□ Top Firewall Deny Sources	Report of firewall deny Sources	Log
□ Top IPS Attack Sources	Report of top IPS Attack Sources	Log
□ Top IPS Attack Destinations	Report of top IPS Attack Destinations	Log

Figure 12.16 List of Pre-Defined Reports

Select one of the reports and click on Generate report. Customize the report name, add a Description, and the number of Top Events you want to be displayed as shown in Figure 12.17:


Report Title

Name*: Application and User Visibility

Description: Maximum 300 Characters

Show Top*: 10

Figure 12.17 Report Customization

MORE? If you need customizable reports, or reports that are not available in the on-box version, Juniper offers Junos Space Security Director and Secure Analytics. Both products have full report customization capabilities. See https://www.juniper.net/us/en/products-services/security/.

The SRX can generate reports and download them to your computer. You can see some examples in Figure 12.18 and Figure 12.19:

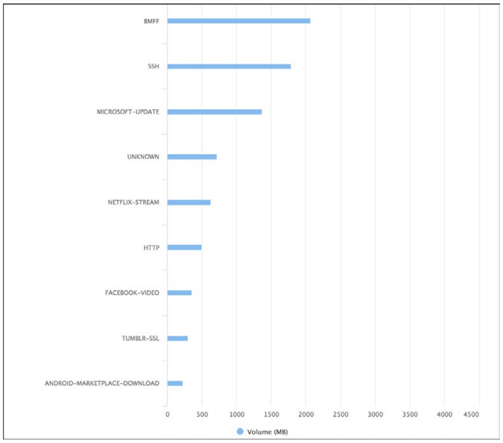
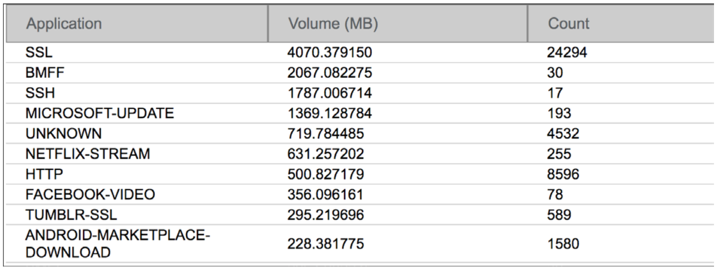


Figure 12.18 Application and User Visibility Report Screenshot Example



Application	Volume (MB)	Count
SSL	4070.379150	24294
BMFF	2067.082275	30
SSH	1787.006714	17
MICROSOFT-UPDATE	1369.128784	193
UNKNOWN	719.784485	4532
NETFLIX-STREAM	631.257202	255
HTTP	500.827179	8596
FACEBOOK-VIDEO	356.096161	78
TUMBLR-SSL	295.219696	589
ANDROID-MARKETPLACE-DOWNLOAD	228.381775	1580

Figure 12.19 Application and User Visibility Report Screenshot Example (cont.)

Chapter 13

Basic Administration and Monitoring

The SRX Series, as does any other networking device, requires management. Tasks like managing users, monitoring the device performance and health, configuration backup and restore, and OS upgrades are common for security administrators. This chapter covers the most common tasks a SRX administrator needs to execute.

Managing Users

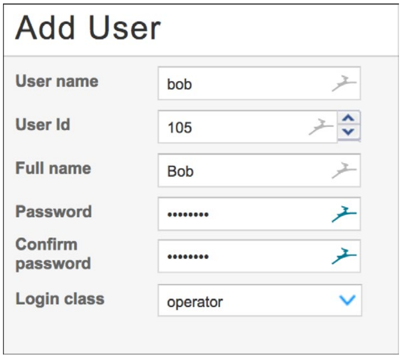
Junos OS supports local and external user authentication methods, such as local passwords, Radius, and TACACs+ servers.

On large networks, administrators rely on a centralized system to manage all accounts and roles. On others, local users are enough.

This section explains how to create a local user.

On J-Web, go to Configure/Basic Settings/User Management. Click on the pencil icon. In the Users tab, click on Add. And on Add user, define the following parameters:

- Username
- User Id
- Full name
- Password
- Login Class



Add User

User name: bob

User Id: 105

Full name: Bob

Password: ••••••••

Confirm password: ••••••••

Login class: operator

Figure 13.1 *Adding Users to the SRX*

With login classes, administrators can enforce the following:

- Access privileges that users have when they are logged in to the router or switch.
- Commands and statements that users can and cannot specify.
- How long a log in session can be idle before it times out and the user is logged out.

Junos has four predefined user accounts that cannot be renamed or modified: *operator*, *read-only*, *super-user*, and *unauthorized*.

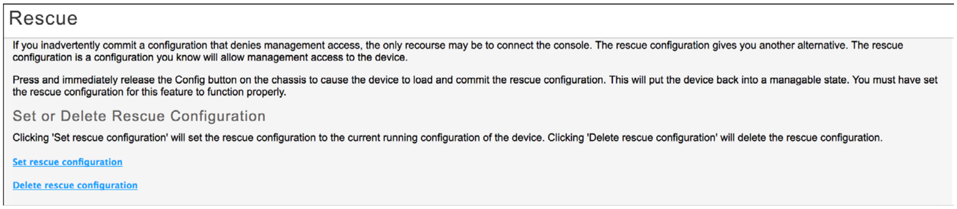
A *class* is a container of permissions that defines allowed/denied commands and configuration options.

Setting Up a Rescue Configuration

Sometimes, things can go wrong. In situations where you inadvertently commit a configuration that denies management access to the SRX or breaks some configuration that impacts the whole network, the rescue configuration comes in handy.

The rescue configuration is a configuration that restores the SRX to a state where the critical services are properly running and/or management access is restored. From there, you can restore a backup or have time to perform the proper analysis.

To set up the rescue configuration navigate to Administration/Config Management/Rescue. Click on *Set rescue configuration* as shown in Figure 13.2:



Rescue

If you inadvertently commit a configuration that denies management access, the only recourse may be to connect the console. The rescue configuration gives you another alternative. The rescue configuration is a configuration you know will allow management access to the device.

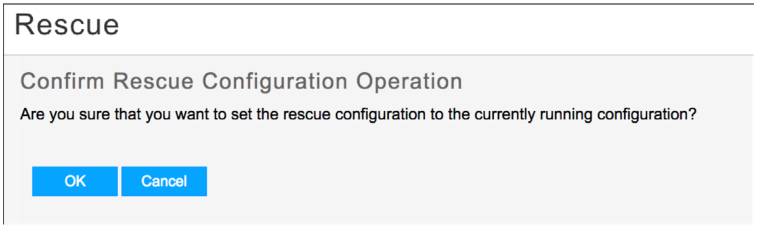
Press and immediately release the Config button on the chassis to cause the device to load and commit the rescue configuration. This will put the device back into a managable state. You must have set the rescue configuration for this feature to function properly.

Set or Delete Rescue Configuration

Clicking 'Set rescue configuration' will set the rescue configuration to the current running configuration of the device. Clicking 'Delete rescue configuration' will delete the rescue configuration.

Figure 13.2 *Enabling the Rescue Configuration*

Next, click OK on the confirmation page:



Rescue

Confirm Rescue Configuration Operation

Are you sure that you want to set the rescue configuration to the currently running configuration?

Figure 13.3 *Confirm Rescue Configuration*

IMPORTANT When enabling the rescue configuration, your active configuration is used. Make sure you enable it once the critical functions of the device are configured and management access is granted.

To activate the Rescue configuration – in case you're unable to access the SRX – at any moment, press and immediately release the *Reset Config* button on the chassis to cause the device to load and commit the rescue configuration. The *Reset Config* button is recessed to prevent it from being pressed accidentally. You will need to insert a small probe (for example, a straightened paper clip) to press the button.

Backup/Restore Configuration

It's very important to have a method of *backing up and restoring* the SRX configuration, just in case. There are several ways this can be achieved in Junos, via scripts, automation tools, or manually. One of the great options that the SRX Series provides is allowing administrators to execute an automated backup every time they commit a configuration.

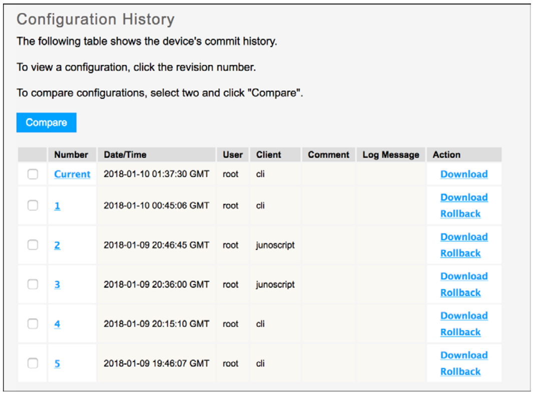
To do this, go to the CLI and execute the following command in configuration mode:

```
set system archival configuration transfer-on-commit archive-sites sftp://user:password@sftp_server_ip
```

The command specifies:

- User: the SFTP server user with proper permissions
- Password: User password
- STFP Server IP: the IP address of the SFTP server

On the GUI, you can manually back up or restore a configuration. To do this, go to Administration/Configuration Management/History and select the desired configuration and click on Download, as shown in Figure 13.4:



Configuration History

The following table shows the device's commit history.

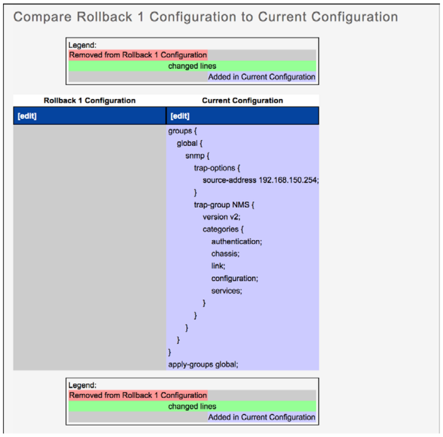
To view a configuration, click the revision number.

To compare configurations, select two and click "Compare".

	Number	Date/Time	User	Client	Comment	Log Message	Action
☐	Current	2018-01-10 01:37:30 GMT	root	cli			Download
☐	1	2018-01-10 00:45:06 GMT	root	cli			Download Rollback
☐	2	2018-01-09 20:46:45 GMT	root	junoscript			Download Rollback
☐	3	2018-01-09 20:36:00 GMT	root	junoscript			Download Rollback
☐	4	2018-01-09 20:15:10 GMT	root	cli			Download Rollback
☐	5	2018-01-09 19:46:07 GMT	root	cli			Download Rollback

Figure 13.4 *Download a Configuration*

If you are unsure which configuration you should download, you can always compare them. Select any two configurations and click on the Compare button. Now you can visualize their differences as in Figure 13.5:



Compare Rollback 1 Configuration to Current Configuration

Legend:
Removed from Rollback 1 Configuration
changed lines
Added in Current Configuration

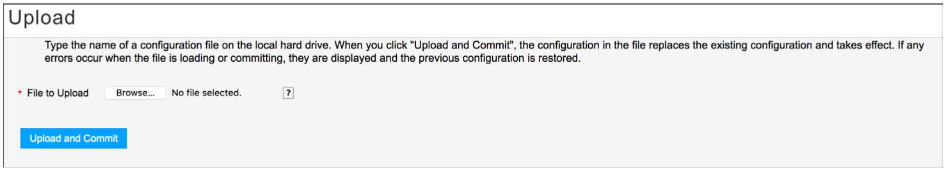
Rollback 1 Configuration	Current Configuration
[edit]	[edit]

```
groups {
    global {
        snmp {
            trap-options {
                source-address 192.168.150.254;
            }
            trap-group NMS {
                version v2;
                categories {
                    authentication;
                    chassis;
                    link;
                    configuration;
                    services;
                }
            }
        }
    }
}
apply-groups global;
```

Legend:
Removed from Rollback 1 Configuration
changed lines
Added in Current Configuration

Figure 13.5 *Comparing Configurations*

To restore a configuration, go to Administration/Configuration Management/Upload and select the configuration that needs to be uploaded, click the Upload and Commit button shown in Figure 13.6:



Upload

Type the name of a configuration file on the local hard drive. When you click "Upload and Commit", the configuration in the file replaces the existing configuration and takes effect. If any errors occur when the file is loading or committing, they are displayed and the previous configuration is restored.

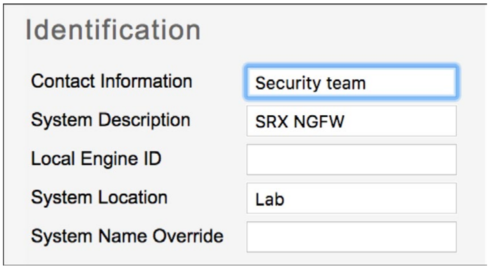
* File to Upload Browse... No file selected.

Figure 13.6 *Restoring a Configuration*

Configuring SNMP

Monitoring the SRX is a very important task. One of the traditional ways of doing this is to use the SNMP protocol to obtain performance and health visibility about your device.

Here's the procedure to configure SNMP. First navigate to Configuration/Basic/Settings/SNMP, and start by inserting the device information as shown in Figure 13.7. You can type only the information that makes sense to your environment, but it's wise to include at least the contact information, system description, and location:



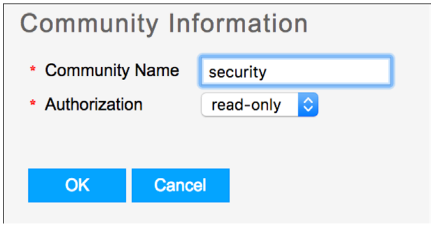
Identification

Contact Information	Security team
System Description	SRX NGFW
Local Engine ID	
System Location	Lab
System Name Override	

Figure 13.7 *SNMP Identification*

Let's now create a SNMP community.

Under Communities click on the Add link. Define a community name and authorization level as in Figure 13.8:



Community Information

* Community Name: security

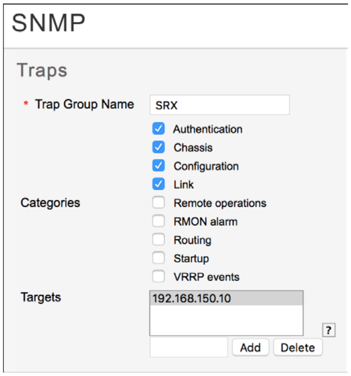
* Authorization: read-only

Figure 13.8 SNMP Community Configuration

Now, let's add a SNMP Trap group, where the SRX will be sending messages. Click on Configuration/Basic Settings/SNMP. Add a new Trap Group. Create a new Group Name, *SNMP-Server.* Now add the following traps (add others as needed):

- Authentication
- Chassis
- Configuration
- Link

Finally, add a Target Server IP (here, *192.168.150.10*) as shown in Figure 13.9:



SNMP

Traps

* Trap Group Name: SRX

Categories:
☑ Authentication
☑ Chassis
☑ Configuration
☑ Link
☐ Remote operations
☐ RMON alarm
☐ Routing
☐ Startup
☐ VRRP events

Targets: 192.168.150.10

Figure 13.9 SNMP Community Configuration

NOTE You can add other SNMP targets and send specific traps to each target.

Figure 13.10 is an example of a SNMP system configured to receive traps from the SRX:

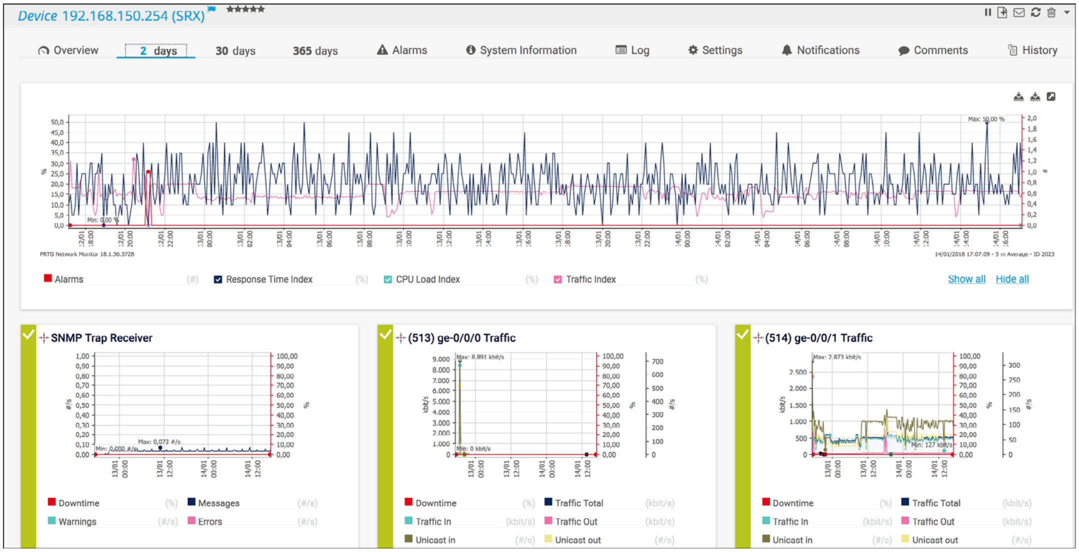


Figure 13.10 Enterprise-Grade SNMP Monitoring System Displaying SRX Statistics

MORE? You need to load the proper Juniper MIBs in your SNMP monitoring system for a proper parser and correct process to occur. Loading MIB files in a third-party system is beyond the scope of this book but you can get more instruction here: https://www.juniper.net/documentation/en_US/junos/topics/task/operational/mib-loadng-to-nms-junos-nm.html.

SRX Health Monitoring

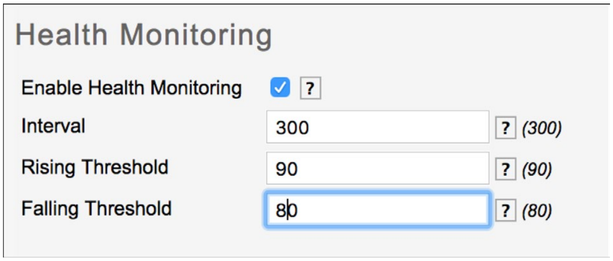
Health monitoring is an SNMP feature that extends the RMON alarm infrastructure to provide monitoring for a predefined set of objects (such as file system usage, CPU usage, and memory usage) for Junos processes.

You can also configure health monitor parameters such as a falling threshold, a rising threshold, and an interval. If the value of a monitored object exceeds the rising or falling threshold, an alarm is triggered and an event may be logged.

The falling threshold is the lower threshold for the monitored object instance. The rising threshold is the upper threshold for the monitored object instance. Each threshold is expressed as a percentage of the maximum possible value. The interval represents the period of time, in seconds, over which the object instance is sampled and compared with the rising and falling thresholds.

Events are only generated when a threshold is first crossed in any one direction, rather than after each sample interval. For example, if a rising threshold alarm, along with its corresponding event, is raised, no more threshold crossing events occur until a corresponding falling alarm occurs.

To configure Health Monitoring, simply go to Configure/Basic Settings/SNMP and define the thresholds in the Health Monitoring area as shown in Figure 13.11:



Health Monitoring

Enable Health Monitoring ☑ ?

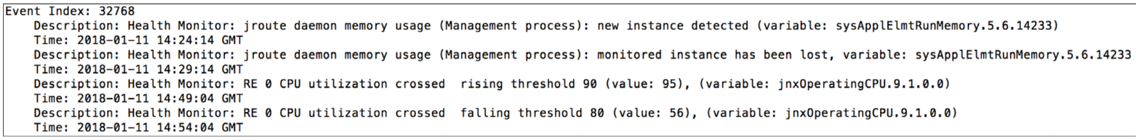
Interval 300 ? (300)

Rising Threshold 90 ? (90)

Falling Threshold 80 ? (80)

Figure 13.11 SNMP Community Configuration

You can visualize the results using the operational *show snmp health-monitor* command. The snippet shown in Figure 13.12 provides an example of a situation where a routing engine CPU has crossed the thresholds:



```
Event Index: 32768
    Description: Health Monitor: jroute daemon memory usage (Management process): new instance detected (variable: sysApplElmtRunMemory.5.6.14233)
    Time: 2018-01-11 14:24:14 GMT
    Description: Health Monitor: jroute daemon memory usage (Management process): monitored instance has been lost, variable: sysApplElmtRunMemory.5.6.14233
    Time: 2018-01-11 14:29:14 GMT
    Description: Health Monitor: RE 0 CPU utilization crossed  rising threshold 90 (value: 95), (variable: jnxOperatingCPU.9.1.0.0)
    Time: 2018-01-11 14:49:04 GMT
    Description: Health Monitor: RE 0 CPU utilization crossed  falling threshold 80 (value: 56), (variable: jnxOperatingCPU.9.1.0.0)
    Time: 2018-01-11 14:54:04 GMT
```

Figure 13.12 Health Monitoring Alarms

SRX Performance Monitoring

The SRX Series also includes important performance monitoring commands that can be visualized in the CLI, (operational mode) as shown in Table 13.1.

Table 13.1 Key Performance Monitoring Commands

Firewall (dataplane SPU performance)	`show security monitoring performance spu`
Firewall (networking sessions)	`show security monitoring performance session`

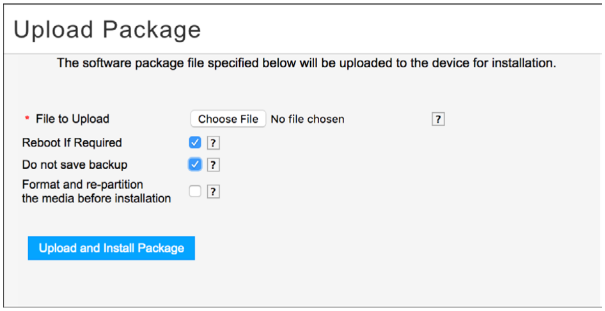
Firewall (performance per FPC) (On most of the SRX Branch platforms, the FPC slot is 0.)	`show security monitoring fpc slot`
Firewall (UTM sessions)	`show security utm session`
Firewall (UTM Anti-Virus)	`show security utm anti-virus statistics`
Firewall (UTM Web-Filtering)	`show security utm anti-virus statistics`
Firewall (UTM Content-Filtering)	`show security utm content-filtering statistics`
Firewall (UTM Anti-Spam)	`show security utm anti-spam statistics`
Firewall (IPS)	`show security idp status`
Firewall (Sky-ATP)	`show services advanced-anti-malware statistics`
Firewall (Security-Intelligence)	`show services security-intelligence statistics`
Firewall (routing engine)	`show chassis routing engine`
Networking Interfaces	`show interfaces interface name statistics detail`

Junos OS Upgrade

Upgrading the operational system of a critical device such as a firewall is an important task and pre-planning is recommended. If possible, always validate the new version in a lab before applying the upgrade. Also, have a backup plan in place (maintenance window time, downgrade image, backup configuration, console cable available, etc.)

When all the preparation is done, select your preferred upgrade method (GUI or CLI) and proceed with your task. (This book covers the J-Web procedure.)

Navigate to the Administration/Devices/Software/Upload package. Select the new image you want to upload. Enable the Reboot if Required option shown in Figure 13.13. If you want to save disk space, enable the *Do not save backup* option:



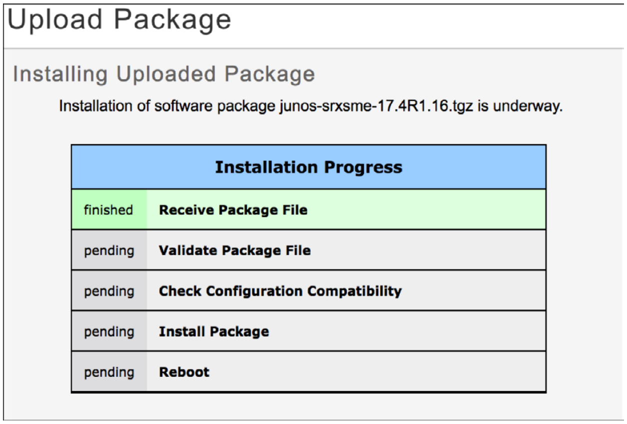
Upload Package

The software package file specified below will be uploaded to the device for installation.

- * File to Upload: Choose File No file chosen ?
- Reboot If Required ☑ ?
- Do not save backup ☑ ?
- Format and re-partition the media before installation □ ?

Figure 13.13 *Junos Upgrade Settings*

You can monitor the upload status from J-Web. After the image is uploaded, J-Web will display the upgrade status as shown in Figure 13.14:



Upload Package

Installing Uploaded Package

Installation of software package junos-srxsme-17.4R1.16.tgz is underway.

Installation Progress	
finished	**Receive Package File**
pending	**Validate Package File**
pending	**Check Configuration Compatibility**
pending	**Install Package**
pending	**Reboot**

Figure 13.14 *Junos Upgrade Status*

After the upgrade process is completed, the system will automatically reboot (depending on the options enabled) or will require a manual reboot. After rebooting, you will be at log in again.

If any errors occur when the file is loading or committing, they are displayed, and the previous configuration is restored.

Chapter 14

Troubleshooting

Once in a while, security teams have to troubleshoot issues that appear in the network. As discussed, the SRX Series offers administrators great graphical tools to search for security events and find why things are happening. But sometimes it is necessary to dig down on an issue, and for that Junos offers additional tools to help administrators to know what to do.

Hence this chapter provides a few tips that serve as a starting point to detect and fix common network connectivity problems.

Session Flow Troubleshooting

Session troubleshooting is one of the most critical skills an administrator needs to develop in the SRX.

Use the ensuing workflow as a reference for you to build up your own.

Is the packet arriving on the SRX?

The first thing that should be checked is to make sure that the traffic is arriving on the SRX itself.

The SRX should be able to show the traffic processed by just viewing the output of the debug itself. This may not be the case if stateless firewall filters are being used, which may drop the packets before they are processed by the flow engine. If stateless packet filtering is used, ensure that the filters are not blocking the traffic by reviewing the configuration, or adding the log option to the *then* statement of the deny filter to log the packets on the SRX.

If you don't see the traffic arriving on the SRX, you should check the routing table of the peer device, as well as checking to see if the peer device has an ARP entry for the IP address that is to be reached. This is particularly important if you are using static NAT, as Proxy ARP may be required.

Is the packet being blocked by a SCREENS?

If a packet is an invalid packet, and screens are enabled on the source zone, they may be dropped. An example would be a packet that has a SYN, ACK, and FIN bits set. Check the output of SCREENS statistic for counters by using the `show security screen statistics zone (insert zone name here)` command. You can also check the messages log file for additional information.

Is the session asymmetric?

The SRX is a stateful device, which means that if the SRX does not see the SYN packet from a given session, the flow will never go through packet/flow processing and the flow will never be inserted in the session table.

So, if the SRX doesn't see the SYN packet but it sees the following packets, it will drop the subsequent packets and the session will not be established.

Also, if the SRX cannot see both directions of the flow then some features such features as AppSecure, UTM, IPS, and Sky ATP may not be able to work. Therefore, it is recommended you design your network so that asymmetric flow does not occur in the location where the firewall is deployed.

Is the packet arriving on the correct interface/zone?

When looking at command outputs, you should be able to tell what interface the packet has arrived on, and subsequently, what the source zone is. This is important for policy lookup, and if it is not matched properly, then most likely a problem will occur.

Is the appropriate route / L2 forwarding path being selected?

Depending on if you are using Layer 3 mode or Transparent mode, the SRX will need to ensure that the appropriate forwarding decision is chosen. With Layer 3 mode, the firewall will do a route lookup based on the destination of the route, which will determine what the egress interface will be (which also determines the to-zone). If the device is in Transparent mode, the device will either do an ARP, or will broadcast the packet out all interfaces (except that from which it came) in the same bridging domain. If the wrong route is set (in transparent mode, the forwarding decision should happen without intervention, unless other mechanisms such as Dynamic ARP inspection or L2 Broadcast filtering are in place to block this), then the SRX may chose the wrong outbound interface to send the traffic out, as well as the wrong NAT decision.

You need to check your routing and Ethernet switching configuration, to make sure that traffic is arriving and leaving as expected.

Is the correct policy being selected by the firewall?

Once all the routing/zone lookups were done, the SRX will look for the proper policy to match the traffic. As discussed earlier, the SRX uses an order selection process, so the first policy that matches the traffic will be selected.

If you have an out of order or generic rule configured, your traffic may not match desired policy.

Is the correct NAT being applied by the policy?

Check if the NAT processing is correct, and if the desired output is what you expect. (Is the source translated or not translated as expected?)

Is the destination translated or not translated as expected? Remember that static and destination address translations happen before policy lookup, while source address translations occur after policy lookup, so you need to make sure that you have factored this in when configuring your policy.

Does the debug show that the packet is being processed by Application Services or is destined to a VPN tunnel?

If the packet is being processed by application services, then further debugging may be necessary, for instance, if you have IPS enabled on a policy, and the IPS detects that packet as malicious, okay, it could still be dropped based upon policy.

The same is true for other UTM features, so you need to keep this in mind and check the security events for information.

IPsec VPN Troubleshooting

Let's take a look at how to troubleshoot VPN problems.

First, identify what phase (1 or 2) is not working and why. The `show security ike security-associations` and `show security IPsec security-associations` command can help with that.

If Phase 1 is *UP*, the output should be:

```
Index State Initiator cookie Responder cookie Mode Remote Address
6585   UP  49861d7a78a7b17a  1e0915fc41684516 Main   1.1.1.2
```

If the State is *Down,* this means that IKE Phase 1 is not working. Check the logs. Configure the SRX to record VPN events on a file, by issuing the following:

```
set system syslog file kmd-logs daemon info and set system syslog file kmd-logs match KMD
```

Commit the new configuration.

Use the `show log kmd` command on operational mode to visualize the log file. You can narrow down the results by issuing a filter. Per example you can use `show log kmd | match 1.1.1.1`. Typical error messages are:

```
Jun 24 21:54:06 210-2 kmd [46022]: IKE negotiation failed with error: No proposal chosen. IKE Version: 
1, VPN: ike-vpn-srx1 Gateway: gw-srx1, Local: 1.1.1.1/500, Remote: 1.1.1.2/500, Local IKE-ID: Not-
Available, Remote IKE-ID: Not-Available, VR-ID:
```

In this case, two possible reasons are possible:

- IKE Phase 1 proposal does not match
- GW (initiator or responder) cannot be contacted

Another possible error message:

```
Jun 24 22:18:29 210-2 kmd[45843]: IKE negotiation failed with error: Invalid syntax. IKE Version: 1,
VPN: ike-vpn-srx1 Gateway: gw-srx1, Local: 1.1.1.1/500, Remote: 1.1.1.2/500,
Jun 24 22:45:50 210-2 kmd[42034]: IKE negotiation failed with error: Invalid payload type. IKE Version:
1, VPN: ike-vpn-srx1 Gateway: gw-srx1, Local: 1.1.1.1/500, Remote: 1.1.1.2/500,
```

If the messages here are present in your log, look for the pre-shared key or certificate being exchanged. There's a mismatch among the involved peers.

Another possible error:

```
Jun 24 23:02:08 210-2 kmd [46386]: IKE negotiation failed with error: Timeout. IKE Version: 1, VPN:
ike-vpn-srx1 Gateway: gw-srx1, Local: 1.1.1.1/500, Remote: 1.1.1.2/500,
```

A common error for this message is not having the IKE service enabled in the proper interface or zone. If the Phase 1 is UP, the next logical step is to look after Phase 2.

Check the Phase 2 status, using the `show security IPsec security-associations` command. If the output is ok, then the output should be similar to the one here:

```
Total active tunnels: 1
  ID   Algorithm     SPI     Life:sec/kb  Mon lsys Port  Gateway
  <131073 ESP:3des/sha1 53627df8 3598/ unlim   -   root 500 1.1.1.2
  >131073 ESP:3des/sha1 c4ec1314 3598/ unlim   -   root 500 1.1.1.2
```

You should be seeing the total number of active tunnels, if no tunnel is returned, then you have a problem on Phase 2. You can also use a search filter to look for a specific tunnel, as the example below:

```
show security IPsec security-associations | match 1.1.1.2:
ID           Algorithm  SPI  Life:sec/kb    Mon lsys Port Gateway
131073 ESP:3des/sha1 53627df8 3598/ unlim   -   root 500 1.1.1.2
131073 ESP:3des/sha1 c4ec1314 3598/ unlim   -   root 500 1.1.1.2
```

If nothing is returned, check the logs using `show log kmd`. Some common errors are:

```
Jul 5 15:38:57 kmd[1393]: IKE negotiation failed with error: No proposal chosen. IKE Version: 1, VPN:
vpn1 Gateway: ike-gw, Local: 1.1.1.1/500, Remote: 1.1.1.2/500, Local IKE-ID: 1.1.1.1, Remote IKE-
ID:1.1.1.2, VR-ID: 0
```

If you see this error message, look for the IPsec configuration mismatch between peers:

- Authentication algorithm
- Encryption algorithm
- Lifetime kilobytes
- Lifetime seconds
- Protocol
- Perfect Forward Secrecy

Another common error message:

```
Jul 5 15:55:08 kmd[1393]: KMD_VPN_TS_MISMATCH: Traffic-selector mismatch, vpn name: vpn1, Peer Proposed
traffic-selector local-ip: ipv4(192.168.5.0-192.168.5.255), Peer Proposed traffic-selector remote-ip:
ipv4(192.168.50.0-192.168.50.255)

Jul 5 15:55:08 kmd[1393]: IKE negotiation failed with error: TS unacceptable. IKE Version: 1, VPN:
test_vpn Gateway: ike-gw, Local: 1.1.1.1/500, Remote: 1.1.1.2/500, Local IKE-ID: 1.1.1.1, Remote
IKE-ID: 1.1.1.2, VR-ID: 0
```

If the above message is displayed, then check the Traffic Selector configuration on both gateways.

Lastly, if everything is correct, check the firewall policies. You need to have firewall policies allowing the communication between the networks.

Another important step is to check the routing table using `show route <IP address>`:

```
show route 192.168.50.100
inet.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.50.0/24   *[Static/5] 17:18:18
                      > via st0.2  <----------
```

If there isn't a route, or if the routing points to an incorrect interface, correct it. You can also look at more specific information about this tunnel.

Let's see how this can be done. Start with the `show security IPsec security-associations` command:

```
Total active tunnels: 1
 ID    Algorithm      SPI     Life:sec/kb  Mon lsys Port  Gateway
 <131073 ESP:3des/sha1 a692efdd 3584/ unlim   -   root 500   1.1.1.2
 >131073 ESP:3des/sha1 dd055f4f 3584/ unlim   -   root 500   1.1.1.2
```

You now have an index (marked in bold). With this number, let's look at the specific tunnel `show security IPsec security-associations index value`, where 131073 is the specific tunnel you want to inspect. The output can be seen next:

```
root@vSRX-Lab> show security IPsec security-associations index 131073
  ID: 131073 Virtual-system: root, VPN Name: VPNR-Node2_VPN_Lab
  Local Gateway: 1.1.1.1, Remote Gateway: 1.1.1.2
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Version: IKEv1
    DF-bit: clear
    Bind-interface: st0.2
  Port: 500, Nego#: 54, Fail#: 0, Def-Del#: 0 Flag: 0x600a21
  Last Tunnel Down Reason: Delete payload received
    Direction: inbound, SPI: d5c85ae4, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3578 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2959 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: disabled
    Direction: outbound, SPI: 82f1d936, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3578 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2959 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: enabled
```

Compare this information against your VPN configuration and check for discrepancies.

Traceoptions

Traceoptions is the Junos equivalent of debugging tools from other vendors. It is a very powerful tool and it can be used to debug nearly every function the SRX has. Let's look into how to use traceoptions to analyze packets as they traverse the SRX. This will trace packets as they enter the SRX until they exit, giving you details of the different actions the SRX is taking along the way.

In this example, you are looking for a flow going from a computer in the Trust network with an IP address of (192.168.100.12) towards our server (192.168.150.10).

First, let's enable traceoptions with the flag `basic-datapath`. On the CLI, enter the following command in configuration mode:

```
set security flow traceoptions flag basic-datapath
```

Now, let's define the file output:

```
set security flow traceoptions file flow-troubleshooting
```

Configure a `packet-filter` to match traffic going one way (outbound in this case):

```
set security flow traceoptions packet-filter match-ip source-prefix 192.168.100.12/24and set security flow
traceoptions packet-filter match-ip destination-prefix 192.168.150.10/24
```

Configure a `packet-filter` to match the reverse or response traffic:

```
set security flow traceoptions packet filter match-ip-reverse source-prefix 192.168.150.10/24and set
security flow traceoptions packet filter match-ip-reverse destination-prefix 192.168.100.12/24
```

Now, let's look in the interesting parts of the traceoptions log file.

The packet from source address 192.168.100.12 (source port 52806) captured by the filter, destined to 192.168.150.10 port 80, with the protocol # 6 for TCP:

```
Jan 11 14:44:43 14:44:43.747590:CID-0:RT:<192.168.100.12/52806->192.168.150.10/80;6,0x0> matched
filter match-ip:
```

The IP ID of the packet shows its 6614, which is very useful for comparing packets across multiple capture points (for example, viewing packets on the originating machine, on the firewall, and on the destination to make sure the packet arrives):

```
Jan 11 14:44:43 14:44:43.747590:CID-0:RT:packet [64] ipid = 6614, @0x43e1d09c
```

Packet arrived at interface ge-0/0/0.0:

```
Jan 11 14:44:43 14:44:43.747590:CID-0:RT: flow process pak fast ifl 67 in_ifp ge-0/0/0.0

Jan 11 14:44:43 14:44:43.747590:CID-0:RT:  ge-0/0/0.0:192.168.100.12/52806->192.168.150.10/80, tcp,
flag 2 syn
```

SRX performs a flow lookup:

```
Jan 11 14:44:43 14:44:43.747590:CID-0:RT: find flow: table 0x5e71ea28, hash 13809(0xffff), sa
192.168.100.12, da 192.168.150.10, sp 52806, dp 80, proto 6, tok 9, conn-tag 0x00000000
```

As there is not a session in the session table, the first-path is selected:

```
Jan 11 14:44:43 14:44:43.747590:CID-0:RT:  no session found, start first path. in_tunnel - 0x0, from_cp_
flag - 0
```

The SRX will perform a NAT lookup to find if a static or destination NAT is needed (in this case, it's not):

```
Jan 11 14:44:43 14:44:43.747706:CID-0:RT:  flow_first_in_dst_nat: in <ge-0/0/0.0>, out <N/A> dst_adr
192.168.150.10, sp 52806, dp 80

Jan 11 14:44:43 14:44:43.747706:CID-0:RT:  chose interface ge-0/0/0.0 as incoming nat if.

Jan 11 14:44:43 14:44:43.747706:CID-0:RT:flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to
192.168.150.10(80)
```

Next, the SRX will perform a route lookup to define the egress interface and zone:

```
Jan 11 14:44:43 14:44:43.747706:CID-0:RT:flow_first_routing: vr_id 0, call flow_route_lookup(): src_ip
192.168.100.12, x_dst_ip 192.168.150.10, in ifp ge-0/0/0.0, out ifp N/A sp 52806, dp 80, ip_proto 6,
tos 0
```

```
Jan 11 14:44:43 14:44:43.747706:CID-0:RT:Doing DESTINATION addr route-lookup

Jan 11 14:44:43 14:44:43.747706:CID-0:RT:flow_ipv4_rt_lkup success 192.168.150.10, iifl 0x43, oifl 0x5c
Jan 11 14:44:43 14:44:43.747706:CID-0:RT:  routed (x_dst_ip 192.168.150.10) from Trust (ge-0/0/0.0 in
0) to ge-0/0/1.0, Next-hop: 192.168.150.10
```

Now a policy lookup is performed that determines that the destination zone is Server, and the policy must be from zone Trust to Zone Server:

```
Jan 11 14:44:43 14:44:43.747706:CID-0:RT:flow_first_policy_search: policy search from zone Trust-> zone
Server (0x0,0xce460050,0x50)

Jan 11 14:44:43 14:44:43.747706:CID-0:RT:Policy lkup: vsys 0 zone(9:Trust) -> zone(10:Server) scope:0

Jan 11 14:44:43 14:44:43.747706:CID-0:RT:192.168.100.12/52806 -> 192.168.150.10/80 proto 6
```

Then, the SRX evaluates what is the matching policy and rule action:

```
Jan 11 14:44:43 14:44:43.747823:CID-0:RT:  permitted by policy All_Trust_Server(11)

Jan 11 14:44:43 14:44:43.747823:CID-0:RT:  packet passed, Permitted by policy.
```

The session timeout is set to 1800 seconds, which is based on the standard TCP application timeout of 30 minutes. Also, it sets a current `ageout` of 20 seconds, which is the initial TCP timeout. This means that if the session isn't established within 20 seconds, then the session will be dropped:

```
Jan 11 14:44:43 14:44:43.747823:CID-0:RT:  app 6, timeout 1800s, curr ageout 20s
```

A source NAT lookup is performed and you can verify that a no source NAT is found for this flow:

```
Jan 11 14:44:43 14:44:43.747823:CID-0:RT:flow_first_src_xlate:  nat_src_xlated: False, nat_src_xlate_
failed: False

Jan 11 14:44:43 14:44:43.747823:CID-0:RT:flow_first_src_xlate: src nat returns status: 0, rule/pool id:
0/0, pst_nat: False.
```

The SRX selects the interface ge-0/0/1.0 as outgoing interface:

```
Jan 11 14:44:43 14:44:43.747823:CID-0:RT:  choose interface ge-0/0/1.0(P2P) as outgoing phy if

Jan 11 14:44:43 14:44:43.747823:CID-0:RT:is_loop_pak: No loop: on ifp: ge-0/0/1.0, addr:
192.168.150.10, rtt_idx:0
```

The flow is installed in the respective session tables (client-to-server and server-to-client):

```
Jan 11 14:44:43 14:44:43.747823:CID-0:RT:first pak processing successful

Jan 11 14:44:43 14:44:43.747823:CID-0:RT:  flow_first_install_session======> 0x69d6ea10

Jan 11 14:44:43 14:44:43.747823:CID-0:RT: nsp 0x69d6ea10, nsp2 0x69d6eaa0


Jan 11 14:44:43 14:44:43.747823:CID-0:RT:Installing c2s NP session wing
Jan 11 14:44:43 14:44:43.747823:CID-0:RT:Installing s2c NP session wing

Jan 11 14:44:43 14:44:43.747823:CID-0:RT:first path session installation succeeded
```

This example explains how the SRX performs a first path processing, and creates an entry in the session table if all goes well. By using traceoptions in the security flow stanza, administrators can identify routing errors and other network/configuration problems by looking into the flow itself. It's a powerful feature, indeed.

NOTE When you're done, remember to delete or deactivate your traceptions as leaving it enabled can consume system resources.

You can deactivate traceoptions by issuing the `deactivate security flow traceoptions` command in configuration mode. Remember to commit the change.

Returning the SRX to the Factory Default Configuration

You can use the Reset Config button on the front panel of the SRX to reset the device to its factory default configuration.

The Reset Config button is recessed to prevent it from being pressed accidentally; so you need to insert a small probe (for example, a straightened paper clip) to press the button. Keep the button pressed for 15 seconds to reset the SRX to its default configuration.

WARNING If you use the Reset Config button to reset the device to its factory default configuration, all the configuration files, including the rescue configuration and backup configurations, will be deleted. Please check your specific device configuration for details.

NOTE The Reset Config button is not available in all SRX models.

Another alternative is to use the load factory-default command. To do this:

- Issue the `load factory-default` command in configuration mode
- Use the `set system root-authentication plain-text-password` command to set a new root password for the device
- Commit the configuration

IMPORTANT Prior to committing the changes, if an IP address is not assigned for your management interface, you can be locked out of the device and you will need to use the console or the fxp0 port. Make sure you add the proper interface, routing, and zone configuration before committing in your transit interface used for management.

Day One: SRX Series Up and Running with Advanced Security Services

The SRX Series

Whatever this book has missed in your SRX deployment, you can find on the Juniper's SRX Series landing page. The newest models and security features, links into the doc set, datasheets, specifications, and more: https://www.juniper.net/us/en/products-services/security/srx-series/.

Juniper SRX TechLibrary

Use the in-depth Juniper TechLibrary documentation for configuration samples and instructions on all aspects of the SRX Series at: https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/srx-series/product/index.html.

Day One Library

There are other *Day One* books and posters on security, the SRX, Junos, and other Juniper technology: https://www.juniper.net/dayone.

Junos Genius

Day One books are part of the broad coverage given to network technologies by Junos Genius. Get the app! Get certified! https://www.juniper.net/us/en/training/junos-genius/.

Security

The landing page for all things Juniper Security: https://www.juniper.net/us/en/products-services/security/.