



Juniper Networks ScreenOS 6.2
Evaluated Configuration for Common Criteria, EAL4

Version: 1.0

Date: March 20, 2010

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

THE MATERIAL CONTAINED HEREIN IS CONFIDENTIAL AND PROPRIETARY TO JUNIPER NETWORKS. ALL RIGHTS PERTAINING TO THE SUBJECT MATTER ARE EXPRESSLY RESERVED.

THIS DOCUMENT IS NOT TO BE REPRODUCED WITHOUT THE PRIOR WRITTEN CONSENT OF JUNIPER NETWORKS.

Table of Contents

Introduction	4
Supported Versions	4
Properly Identifying the Juniper Networks Security Appliances for Common Criteria EAL4	4
Upgrading a Juniper Networks Security Appliance for Common Criteria EAL4	5
Placing a Security Appliance in the Evaluated Configuration	8
Enabling FIPS Mode.....	8
Setting Password Length Restrictions	9
Creating the Three Administrator Roles	9
Configuring Certificate-Based Authentication for Remote Administration through SSH	10
Configuring Administrator Account Lockout	11
Configuring Security Alarms and Potential Violation Analysis	11
Configuring Key Protection for Persistent Private Keys	12
Configuring Firewall Policy Review	13
Setting the Date and Time	13
Juniper Networks Security Appliance Models and Interface Naming Convention	14
NAT/Route Mode Firewall	15
Transparent Mode Firewall	18
NAT/Route Mode VPN	23
Transparent Mode VPN	39
Restricting Remote Access.....	48
Logging Permitted Packets.....	50
Logging Dropped Packets.....	50
Configuring Screen Options.....	50
Removing Permissive Default Policy	54
Setting a Policy to Permit Traffic	54
Saving the Applied Configuration	57
Backup and Recovery from the Last-Known-Good Configuration.....	57
Evaluated Configuration Usage Guidance	58
Starting, Stopping, and Reviewing Audit Logs	58
Commands That Are Not Included in the Evaluated Configuration	61

This page was intentionally left blank

Introduction

Common Criteria is an international standard for evaluating IT security devices. ScreenOS 6.2.0 has been evaluated for Common Criteria compliance at Evaluation Assurance Level 4 (EAL4). Full details are available in the Juniper Networks Security Appliances Security Target document.

This document describes the steps necessary to place a security appliance into the same configuration that was used during the Common Criteria evaluation, henceforth referred to as the *evaluated configuration*.

Supported Versions

The evaluated configuration consists of ScreenOS 6.2.0r3 running on any of the following platforms:

- Juniper Networks SSG5 Secure Services Gateway
- Juniper Networks SSG20 Secure Services Gateway
- Juniper Networks SSG140 Secure Services Gateway
- Juniper Networks SSG320M, and SSG350M Secure Services Gateway
- Juniper Networks SSG520M, and SSG550M Secure Services Gateway

or ScreenOS 6.2.0r3a running on any of the following platforms:

- Juniper Networks ISG1000, and ISG2000 Integrated Security Gateway
- Juniper Networks NetScreen-5200, and NetScreen-5400

Properly Identifying the Juniper Networks Security Appliances for Common Criteria EAL4

Before carrying out any steps to secure a Juniper Networks security appliance, you must make sure that the received product has not been tampered with, and ensure that the product received matches the version that is certified as Common Criteria EAL4 compliant.

- To ensure that the product has not been tampered with, verify the following items:
 - ✓ The outside packaging cannot show damage, or evidence that it has been opened. If the cardboard shows damage that would allow the device to be removed or exchanged, this might be evidence of tampering.

- ✓ Each box is packaged with custom tape to indicate that Juniper Networks or an authorized manufacturer packaged the device. The tape is unique; the word “Juniper” is printed repeatedly throughout the tape. If the tape is not present, this might be evidence of tampering.
- ✓ The internal packaging cannot show damage or evidence of tampering. The plastic bag should not have a large hole and the label that seals the plastic bag should not be detached or missing. If the bag or the seal are damaged in any way, this might be evidence of tampering.

These tamper evidence criteria must be met to ensure that the product has not been tampered with during shipment.

- To verify that the product received is the correct version of hardware and software, run the following command from the Command Line Interface (CLI):

```
get system
```

The output of this command includes two key items, hardware version and software version. The Common Criteria evaluated versions are listed in *Juniper Networks Security Appliances Security Target EAL4*. The hardware and software versions must match the Security Target to be in full compliance with the Common Criteria evaluated configuration.

All security appliances are shipped out to the customers with ScreenOS software installed. However, the version of ScreenOS installed on an appliance will vary depending on the date of manufacture.

Upgrading a Juniper Networks Security Appliance for Common Criteria EAL4

If a security appliance does not use the ScreenOS version used in the evaluated configuration, the correct ScreenOS software image needs to be loaded on to the security appliance.

Before the ScreenOS image can be loaded on to the security appliance, you need to configure the management interface through which the image can be downloaded from the FTP server to the security appliance. To configure the zone and the IP address for management interface, enter the following commands:

```
set interface interface-name zone trust  
set interface interface-name ip ip-address
```

where,

interface-name is the name of the actual interface connected to the PC serving as FTP server; through this interface the security appliance can communicate with the FTP server.

Interface ethernet1/1 can be used for the ISG1000 and ISG2000.
Interface ethernet0/0 can be used for SSG140.
Interface ethernet0/0 can be used for SSG320M, and SSG350M.
Interface ethernet0/0 can be used for SSG-520M, and SSG-550M.
Interface ethernet2/1 can be used for NetScreen-5200 and NetScreen-5400.

and,

ip-address is a valid IP address, which can be in the same or different subnet with the TFTP server. However, for the scope of the Common Criteria testing environment, select the IP address in the same subnet with the TFTP server connected to the devices via the interface in the zone **trust**.

Once the manage interface is configured for the security appliance, use the following commands to download the ScreenOS image from the FTP server to the security appliance.

```
save software from tftp tftp-server-ip screenOS-image to flash
```

where,

tftp-server-ip is the IP address for PC serving as TFTP server where the ScreenOS software images reside.

and,

screenOS-image is relative path to the ScreenOS software image file and the name of the file itself.

For example, if the ScreenOS image for the ISG2000 is named “n2000.6.2.0r3a.0” and resides on FTP server (with IP address 10.155.95.253), under the directory /tftpboot/screenOS-image/6.2/, enter the following command:

```
save software from tftp 10.150.39.252 /tftpboot/screenOS-  
image/6.2/ n2000.6.2.0r2.0 to flash
```

The downloading process takes a few minutes. After the downloading process is complete, the security appliance returns to the CLI prompt. Reboot the security appliance. To load the screenOS image completely to the security appliance and restore the default manufacture configurations, from the CLI, issue **reset** command. You will be prompted to answer the following questions:

```
reset  
Configuration modified, save? [y]/n n  
System reset, are you sure? y/[n] y
```

The security appliance will return to the login prompt. At this time, the security appliance has been completely loaded with proper ScreenOS software version.

Placing a Security Appliance in the Evaluated Configuration

The following steps will place a security appliance in the evaluated configuration.

Enabling FIPS Mode

The security appliance must be placed in FIPS mode prior to any other configuration taking place.

WARNING! Switching the security appliance from non-FIPS mode to FIPS mode or vice versa automatically resets the device to the factory default configuration.

Use the “**set fips-mode enable**” command to enable FIPS mode on a security appliance:

```
set fips-mode enable
```

```
WARNING: Changing FIPS mode will set the device configuration back to factory defaults.
```

```
The device will automatically be reset.
```

```
Enable FIPS mode? [y]/n y
```

```
Resetting device to factory default.
```

```
In reset ...
```

Once FIPS mode process has been successfully completed, use the “**get system**” command to validate that FIPS mode is successfully enabled on a security appliance.

Message “**Mode: FIPS**” from the output of “**get system**” command indicates that the security appliance is currently operating in FIPS mode

Enabling FIPS mode successfully (Security Appliance in FIPS mode):

Example:

```
-> get system
```

```
Product Name: NSISG2000
```

```
Serial Number: 0099122004000991, Control Number: 00000000, Mode: FIPS
```

```
Hardware Version: 0110(0)-(12), FPGA checksum: 00000000, VLAN1 IP (0.0.0.0)
```

```
Software Version: 6.2.0r3.0, Type: Firewall+VPN
```

```
Base Mac: 0010.db90.f770
```

```
File Name: i1000.r3, Checksum: 48e3d429
```

For the SSG5, SSG20, SSG140, SSG320M, SSG 350M, SSG520M and SSG550M appliances, the software version used in the evaluated configuration is “6.2.0r3.0”. For the ISG1000, ISG2000, NS-5200 and NS-5400, the software version used in the

evaluated configuration is “6.2.0.r3a.0”.

For more details on the differences in behavior between FIPS mode and standard mode, see the FIPS Security Policy document for that appliance.

Note: The FIPS Security Policy states that the local serial console should be disabled. In the evaluated configuration, the use of the console may be retained while remaining in compliance with FIPS 140-2 requirements, but strictly for the purpose of monitoring alarms. The local console is not to be used for administration of the appliance.

Setting Password Length Restrictions

Security appliance administrators must choose login names and passwords that not only have the length of at least 8 characters, but that also employ as many types of characters as possible. Passwords are case sensitive, so a combination of lower case and upper case letters is required to ensure proper protection. In addition, usernames and passwords should not be easily guessed, such as a mother’s maiden name, a birth date, or names of relatives.

Security appliances ship with a default username and password of “netscreen”. You must change the default username and password as soon as possible to prevent unauthorized access. See *Chapter 1, “Administration,” in Volume 3 in the ScreenOS Concepts & Examples* for more information on administrative passwords. The recommended time between password changes is no longer than 30 days to mitigate the effects of a compromised administrator identity.

To ensure that passwords of eight characters or more are always used, you must first set the administrator password length by issuing the following command:

```
set admin password restrict length <password-length>
```

where, *password-length* is a decimal value equal to or greater than 8 and less than or equal to 31.

Creating the Three Administrator Roles

The root administrator must create three administrative accounts and assign privileges based on these three roles:

- Audit administrator
- Cryptographic administrator
- Security administrator

The `set admin` command allows the root administrator to create a new administrative account and assign the password, privilege level (read-write or read-only) and role to that new user. This is a two-step process in which the account name, password and privilege level for the new account are specified in the first command, and the role in a second command. The following syntax is used:

```
set admin user <name> password <password> privilege {all | read-only}
set admin user <name> role {audit | cryptographic | security}
```

The following example creates a read-write and read-only version for each of the administrative roles:

```
set admin user CryptoAdminRW password CryptoPassRW privilege all
set admin user CryptoAdminRW role crypto
set admin user CryptoAdminRO password CryptoPassRO privilege read-only
set admin user CryptoAdminRO role crypto

set admin user AuditAdminRW password AuditPassRW privilege all
set admin user AuditAdminRW role audit
set admin user AuditAdminRO password AuditPassRO privilege read-only
set admin user AuditAdminRO role audit

set admin user SecAdminRW password SecPassRW privilege all
set admin user SecAdminRW role security
set admin user SecAdminRO password SecPassRO privilege read-only
set admin user SecAdminRO role security
```

After the root administrator has created an account for each of the above roles, the root account should not be used anymore. All operations on the device should be performed from one of the three administrator accounts mentioned above.

ScreenOS supports the concept of a *virtual system*, referred to as a VSYS. Virtual systems and VSYS administrative accounts are not included in the evaluated configuration.

The authentication of administrators via external authentication servers, such as RADIUS, LDAP and TACACS, is not included in the evaluated configuration.

Configuring Certificate-Based Authentication for Remote Administration through SSH

Installing the Host Certificate:

A local certificate must be loaded into the device with a subject name “`ssh-cert-dsa`” along with the related CA certificate and CRL. For instructions on how to obtain a certificate, see “Certificates and CRLs” in *Concepts & Examples ScreenOS Reference Guide: Vol 5, VPNs*.

Once the certificate is loaded on the device, indicate that this certificate is intended to identify the device by executing the following command:

```
set ssh host-identity cert-dsa <cert-id>
```

The SSH client application or other SSH utility is responsible for creating PKA certificate. The certificate can be loaded to the device by any of the existing means.

After the certificate is loaded to the device, a unique number called PKA certificate ID number is assigned by the device's PKI DB module. The ID number can be used to bind the certificate to a specific admin's account with the following commands:

```
set ssh pka-dsa cert-id <cert-id>
```

```
set ssh pka-dsa user-name <login-id> cert-id <cert-id>
```

Configuring Administrator Account Lockout

The security admin should configure the number of failed login attempts with the following command:

```
set admin access attempts <number>
```

After the configured number of failed login attempts from a remote terminal, the connection is closed, and a log message is created to indicate multiple login failures that have occurred.

The security administrator should configure locking time to lock out the account after the number of failed login attempts come to the specified value:

```
set admin access lock-on-failure <number>
```

Configuring Security Alarms and Potential Violation Analysis

The security administrator should enable the security alarms mechanism by issuing the following command:

```
set alarm security enable
```

The audible alarm option should be enabled by issuing the following command:

```
set alarm security audible
```

The security administrator should enable the potential security violation analysis mechanism by issuing the following commands:

```
set alarm security potential-violation
set alarm security potential-violation replay enable
set alarm security potential-violation crypto-failure-self-test enable
set alarm security potential-violation key-gen-failure-self-test enable
set alarm security potential-violation non-crypto-failure-self-test
enable
set alarm security potential-violation encryption-failures <number>
set alarm security potential-violation decryption-failures <number>
set alarm security potential-violation ike-p1-failures <number>
set alarm security potential-violation ike-p2-failures <number>
set alarm security potential-violation policy-violation rate <number>
per [second | minute]]
set alarm security potential-violation policy-violation threshold
<number> duration <number second between 10 - 3600>

set alarm security potential-violation policy-violation source-table-
size <number between 1 - 10240>

set alarm security potential-violation policy-violation destination-
table-size <number between 1 - 10240>

set alarm security potential-violation policy-violation service-table-
size <number between 1 - 10240>

set alarm security potential-violation policy-violation policy-group-
table-size <number between 1 - 10240>
set alarm security potential-violation policy-violation policy-group
<name-string>
set alarm security potential-violation policy-violation policy-group
<name-string> policy-id <id-num>

set alarm security potential-violation authentication-violation enable
```

The security administrator should set the event threshold that is appropriate for the environment. When the threshold is exceeded, a security alarm is generated.

Configuring Key Protection for Persistent Private Keys

The security administrator must enable key protection by issuing the following command:

```
set key protection enable
```

When key protection is enabled:

- Persistent keys are encrypted when not in use.
- Integrity checks are performed whenever a key is copied from one memory location to another.
- When a key is deleted, the memory location it occupied is overwritten with a pseudo-random pattern before being recycled.

Please note that a system reboot is required for key protection to take effect.

Configuring Firewall Policy Review

To allow the security administrator to review the firewall policy rule set prior to activating it, the default status of a firewall policy rule should be set to *disabled* by issuing the following command:

```
set policy default-status-disable
```

The policy rule set can be reviewed by using the **get policy all** command to view all policies, or **get policy disable** command to view only the disabled policies. To enable a policy, enter the following command:

```
unset policy <policy-id> disable
```

Setting the Date and Time

To ensure that the date and time stamps used on audit messages are accurate, enter the following command:

```
set clock mm/dd/yyyy hh:mm
```

Juniper Networks Security Appliance Models and Interface Naming Convention

SSG5, SSG20	SSG140	SSG320M, SSG350M
Trust Zone Connection: Ethernet0/0	Trust Zone Connection: Ethernet0/0	Trust Zone Connection: Ethernet0/0
DMZ Zone Connection: Ethernet0/1	DMZ Zone Connection: Ethernet0/1	DMZ Zone Connection: Ethernet0/1
Untrust Zone Connection: Ethernet0/2	Untrust Zone Connection: Ethernet0/2	Untrust Zone Connection: Ethernet0/2
HA Connection: Ethernet0/4	HA Connection: Ethernet0/3	HA Connection: Ethernet0/3

SSG520M, SSG550M	ISG1000, ISG2000	NetScreen-5200
Trust Zone Connection: Ethernet0/0	Trust Zone Connection: Ethernet1/1	Trust Zone Connection: Ethernet2/1
DMZ Zone Connection: Ethernet0/1	DMZ Zone Connection: Ethernet1/2	DMZ Zone Connection: Ethernet2/2
Untrust Zone Connection: Ethernet0/2	Untrust Zone Connection: Ethernet1/3	Untrust Zone Connection: Ethernet2/3
HA Connection: Ethernet0/3	HA Connection: Ethernet1/4	HA Connection: ha1 and ha2

NetScreen-5400

Trust Zone Connection:

Ethernet2/1 Interface

DMZ Zone Connection:

Ethernet3/2 Interface

Untrust Zone

Connection:

Ethernet2/3 Interface

HA Connection:

ha1 and ha2

Note: The word Ethernet when used to describe the interface can be truncated to **eth** or **e**. For example ethernet1/1 is the same as eth1/1, and the same as e1/1. But it is recommended to use "ethernet" for referencing interface.

All security appliances are, by default, configured in NAT/Route mode without VPN

To ensure that a security appliance is configured in a mode compliant with the Common Criteria EAL4 evaluated configuration, one of the following three sets of steps should be followed depending on the desired configuration:

Note:

ip-address documented in the following commands should be replaced with actual IP address accordingly to the testbed setup/configurations.

NAT/Route Mode Firewall

To configure a security appliance in NAT/route mode firewall, enter the following commands for the appropriate security appliance:

SSG5 and SSG20:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway

set address trust local-LAN local-subnet
```

```
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save
```

SSG140:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save
```

SSG320M and SSG350M

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save
```

SSG520M and SSG550M:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save
```

ISG1000 and ISG2000:

```
unset interface mgt ip
set interface ethernet1/1 zone trust
set interface ethernet1/1 ip ip-address
set interface ethernet1/2 zone dmz
set interface ethernet1/2 ip ip-address
set interface ethernet1/3 zone untrust
set interface ethernet1/3 ip ip-address

set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/3
gateway local-gateway

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save
```

NetScreen-5200:

```
unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet2/2 zone dmz
set interface ethernet2/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address
```

```

set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save

```

NetScreen-5400:

```

unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet3/2 zone dmz
set interface ethernet3/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address

set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save

```

Transparent Mode Firewall

To configure a security appliance in transparent mode firewall, enter the following commands for the appropriate security appliance:

Note: All interfaces must be unbound from L3 zone (trust, untrust or dmz) and bound to L2 zone (v1-trust, v1-untrust or v1-dmz) in order to place the security appliance in transparent mode.

Juniper SSG-5 and SSG-20:

```

unset interface ethernet0/0 ip
unset interface ethernet0/1 ip
unset interface ethernet0/2 ip

unset interface ethernet0/0 zone
unset interface ethernet0/1 zone

```

```
unset interface ethernet0/2 zone

set interface ethernet0/0 zone vl-trust
set interface ethernet0/1 zone vl-untrust

set interface vlan1 ip ip-address

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN service-name permit log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN service-name permit log

save
```

Juniper SSG-140:

```
unset interface ethernet0/0 ip
unset interface ethernet0/1 ip
unset interface ethernet0/2 ip

unset interface ethernet0/0 zone
unset interface ethernet0/1 zone
unset interface ethernet0/2 zone

set interface ethernet0/0 zone vl-trust
set interface ethernet0/1 zone vl-untrust

set interface vlan1 ip ip-address

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN service-name permit log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN service-name permit log

save
```

Juniper SSG-320M and SSG-350M

```
unset interface ethernet0/0 ip
unset interface ethernet0/1 ip
unset interface ethernet0/2 ip

unset interface ethernet0/0 zone
unset interface ethernet0/1 zone
unset interface ethernet0/2 zone

set interface ethernet0/0 zone vl-trust
set interface ethernet0/1 zone vl-untrust
```

```
set interface vlan1 ip ip-address

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from v1-trust to v1-untrust local-LAN
peer-LAN service-name permit log
set policy id id-num top from v1-untrust to v1-trust peer-LAN
local-LAN service-name permit log

save
```

Juniper SSG-520M and SSG-550M:

```
unset interface ethernet0/0 ip
unset interface ethernet0/1 ip
unset interface ethernet0/2 ip

unset interface ethernet0/0 zone
unset interface ethernet0/1 zone
unset interface ethernet0/2 zone

set interface ethernet0/0 zone v1-trust
set interface ethernet0/1 zone v1-untrust

set interface vlan1 ip ip-address

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from v1-trust to v1-untrust local-LAN
peer-LAN service-name permit log
set policy id id-num top from v1-untrust to v1-trust peer-LAN
local-LAN service-name permit log

save
```

Juniper ISG-1000 and ISG-2000:

```
unset interface ethernet1/1 ip
unset interface ethernet1/2 ip
unset interface ethernet1/3 ip

unset interface ethernet1/1 zone
unset interface ethernet1/2 zone
unset interface ethernet1/3 zone

set interface ethernet1/1 zone v1-trust
set interface ethernet1/3 zone v1-untrust

unset interface mgt ip

set interface vlan1 ip ip-address
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from v1-trust to v1-untrust local-LAN
peer-LAN service-name permit log
set policy id id-num top from v1-untrust to v1-trust peer-LAN
local-LAN service-name permit log

save
```

Juniper NS-5200:

```
unset interface ethernet2/1 ip
unset interface ethernet2/2 ip
unset interface ethernet2/3 ip

unset interface ethernet2/1 zone
unset interface ethernet2/2 zone
unset interface ethernet2/3 zone

set interface ethernet2/1 zone v1-trust
set interface ethernet2/3 zone v1-untrust

unset interface mgt ip

set interface vlan1 ip ip-address

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from v1-trust to v1-untrust local-LAN
peer-LAN service-name permit log
set policy id id-num top from v1-untrust to v1-trust peer-LAN
local-LAN service-name permit log

save
```

Juniper NS-5400:

```
unset interface ethernet2/1 ip
unset interface ethernet3/2 ip
unset interface ethernet2/3 ip

unset interface ethernet2/1 zone
unset interface ethernet3/2 zone
unset interface ethernet2/3 zone

set interface ethernet2/1 zone v1-trust
set interface ethernet2/3 zone v1-untrust

unset interface mgt ip

set interface vlan1 ip ip-address
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN service-name permit log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN service-name permit log

save
```

NAT/Route Mode VPN

A security appliance can be configured in NAT/route mode VPN using either a route-based VPN or policy-based VPN. Both route-based VPN and policy-based VPN are supported in NAT/route mode VPN.

Care must be taken in selecting Manual Key values such that they follow the same rules as administrative passwords. The Manual Keys should also be distributed using a secure method to ensure that they are not publicly accessible.

Manual Key Route-Based VPN

To configure the security appliance with a Manual Key route-based VPN in NAT/route mode VPN, enter the following commands for the appropriate security appliance. (Note: The following is a sample configuration of Manual Key route-based VPN.)

SSG5 and SSG20:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet0/2

set vpn vpn-name manual local-spi remote-spi gateway remote-
untrust-interface-ip outgoing-interface ethernet0/2 esp 3des key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind interface tunnel.1

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust local-LAN peer-LAN
service-name permit

save
```

SSG140:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet0/2

set vpn vpn-name manual local-spi remote-spi gateway remote-
untrust-interface-ip outgoing-interface ethernet0/2 esp 3des key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind interface tunnel.1

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust local-LAN peer-LAN
service-name permit

save
```

SSG320M and SSG350M:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet0/2

set vpn vpn-name manual local-spi remote-spi gateway remote-
untrust-interface-ip outgoing-interface ethernet0/2 esp 3des key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind interface tunnel.1

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN  
service-name permit log  
set policy id id-num top from untrust to trust local-LAN peer-LAN  
service-name permit
```

```
save
```

SSG520M and SSG550M:

```
unset interface mgt ip  
set interface ethernet0/0 zone trust  
set interface ethernet0/0 ip ip-address  
set interface ethernet0/1 zone dmz  
set interface ethernet0/1 ip ip-address  
set interface ethernet0/2 zone untrust  
set interface ethernet0/2 ip ip-address  
  
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface ethernet0/2  
  
set vpn vpn-name manual local-spi remote-spi gateway remote-  
untrust-interface-ip outgoing-interface ethernet0/2 esp 3des key  
key-string1 auth sha-1 key key-string2  
set vpn configured-vpn-name bind interface tunnel.1  
  
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2  
gateway local-gateway  
set vrouter trust-vr route local-subnet interface tunnel.1  
  
set address trust local-LAN local-subnet  
set address untrust peer-LAN peer-subnet  
  
set policy id id-num top from trust to untrust local-LAN peer-LAN  
service-name permit log  
set policy id id-num top from untrust to trust local-LAN peer-LAN  
service-name permit log  
  
save
```

ISG1000 and ISG2000:

```
unset interface mgt ip  
set interface ethernet1/1 zone trust  
set interface ethernet1/1 ip ip-address  
set interface ethernet1/2 zone dmz  
set interface ethernet1/2 ip ip-address  
set interface ethernet1/3 zone untrust  
set interface ethernet1/3 ip ip-address  
  
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface ethernet1/3
```

```

set vpn vpn-name manual local-spi remote-spi gateway remote-
untrust-interface-ip outgoing-interface ethernet1/3 esp 3des key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind interface tunnel.1

set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/3
gateway local-gateway
set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust local-LAN peer-LAN
service-name permit log

save

```

NetScreen-5200:

```

unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet2/2 zone dmz
set interface ethernet2/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet2/3

set vpn vpn-name manual local-spi remote-spi gateway remote-
untrust-interface-ip outgoing-interface ethernet2/3 esp 3des key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind interface tunnel.1

set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway
set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust local-LAN peer-LAN
service-name permit log

save

```

NetScreen-5400:

```

unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address

```

```

set interface ethernet3/2 zone dmz
set interface ethernet3/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet2/3

set vpn vpn-name manual local-spi remote-spi gateway remote-
untrust-interface-ip outgoing-interface ethernet2/3 esp 3des key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind interface tunnel.1

set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway
set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust local-LAN peer-LAN
service-name permit log

save

```

Manual Key Policy-Based VPN

To configure the security appliance with a Manual Key policy-based VPN in NAT/Route mode VPN, enter the following commands for the appropriate security appliance: (Note: The following is a sample configuration of Manual Key policy-based VPN.)

SSG5 and SSG20:

```

set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface ethernet0/2 esp aes128 key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind zone untrust-tun

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

save

SSG140:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface ethernet0/2 esp aes128 key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

save

SSG320M and SSG350M:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface ethernet0/2 esp aes128 key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

SSG520M, SSG550M:

```
unset interface mgt ip
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface ethernet0/2 esp aes128 key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

ISG1000 and ISG2000:

```
unset interface mgt ip
set interface ethernet1/1 zone trust
set interface ethernet1/1 ip ip-address
set interface ethernet1/2 zone dmz
set interface ethernet1/2 ip ip-address
set interface ethernet1/3 zone untrust
set interface ethernet1/3 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface ethernet1/3 esp aes128 key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/3
gateway local-gateway
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

NetScreen-5200:

```
unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet2/2 zone dmz
set interface ethernet2/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface ethernet2/3 esp aes128 key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

NetScreen-5400:

```
unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet3/2 zone dmz
set interface ethernet3/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface ethernet2/3 esp aes128 key
key-string1 auth sha-1 key key-string2
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway
```

```
set address trust local-LAN local-subnet
```

```

set address untrust peer-LAN peer-subnet

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log

save

```

AutoKey IKE Route-Based VPN

To configure the security appliance with an AutoKey IKE route-based VPN in NAT/Route mode VPN, enter the following commands for the appropriate security appliance: (Note: The following is a sample configuration of AutoKey IKE route-based VPN.)

SSG5 and SSG20:

```

set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet0/2

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
set vrouter trust-vr route peer-subnet interface tunnel.1

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save

```

SSG140:

```

set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz

```

```

set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet0/2

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
set vrouter trust-vr route peer-subnet interface tunnel.1

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save

```

SSG320M and SSG350M:

```

set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet0/2

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
set vrouter trust-vr route peer-subnet interface tunnel.1

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

```

save

SSG520M, SSG550M:

```
unset interface mgt ip
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet0/2

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
set vrouter trust-vr route peer-subnet interface tunnel.1

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save
```

ISG1000 and ISG2000:

```
unset interface mgt ip
set interface ethernet1/1 zone trust
set interface ethernet1/1 ip ip-address
set interface ethernet1/2 zone dmz
set interface ethernet1/2 ip ip-address
set interface ethernet1/3 zone untrust
set interface ethernet1/3 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet1/3

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet1/3 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name
```

```

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/3
gateway local-gateway
set vrouter trust-vr route peer-subnet interface tunnel.1

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save

```

NetScreen-5200:

```

unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet2/2 zone dmz
set interface ethernet2/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet2/3

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet2/3 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway
set vrouter trust-vr route peer-subnet interface tunnel.1

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save

```

NetScreen-5400:

```

unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet3/2 zone dmz
set interface ethernet3/2 ip ip-address
set interface ethernet2/3 zone untrust

```

```

set interface ethernet2/3 ip ip-address

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet2/3

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet2/3 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway
set vrouter trust-vr route peer-subnet interface tunnel.1

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name permit log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name permit log

save

```

AutoKey IKE Policy-Based VPN

To configure the security appliance with an AutoKey IKE policy-based VPN in NAT/Route mode VPN, enter the following commands for the appropriate security appliance: (Note: The following is a sample configuration of AutoKey IKE policy-based VPN.)

SSG5 and SSG20:

```

set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway

```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

SSG140:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip-address
```

```
set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

SSG320M and SSG350M:

```
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address
```

```
set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log

save
```

SSG520M, SSG550M:

```
unset interface mgt ip
set interface ethernet0/0 zone trust
set interface ethernet0/0 ip ip-address
set interface ethernet0/1 zone dmz
set interface ethernet0/1 ip ip-address
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip ip-address

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet0/2 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2
gateway local-gateway

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log

save
```

ISG1000 and ISG2000:

```
unset interface mgt ip
set interface ethernet1/1 zone trust
set interface ethernet1/1 ip ip-address
set interface ethernet1/2 zone dmz
set interface ethernet1/2 ip ip-address
set interface ethernet1/3 zone untrust
set interface ethernet1/3 ip ip-address

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet1/3 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/3
gateway local-gateway
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

NetScreen-5200:

```
unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet2/2 zone dmz
set interface ethernet2/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address
```

```
set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet2/3 preshare preshare-key
proposal phase1-proposal
set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name
```

```
set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet
```

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway
```

```
set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log
```

```
save
```

NetScreen-5400:

```
unset interface mgt ip
set interface ethernet2/1 zone trust
set interface ethernet2/1 ip ip-address
set interface ethernet3/2 zone dmz
set interface ethernet3/2 ip ip-address
set interface ethernet2/3 zone untrust
set interface ethernet2/3 ip ip-address
```

```
set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-interface ethernet2/3 preshare preshare-key
proposal phase1-proposal
```

```

set vpn vpn-name gateway configured-ike-gateway-name proposal
phase2-proposal-name

set address trust local-LAN local-subnet
set address untrust peer-LAN peer-subnet

set vrouter trust-vr route 0.0.0.0/0 interface ethernet2/3
gateway local-gateway

set policy id id-num top from trust to untrust local-LAN peer-LAN
service-name tunnel vpn configured-vpn-name log
set policy id id-num top from untrust to trust peer-LAN local-LAN
service-name tunnel vpn configured-vpn-name log

save

```

Transparent Mode VPN

In Transparent mode, only policy-based VPNs are supported. To configure a security appliance with a Policy-based VPN in Transparent Mode, enter the commands below for the appropriate security appliance. After the commands have been entered, save the configuration using the **save** command and then the device **reset** command.

Manual Key Policy-Based VPN

To configure the security appliance with an Manual Key policy-based VPN in Transparent mode, enter the following commands for the appropriate security appliance: (Note: The following is a sample configuration of Manual Key policy-based VPN in Transparent mode.)

SSG5 and SSG20:

```

unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
unset interface ethernet0/2 zone

set interface ethernet0/0 zone v1-trust
set interface ethernet0/1 zone v1-dmz
set interface ethernet0/2 zone v1-untrust

set interface vlan1 ip ip-address

set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet

```

```
set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone vl-untrust esp aes256 key
key-string1 auth sha-1 key key-string2
```

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway
```

```
set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN any tunnel vpn configured-vpn-name log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN any tunnel vpn configured-vpn-name log
```

```
save
reset
```

SSG140:

```
unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
unset interface ethernet0/2 zone
```

```
set interface ethernet0/0 zone vl-trust
set interface ethernet0/1 zone vl-dmz
set interface ethernet0/2 zone vl-untrust
```

```
set interface vlan1 ip ip-address
```

```
set address vl-trust local-LAN local-subnet
set address vl-untrust peer-LAN peer-subnet
```

```
set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone vl-untrust esp aes256 key
key-string1 auth sha-1 key key-string2
```

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway
```

```
set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN any tunnel vpn configured-vpn-name log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN any tunnel vpn configured-vpn-name log
```

```
save
reset
```

SSG320M and SSG350M:

```
unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
```

```

unset interface ethernet0/2 zone

set interface ethernet0/0 zone vl-trust
set interface ethernet0/1 zone vl-dmz
set interface ethernet0/2 zone vl-untrust

set interface vlan1 ip ip-address

set address vl-trust local-LAN local-subnet
set address vl-untrust peer-LAN peer-subnet

set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone vl-untrust esp aes256 key
key-string1 auth sha-1 key key-string2

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN any tunnel vpn configured-vpn-name log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN any tunnel vpn configured-vpn-name log

save
reset

```

SSG520M, and SSG550M:

```

unset interface mgt ip

unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
unset interface ethernet0/2 zone

set interface ethernet0/0 zone vl-trust
set interface ethernet0/1 zone vl-dmz
set interface ethernet0/2 zone vl-untrust

set interface vlan1 ip ip-address

set address vl-trust local-LAN local-subnet
set address vl-untrust peer-LAN peer-subnet

set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone vl-untrust esp aes256 key
key-string1 auth sha-1 key key-string2

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN any tunnel vpn configured-vpn-name log

```

```
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN any tunnel vpn configured-vpn-name log

save
reset
```

ISG1000 and ISG2000:

```
unset interface mgt ip

unset interface ethernet1/1 ip
unset interface ethernet1/1 zone
unset interface ethernet1/2 ip
unset interface ethernet1/2 zone
unset interface ethernet1/3 ip
unset interface ethernet1/3 zone

set interface ethernet1/1 zone vl-trust
set interface ethernet1/2 zone vl-dmz
set interface ethernet1/3 zone vl-untrust

set interface vlan1 ip ip-address

set address vl-trust local-LAN local-subnet
set address vl-untrust peer-LAN peer-subnet

set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone vl-untrust esp aes256 key
key-string1 auth sha-1 key key-string2

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN any tunnel vpn configured-vpn-name log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN any tunnel vpn configured-vpn-name log

save
reset
```

NetScreen-5200:

```
unset interface mgt ip

unset interface ethernet2/1 ip
unset interface ethernet2/1 zone
unset interface ethernet2/2 ip
unset interface ethernet2/2 zone
unset interface ethernet2/3 ip
unset interface ethernet2/3 zone

set interface ethernet2/1 zone vl-trust
set interface ethernet2/2 zone vl-dmz
```

```

set interface ethernet2/3 zone vl-untrust

set interface vlan1 ip ip-address

set address vl-trust local-LAN local-subnet
set address vl-untrust peer-LAN peer-subnet

set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone vl-untrust esp aes256 key
key-string1 auth sha-1 key key-string2

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN any tunnel vpn configured-vpn-name log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN any tunnel vpn configured-vpn-name log

save
reset

```

NetScreen-5400:

```

unset interface mgt ip

unset interface ethernet2/1 ip
unset interface ethernet2/1 zone
unset interface ethernet3/2 ip
unset interface ethernet3/2 zone
unset interface ethernet2/3 ip
unset interface ethernet2/3 zone

set interface ethernet2/1 zone vl-trust
set interface ethernet3/2 zone vl-dmz
set interface ethernet2/3 zone vl-untrust

set interface vlan1 ip ip-address

set address vl-trust local-LAN local-subnet
set address vl-untrust peer-LAN peer-subnet

set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone vl-untrust esp aes256 key
key-string1 auth sha-1 key key-string2

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from vl-trust to vl-untrust local-LAN
peer-LAN any tunnel vpn configured-vpn-name log
set policy id id-num top from vl-untrust to vl-trust peer-LAN
local-LAN any tunnel vpn configured-vpn-name log

save
reset

```

AutoKey IKE Policy-Based VPN

To configure the security appliance with an Auto-Key IKE policy-based VPN in Transparent mode, enter the following commands for the appropriate security appliance: (Note: The following is a sample configuration of Auto-Key policy-based VPN in Transparent mode.)

SSG5 and SSG20:

```
unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
unset interface ethernet0/2 zone

set interface ethernet0/0 zone v1-trust
set interface ethernet0/1 zone v1-dmz
set interface ethernet0/2 zone v1-untrust

set interface vlan1 ip ip-address

set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet

set ike gateway ike-gateway-name address peer-outbound-interface-ip main outgoing-zone v1-untrust preshare preshare-key proposal phase1-proposal-name
set vpn vpn-name gateway configured-ike-gateway proposal phase2-proposal-name

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway local-gateway

set policy id id-num top from v1-trust to v1-untrust local-subnet peer-subnet service-name tunnel vpn configured vpn-name log
set policy id id-num top from v1-trust to v1-untrust local-subnet peer-subnet service-name tunnel vpn configured vpn-name log

save
reset
```

SSG140:

```
unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
unset interface ethernet0/2 zone
```

```

set interface ethernet0/0 zone v1-trust
set interface ethernet0/1 zone v1-dmz
set interface ethernet0/2 zone v1-untrust

set interface vlan1 ip ip-address

set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-zone v1-untrust preshare preshare-key proposal
phase1-proposal-name
set vpn vpn-name gateway configured-ike-gateway proposal phase2-
proposal-name

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log

save
reset

```

SSG320M and SSG350M:

```

unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
unset interface ethernet0/2 zone

set interface ethernet0/0 zone v1-trust
set interface ethernet0/1 zone v1-dmz
set interface ethernet0/2 zone v1-untrust

set interface vlan1 ip ip-address

set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-zone v1-untrust preshare preshare-key proposal
phase1-proposal-name
set vpn vpn-name gateway configured-ike-gateway proposal phase2-
proposal-name

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log

```

```
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log

save
reset
```

SSG520M, SSG550M:

```
unset interface mgt ip

unset interface ethernet0/0 ip
unset interface ethernet0/0 zone
unset interface ethernet0/1 ip
unset interface ethernet0/1 zone
unset interface ethernet0/2 ip
unset interface ethernet0/2 zone

set interface ethernet0/0 zone v1-trust
set interface ethernet0/1 zone v1-dmz
set interface ethernet0/2 zone v1-untrust

set interface vlan1 ip ip-address

set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-zone v1-untrust preshare preshare-key proposal
phase1-proposal-name
set vpn vpn-name gateway configured-ike-gateway proposal phase2-
proposal-name

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log

save
reset
```

ISG1000 and ISG2000:

```
unset interface mgt ip

unset interface ethernet1/1 ip
unset interface ethernet1/1 zone
unset interface ethernet1/2 ip
unset interface ethernet1/2 zone
unset interface ethernet1/3 ip
unset interface ethernet1/3 zone
```

```

set interface ethernet1/1 zone v1-trust
set interface ethernet1/2 zone v1-dmz
set interface ethernet1/3 zone v1-untrust

set interface vlan1 ip ip-address

set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-zone v1-untrust preshare preshare-key proposal
phase1-proposal-name
set vpn vpn-name gateway configured-ike-gateway proposal phase2-
proposal-name

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log

save
reset

```

NetScreen-5200:

```

unset interface mgt ip

unset interface ethernet2/1 ip
unset interface ethernet2/1 zone
unset interface ethernet2/2 ip
unset interface ethernet2/2 zone
unset interface ethernet2/3 ip
unset interface ethernet2/3 zone

set interface ethernet2/1 zone v1-trust
set interface ethernet2/2 zone v1-dmz
set interface ethernet2/3 zone v1-untrust

set interface vlan1 ip ip-address

set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet

set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-zone v1-untrust preshare preshare-key proposal
phase1-proposal-name
set vpn vpn-name gateway configured-ike-gateway proposal phase2-
proposal-name

set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway

```

```
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log
```

```
save
reset
```

NetScreen-5400:

```
unset interface mgt ip
```

```
unset interface ethernet2/1 ip
unset interface ethernet2/1 zone
unset interface ethernet3/2 ip
unset interface ethernet3/2 zone
unset interface ethernet2/3 ip
unset interface ethernet2/3 zone
```

```
set interface ethernet2/1 zone v1-trust
set interface ethernet3/2 zone v1-dmz
set interface ethernet2/3 zone v1-untrust
```

```
set interface vlan1 ip ip-address
```

```
set address v1-trust local-LAN local-subnet
set address v1-untrust peer-LAN peer-subnet
set ike gateway ike-gateway-name address peer-outbound-interface-
ip main outgoing-zone v1-untrust preshare preshare-key proposal
phase1-proposal-name
set vpn vpn-name gateway configured-ike-gateway proposal phase2-
proposal-name
```

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway
local-gateway
```

```
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log
set policy id id-num top from v1-trust to v1-untrust local-subnet
peer-subnet service-name tunnel vpn configured vpn-name log
```

```
save
reset
```

Restricting Remote Access

Management access to management interface must be limited to the locally connected console port and SSH connection. Security appliances are not shipped in this mode by default.

To limit management access to the management port, the interface that is by default in the **V1-Trust** or **Trust** security zone needs to have management access disabled. See the interface commands in the *Juniper Networks ScreenOS CLI Reference Guide* for more information.

By default, management access is disabled on all other interfaces. No action is required to turn off the management access.

To disable management to the interface in the **Trust** or **V1-Trust** security zone, issue the following CLI command:

```
unset interface interface-name manage
```

To enable SSH connection to management interface in **Trust** or **V1-Trust** security zone, issue the following CLI command:

```
set interface interface-name manage ssh
```

For each security appliance, you must enter the following commands:

SSG5 and SSG20:	<pre>unset interface ethernet0/0 manage set interface ethernet0/0 manage ssh</pre>
SSG140:	<pre>unset interface ethernet0/0 manage set interface ethernet0/0 manage ssh</pre>
SSG320M and SSG-350M:	<pre>unset interface ethernet0/0 manage set interface ethernet0/0 manage ssh</pre>
SSG520M and SSG550M:	<pre>unset interface ethernet0/0 manage set interface ethernet0/0 manage ssh</pre>
ISG1000 and ISG2000:	<pre>unset interface ethernet1/1 manage set interface ethernet1/1 manage ssh</pre>
NetScreen-5200:	<pre>unset interface ethernet2/1 manage set interface ethernet2/1 manage ssh</pre>
NetScreen-5400:	<pre>unset interface ethernet2/1 manage set interface ethernet2/1 manage ssh</pre>

When operating in Transparent mode (including Transparent mode VPN and Transparent mode firewall), management to the interface in vlan zone should also be disabled.

The following command is applied for all models (including Juniper Networks SSG5, SSG20, SSG140, SSG320M, SSG350M, SSG520M, SSG550M, ISG1000, ISG2000, NetScreen-5200, and NetScreen-5400):

```
unset interface vlan1 manage  
set interface vlan1 manage ssh
```

Logging Permitted Packets

- To log permitted packets passing through the device enable logging option on all VPN policies and/or firewall traffic policies.
- In this document all permitted policies include the keyword **log**, to create traffic log entries for permitted traffic.
- Permitted traffic logs are created upon completion of the application session.
- You can use the following command to view the overall traffic logs, or specific policy's traffic log:

```
get log traffic
get log traffic policy id
```

Logging Dropped Packets

- To log dropped packets sent to terminate on any of the device interfaces, you must enable the following command:

```
set firewall log-self
```

- To log dropped packets that have been authenticated, you must add the **log** keyword to the first policy associated with a VPN tunnel. Packets that do not match any of the policies associated with the tunnel are dropped. The log entries for these dropped packets are linked with the highest priority policy (first in the 'get policy all' list) associated with the tunnel and the traffic flow direction.

Configuring Screen Options

Security appliances must be configured to prevent all types of Denial of Service (DoS) and attack signatures on every security zone to prevent these types of attacks from occurring on the network. See *Chapter 2, "Zones," in Volume 2 in the ScreenOS Concepts & Examples manual* for more information on configuring the Screen functions and for descriptions of the attacks that the Screen functions are designed to prevent.

To view the default screening options for a particular security zone, issue the following command.

```
get zone zone-name screen
```

By default, the screening options that are enabled for the **Untrust/V1-Untrust** security zone (and the interfaces in **Untrust/V1-Untrust** zone) in ScreenOS 6.2.0 are listed below:

Tear-drop Attack Protection	on
SYN Flood Protection (200)	on
Alarm Threshold:	<i>alarm-threshold</i>
Queue Size:	<i>Q-size</i>
Timeout Value:	20
Source Threshold:	<i>src-threshold</i>
Destination Threshold:	<i>dst-threshold</i>
Drop unknown MAC (transparent mode only):	off
Ping-of-Death Protection	on
Source Route IP Option Filter	on
Land Attack Protection	on

where,

alarm-threshold, ***Q-size***, ***src-threshold***, and ***dst-threshold*** are platform dependent as specified in the table below.

Platforms Platform Screening Values	SSG5, SSG20	SSG140	SSG320M, SSG350M
<i>alarm-threshold</i>	512	1024	1024
<i>Q-size</i>	512	10240	10240
<i>src-threshold</i>	512	1024	4000
<i>dst-threshold</i>	512	2148	40000

Platforms Platform Screening Values	SSG520M, SSG550M	ISG1000, ISG2000	NetScreen-5200
<i>alarm-threshold</i>	1024	1024	1024
<i>Q-size</i>	10240	10240	10240
<i>src-threshold</i>	4000	4000	4000
<i>dst-threshold</i>	40000	40000	40000

Platforms	NetScreen-5400
Platform Screening Values	
<i>alarm-threshold</i>	1024
<i>Q-size</i>	10240
<i>src-threshold</i>	4000
<i>dst-threshold</i>	40000

For the **Trust/V1-Trust** and **DMZ/V1-DMZ** zones (and the interfaces in **Trust** and **DMZ** zone), no screen options are enabled by default.

To disable all the default screening option for zone **Untrust/V1-Untrust**, the following commands can be used:

```
unset zone [untrust | v1-untrust] screen tear-drop
unset zone [untrust | v1-untrust] screen syn-flood
unset zone [untrust | v1-untrust] screen ping-death
unset zone [untrust | v1-untrust] screen ip-filter-src
unset zone [untrust | v1-untrust] screen land
save
```

The security zone displays the following message when no screening options are enabled:

```
Screen function only generate alarm without dropping packet: OFF.
```

The following CLI command enables all screens on a per-zone basis (and is applied to all interfaces within that zone):

```
set zone zone-name screen block-frag
set zone zone-name screen component-block
set zone zone-name screen fin-no-ack
set zone zone-name screen icmp-flood
set zone zone-name screen icmp-fragment
set zone zone-name screen icmp-large
set zone zone-name screen ip-bad-option
set zone zone-name screen ip-filter-src
set zone zone-name screen ip-loose-src-route
set zone zone-name screen ip-record-route
set zone zone-name screen ip-security-opt
set zone zone-name screen ip-spoofing
set zone zone-name screen ip-stream-opt
set zone zone-name screen ip-strict-src-route
set zone zone-name screen ip-sweep
set zone zone-name screen ip-timestamp-opt
set zone zone-name screen land
```

```
set zone zone-name screen limit-session
set zone zone-name screen mal-url code-red
set zone zone-name screen ping-death
set zone zone-name screen port-scan
set zone zone-name screen syn-ack-ack-proxy
set zone zone-name screen syn-fin
set zone zone-name screen syn-flood
set zone zone-name screen syn-frag
set zone zone-name screen tcp-no-flag
set zone zone-name screen tear-drop
set zone zone-name screen udp-flood
set zone zone-name screen unknown-protocol
set zone zone-name screen winnuke
save
```

For the purposes of Common Criteria EAL4, you must run the above commands for both the internal and external zones (i.e. Trust and Untrust) to protect the internal and external networks.

When the security appliance is in NAT/Route mode, run the above commands for security zones **Trust** and **Untrust**.

When the security appliance is in Transparent mode (including Transparent mode VPN and Transparent mode firewall), run the above commands for security zones **V1-Trust** and **V1-Untrust**.

You must run the same commands (as above) for each additional security zone that is configured and used.

When the security appliance operates in NAT/route mode (including NAT/route firewall and Nat/route mode VPN), you must also enable dropping packets that have no source IP address, or that have a non-routable source IP address by using the following command.

```
set zone zone-name screen ip-spoofing drop-no-rpf-route
```

where,

zone-name is the name of the security zone such as **Trust** or **Untrust**.

See the zone commands in the *Juniper Networks ScreenOS CLI Reference Guide*, for more information.

For instance, when the security is in NAT/route mode, to turn on dropping packets capability for the security zone **trust** and **untrust**, issue the following commands.

```
set zone trust screen ip-spoofing drop-no-rpf-route
set zone untrust screen ip-spoofing drop-no-rpf-route
```

Ensure to execute the same command (as above) for any Layer-3 or Layer-2 security zones that are configured and used.

When security appliance operates in VPN mode (including NAT/Route mode VPN or Transparent mode VPN), explicit configuration must be enabled in order to provide screening protection per zone basis.

For instance, when security appliance operates in NAT/route mode VPN, to turn on screening protection on zone **Trust**, configure the following command:

```
set zone trust screen on-tunnel
```

When changing the HTTP blocking option the changes will only apply to the sessions newly created after this blocking option is set.

Removing Permissive Default Policy

The SSG5 and SSG20 have a default policy that allows traffic to traverse the device from the interface in the **Trust** zone to the interface in the **Untrust** zone. This policy is not defined by default for all other security appliances. You must delete this default policy to avoid inadvertently allowing information to traverse the device. See the policy commands in the *Juniper Networks ScreenOS CLI Reference Guide, Version* for more information on how to set and unset policies.

To disable this default policy on the SSG5 and SSG20 use the following CLI command:

```
unset policy id 1
```

Setting a Policy to Permit Traffic

By default, security appliance will drop any traffic that does not match any permit policy. However, only traffic that matches a policy will actually be logged. Therefore, the administrator must add a policy to the end of the policy list to log denied traffic which matches no policy. The policy command is as follows:

```
set policy id pol-id from scr-zone to dst-zone any any any deny log
```

where,

pol-id is the policy ID

scr-zone and *dst-zone* are, respectively, source zone from which the traffic comes and destination zone to which the traffic arrives. *scr-zone* and *dst-zone* can be

predefined in Layer 3 (L3) security zone (**Trust/Untrust/DMZ**), Layer 2 (L2) security zone (**V1-Trust, V1-Untrust, V1-DMZ**), or user-defined security zone.

Because policies are defined by source and destination zone, this command must be entered for each set of zones that are being used on the device. If the device is configured in the default (Layer 3 NAT/route) mode, execute the following commands:

```
set policy id pol-id from trust to untrust any any any deny log
set policy id pol-id from untrust to trust any any any deny log

set policy id pol-id from trust to dmz any any any deny log
set policy id pol-id from dmz to trust any any any deny log

set policy id pol-id from untrust to dmz any any any deny log
set policy id pol-id from dmz to untrust any any any deny log
```

If the device is not configured in Layer 3 NAT/route mode (as indicated above by the zones shown), but rather in Layer 2 Transparent mode, then the above commands will be replaced by commands using the **V1-Trust, V1-Untrust, and V1-DMZ** zones.

For every additional security zone used on the device that has a network interface assigned to it, the above policies should be added to the end of the policy tables to ensure that dropped traffic is logged.

There are two important steps to take every time a policy is being created. First, all security policies that are created must have counting and logging enabled to ensure that all audit log information is maintained for traffic passing through the device. Second, policies must be as specific as possible to ensure that the traffic being permitted is done intentionally, and not as part of a generic policy.

When creating a policy, always use specific source IP (source address), destination IP (destination address), source zone, destination zone, protocol, and service when feasible. One example where it might not make sense to be specific is for traffic destined for an external network for general web access.

The source and destination addresses must be created before a policy can be created. To create a host or network address in a security zone, use the following command:

```
set address security-zone addr-name ip-address/netmask
```

where,

addr-name is the string presenting the name for the host or network address

netmask is a decimal number in the range [1, 32]; for a host address the netmask is 32; for a network address the netmask can be any in the range [1, 31]

The example below shows the configurations for valid host and network addresses (which can be later used as *scr-addr* or *dst-addr*)

```
set address trust trust-HostA 10.155.95.100/32
set address untrust untr-NetworkB 192.168.1.0/24
```

After configuring the source and destination addresses, configure the policy with counting and logging options enabled using the following command:

```
set policy id id-num from src-zone to dst-zone src-addr dst-addr
service-name action log
```

where,

id-num is the decimal number presenting the policy ID number

src-zone is source zone from which the traffic is initiated

dst-zone is destination zone to which the traffic is forwarded

src-addr is the source address which can be a host or network address in the source zone

dst-addr is the destination address which can be a host or network address in the destination zone

service-name is the name(s) of the service (example: FTP, Telnet, Ping, etc)

action can be **permit** to allow specific service to pass from source address across the security appliance to the destination address; or **deny** to block service from passing though the security appliance

The following is an example of configuring a valid policy:

```
set policy id 5 from trust to untrust trust-HostA untr-NetworkB ftp
permit log
```

where,

trust-HostA and *untr-NetworkB* are, respectively, host and network addresses that have been previously configured.

The above policy allows only FTP traffic from a host *trust-HostA* in security zone **Trust** to a network *untr-NetworkB* in security zone **Untrust**, with the **Trust** as the source zone and the **Untrust** zone as the destination zone, and enables logging and counting.

The order of policies is important, as policies are searched in order beginning with the first one in the policy list and moving through the list. The first matching policy is applied to network traffic to determine the action taken.

By default, a newly created policy appears at the bottom of a policy list.

There is an option that allows you to position a policy at the top of the list instead. In the CLI, add the key word **top** to the **set policy** command:

For example,

```
set policy id 6 top from trust to untrust trust-HostA untr-NetworkB
http permit log
```

The newly created policy can also be positioned at any location in the policy list by using the keyword option **before** to the **set policy** CLI command.

For example:

```
set policy id 4 before 98 from untrust to trust untr-NetworkB trust-
HostA ftp permit log
```

If global policies are used then the above policy must be replaced as it will be executed prior to any global policy. A Global deny policy can be used which must be added at the end of the Global policy list

```
set policy global id pol-id any any any deny log
```

For more information, see *“Reordering Policies” in Chapter 7, “Policies,” in Volume 2 of the Juniper Networks Concepts & Examples ScreenOS Reference Guide..*

Saving the Applied Configuration

The configuration should be saved to ensure that the device will remain in this configuration if it is rebooted or reset. Enter the **save** command.

Backup and Recovery from the Last-Known-Good Configuration

In the event that a security appliance is not configured correctly and reaches an inoperable or insecure state, execute the following command directly after saving the configuration to create a recovery point, referred to as the last-known-good configuration.

```
save config to last-known-good
```

To recover from the last-known-good configuration, execute the following command:

```
exec config rollback
```

Evaluated Configuration Usage Guidance

When the security appliance is operating in Layer 2 mode (i.e. Transparent mode VPN and Transparent mode firewall), it allows ARP packets to pass through without checking the policy. This behavior is required to operate in the network in Transparent mode. However ARP attacks are countered, by ensuring that all non-arp traffic is encrypted. The behavior is different when the device is set up in Layer 3 mode (i.e. NAT/route Mode VPN or NAT/route mode firewall). In Layer 3 mode, ARP packets are not passed through the device, but the packets receive responses if they are destined for an internal IP address.

All traffic from an internal network to an external network must flow through the security appliance. Setting up network connections that do not cross the security appliance is not a secure setup and leaves the network susceptible to intrusion attacks.

It is expected and assumed that authorized administrators are not hostile, yet are capable of error.

The security appliance must be placed in a physically secure location to prevent physical tampering, or device startup or shutdown. All persons who have physical access to this location, including access to the console, must have the same level of trustworthiness as an administrator.

The security appliances do not possess any general purpose computing or storage repository capabilities and do not host any public data.

The use of global policies are not supported in policy-based VPN.

Starting, Stopping, and Reviewing Audit Logs

The security appliance automatically logs the starting and stopping of audit logs. Each time the device boots up, message logging automatically begins (see the Traffic Log messages section in the Messages Log). Upon initial boot-up, the message “**system is operational**” indicates that all message logging has started. The command **get log setting** shows the current state of the logging settings.

To enable or disable any of the eight message logging states, the administrator must issue one of the following commands:

```
set log module system level level-name destination syslog
unset log module system level level-name destination syslog
```

where, *level-name* is one of the following:

- emergency**
- alert**
- critical**
- error**
- warning**
- notification**
- information**
- debugging**

The event log shows the following events:

```
Log setting is modified to {enable | disable} level-name level by admin
name-str
```

where,

- level-name* is the same as the *level-name* in the issued command (as specified above)
- name-str* is the user account making the change (i.e. the person making the change).

The security appliance logs an event each time an audit log is reviewed. The event log shows the following events:

```
Alarm log was reviewed by admin name-str
Traffic log was reviewed by admin name-str
Asset recovery log was reviewed by admin name-str
Self log was reviewed by admin name-str
Event log was reviewed by admin name-str
```

where,

- name-str* is the user account making the change (i.e. the person making the change).

The remaining portion of this page was intentionally left blank

Commands That Are Not Included in the Evaluated Configuration

The following commands are not included in the evaluated configuration. When a command is specified without listing any parameters, the entire command is excluded from the evaluated configuration. When a command is listed with parameters, only those parameters listed are excluded.

Command	Parameter
<ul style="list-style-type: none"> • admin 	<ul style="list-style-type: none"> • auth server • auth fallback permit • auth primary • auth read-only • auth root • port • privilege • telnet
<ul style="list-style-type: none"> • alg 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • alias 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • all 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • antispan 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • asic 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • Attack 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • attack-db 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • audible-alarm 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • Auth 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • auth-server 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • av 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • Bgp 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • bgroup 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • Bulk-cli 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • chassis 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • core-dump 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • cpu-limit 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • cpu-protection 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • dbuf 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • deny-message 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • di 	<ul style="list-style-type: none"> •
<ul style="list-style-type: none"> • dot1x 	<ul style="list-style-type: none"> •

• event	• cluster
• failover	•
• file	•
• flow	• allow-dns-reply • gre-in-tcp-mss • gre-out-tcp-mss • hub-n-spoke-mip • mac-flooding • no-tcp-seq-check
• gtp	•
• icap	•
• igmp	•
• infranet	•
• interface	• manage • ident-reset • snmp • ssl •
• ip	•
• ippool	•
• l2tp	•
• lcd	•
• matchgroup	•
• management-vrouter	•
• modem	•
• multicast-group-policy	•
• nrtp	•
• nsmgmt	•
• nsgp	•
• nsrp	•
• ospf	•
• override	•
• pattern-update	•
• pbr	•
• pim	•
• ppp	•
• pppoa	•
• pppoe	•
• proxy-id	•
• rip	•
• save	• all-virtual-system

	<ul style="list-style-type: none"> • From/to [usb slot1 tftp]
• shdsl	•
• sm-ctx	•
• sm-ksh	•
• snmp	•
• ssid	•
• ssl	•
• switch	•
• syslog	•
• telnet	•
• timer	•
• traffic-shaping	•
• url	•
• usb	•
• vlan	•
• vpn	<ul style="list-style-type: none"> • auto • sec-level
• vpn-group	•
• vrouter	<ul style="list-style-type: none"> • default-vrouter: VSYS command • router-id: specifies the router id for the OSPF or BGP instance • rule: VSYS command • sharable: VSYS command
• vsys	•
• vsys-profile	•
• webauth	•
• webtrends	•
• wlan	•
• xauth	•

The remaining portion of this page was intentionally left blank

