



Configuration for Common Criteria, EAL4

Document Number: 093-1737-000

Version: E

Date: Apr 17, 2007

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.

Change History

Ver	Change Description	ECO No.	Date
A	1. Initial Draft		8/2/2005
B	1. Formatted as a stand-alone document Interface setup syntax for NS-25/50 was updated.		11/8/2005
C	<ol style="list-style-type: none"> 1. Add “unset interface vlan1 manage” to disable management to interface in vlan zone when the appliance operates in Transparent mode 2. Add notes indicating that the “Evaluated Configuration Examples” are based on NS-500 3. Change interface name in the “Evaluated Configuration Examples” from “mgmt” to “mgt” 4. Add “set interface e1/1 zone trust” to the “Evaluated Configuration Examples” for Unauthenticated NAT/Route mode and Authenticated NAT/Route mode 5. Add “unset interface e1/1 manage” to the “Evaluated Configuration Examples” for Unauthenticated NAT/Route mode and Authenticated NAT/Route mode 6. Add “unset interface vlan1 manage” the “Evaluated Configuration Examples” for Authenticated Transparent mode 		11/11/2005
D	<ol style="list-style-type: none"> 1. Add CLI command to set new password for administrator 2. Add management “mgt Interface” for NS-500, ISG-1000, ISG-2000, NS-5200, NS-5400 in the Juniper NetScreen Security Appliance models table 3. Clarify that “screen ip-spoofing drop-no-rpf-route” is only applied when the security appliance operates under NAT/Route Unauthenticated or NAT/Route Authenticated mode 4. Remove Guidance to enable “screen ip-spoofing drop-no-rpf-route” for Layer-2 zones (e.g. v1-trust or v1-untrust) when operating in Transparent mode (including Transparent Authenticated mode) 		11/14/2005

D	<ol style="list-style-type: none"> 5. Added reset instruction to Authenticated Transparent Mode setup procedures. 6. Add Global deny policy 7. Added statement for Intrazone spoofing prevention. 8. Added traffic logging option (log) for all policy statements 9. Added Logging Permitted Packets section 10. Add statement for positioning newly created policy at any specific location in the policy list 11. Added a description for logging dropped policy based authenticated packets. 12. Add a footnote at the bottom of the table in “Setting the Operation Mode, interface table to clarify the use of ethernet, eth and e in command syntaxes. 13. Moved the section “Logging Permitted Packets” ahead of section “Logging Dropped Packets”. 14. In section “Configuring Screen Options” added clarifications that changes in the HTTP blocking option only applies to the newly created application sessions. 15. Updated and correct sample script for “Authenticated Transparent Mode” to remove screen ip-spoofing command and change trust to v1-trust, and untrust to v1-untrust. 		
E	<ol style="list-style-type: none"> 1. Initial Draft for ScreenOS 5.4 ... based on revision D of CC-OS5 2. Correction to CLI command <ol style="list-style-type: none"> a. Typographical corrections b. In the sample scripts to reflect the ATE needed initial setup <ol style="list-style-type: none"> i. Interface references ii. IP addresses and labels 3. Added reference to new hardware platforms, i.e. SSG 520M/550M, etc. 		4/17/07

The remaining portion of this page was intentionally left blank

Table of Contents

Introduction	6
Properly Identifying the Juniper Networks Security Appliances for Common Criteria EAL4	6
Upgrading a Juniper NetScreen Device for Common Criteria EAL4	7
Proper Steps to Secure a Juniper NetScreen Device for Common Criteria EAL4... 9	9
Restoring to the Default Settings.....	9
Setting the Date and Time	9
Setting/Changing Administrator Name & Password and Password Length Restrictions.....	10
Setting the Operation Mode.....	11
Unauthenticated NAT/Route Mode	13
Authenticated NAT/Route Mode	14
Authenticated Transparent Mode.....	24
Restricting Remote Access	29
Disabling Internal Commands.....	30
Configuring Syslog	31
Configuring Audit Loss Mitigation	32
Logging Permitted Packets.....	32
Logging Dropped Packets	32
Configuring Screen Options.....	33
Removing Permissive Default Policy	37
Setting a Policy to Permit Traffic.....	37
Configuring IP Spoofing Protection.....	41
Unauthenticated NAT/Route Mode	41
Authenticated NAT/Route Mode & Authenticated Transparent Mode.....	41
Saving the Applied Configuration	43
Backup and Recovery from the Last-Known-Good Configuration	43
Evaluated Configuration Usage Guidance.....	45
Starting, Stopping, and Reviewing Audit Logs.....	46

Commands Not Included in the Evaluated Configuration	48
Evaluated Configuration Examples	51
Unauthenticated NAT/Route Mode.....	51
Authenticated NAT/Route Mode	53
Authenticated Transparent Mode	58

The remaining portion of this page was intentionally left blank

Introduction

All Juniper Networks security appliances, hereafter referred to as security appliances, are designed to meet the Common Criteria requirements for Common Criteria, EAL4. However, there are certain configuration actions that are required for a security administrator to properly secure the device to be in compliance with the Common Criteria EAL4 security target. While these requirements are for anyone needing Common Criteria assurance, they can also be used as general guidelines for administrators wishing to better secure the deployment of a Security appliance.

Properly Identifying the Juniper Networks Security Appliances for Common Criteria EAL4

Before carrying out any step to secure a Juniper NetScreen device, 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 may be evidence of tampering.
 - ✓ Each box is packaged with custom tape to indicate that Juniper 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 may 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 may 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, section 1.1. 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 ScreenOS software versions installed on the devices might vary depending on the manufacturing time of the security appliances.

Upgrading a Juniper NetScreen Device for Common Criteria EAL4

In the case a security appliance does not use the ScreenOS software versions compliant with the *Juniper Networks Security Appliances Security Target EAL4*, the correct ScreenOS software image needs to be loaded on to the security appliance.

Before the ScreenOS software image can be loaded on to the security appliance, you need to configure the manage interface through which the images can be downloaded from the FTP server to the security appliances. The following commands will configure the zone and IP address for the manage interface.

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

Note:

*The security zone name does not have to be capitalized (i.e. **Trust**) in the command*

where,

interface-name should be the name of the actual interface connected to the PC serving as FTP server; through this interface the security appliances can communicate with the FTP server. For the 5-series devices (including Juniper NetScreen-5GT), interface **trust** – bound to the security zone **trust** by default – can be used. For devices Juniper NetScreen-204, and -208, you can use interface **ethernet1**. For Juniper NetScreen-500, interface **ethernet1/1** in the security zone **trust** can be in place of *interface-name*. On high-level security appliances including Juniper NetScreen-ISG2000 and ISG1000 interface ethernet1/1 can be used. Interface ethernet2/1 can be used for Juniper NetScreen-5200 and NetScreen 5400.

and,

ip-address: should be 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 IP address for PC serving as the 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 device Juniper NetScreen-5GT is named “ns5gt.5.4.0r4.0” and resides on FTP server (with IP address 10.155.95.253), under the directory */tftpboot/screenOS-image/5.4/*, the command should be as the following:

**save software from tftp 10.155.95.253 /tftpboot/screenOS-image/5.4/
ns5gt.5.4.0r4.0 to flash**

The downloading process will take a few minutes. After the downloading process is completed, the security appliance will return to the CLI prompt and will need to be rebooted. Issue the command **reset** and provide answers for the questions you are asked as below to completely load the image to the security appliance and restore the default manufacture configurations.

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.

Proper Steps to Secure a Juniper NetScreen Device for Common Criteria EAL4

To configure a security appliance to operate securely, and in conformance with the requirements outlined in *Juniper Networks Security Appliances Security Target EAL4*, the following actions must be taken:

Restoring to the Default Settings

- To comply with Common Criteria, the security appliance should be restored to the default manufacturing operation mode and configurations before putting the appliance in a different operation modes including Transparent Authenticated mode (a.s.k.a. Transparent VPN mode) or NAT/Route Authenticated mode (a.s.k.a. NAT/Route VPN mode) or before perform any configurations for any specific testing.

Use the commands **unset all** and **reset** along with the following answers to restored the default operation mode and configurations for the appliance.

```
unset all
Erase all system config, are you sure y/[n] ? y
reset
Configuration modified, save? [y]/n n
System reset, are you sure? y/[n] y
```

Setting the Date and Time

- The following command must be enabled to ensure that the date and time stamps used on audit messages are accurate:

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

Setting/Changing Administrator Name & Password and 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 mixing lower case and upper case 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 as soon as possible to prevent unauthorized access. See *Chapter 1, "Administration," in Volume 3 in the NetScreen Concepts & Examples manual* 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 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.

The following CLI commands, in order, are required to set a new administrator name and password:

```
set admin name name-string
```

```
set admin password password-string
```

where,

name-string and *password-string* should be replaced with actual login name and password of administrator

Setting the Operation Mode

To determine on which operation mode a security appliance is, use the following command.

get system

You should see the following either of the following messages:

“**System in NAT/Route mode**” which indicates that the security appliance is operating in NAT/Route mode;

or,

“**System in transparent mode**” which indicates that the security appliance is operating in transparent mode.

- Juniper NetScreen Security Appliance models

Juniper NetScreen -5GT	Juniper NetScreen -204, -208	Juniper NetScreen SSG-5, -20
Trust Zone Connection: Trusted Interface	Trust Zone Connection: Ethernet1 Interface	Trust Zone Connection: Ethernet0/0
DMZ Zone Connection: N/A	DMZ Zone Connection: Ethernet2 Interface	DMZ Zone Connection: Ethernet0/1
Untrust Zone Connection: Untrusted Interface	Untrust Zone Connection: Ethernet3 Interface	Untrust Zone Connection: Ethernet0/2
HA Connection: N/A	HA Connection: Ethernet 4 Interface	HA Connection: N/A

*The remaining portion of this page was intentionally left blank
Continued on the next page.*

Juniper NetScreen -500	Juniper NetScreen -ISG1000, -ISG2000	Juniper NetScreen SSG-520M, -550M
Trust Zone Connection: Ethernet1/1	Trust Zone Connection: Ethernet1/1 Interface	Trust Zone Connection: Ethernet0/0
DMZ Zone Connection: Ethernet2/1	DMZ Zone Connection: Ethernet1/2 Interface	DMZ Zone Connection: Ethernet0/1
Untrust Zone Connection: Ethernet3/1	Untrust Zone Connection: Ethernet1/3 Interface	Untrust Zone Connection: Ethernet0/2
HA Connection: ha1 and ha2	HA Connection: N/A	HA Connection: Ethernet0/3

Juniper NetScreen -5200	Juniper NetScreen- 5400
Trust Zone Connection: Ethernet2/1 Interface	Trust Zone Connection: Ethernet2/1 Interface
DMZ Zone Connection: Ethernet2/2 Interface	DMZ Zone Connection: Ethernet3/2 Interface
Untrust Zone Connection: Ethernet2/3 Interface	Untrust Zone Connection: Ethernet2/3 Interface
HA Connection: ha1 and ha2	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.

- 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

Unauthenticated NAT/Route Mode

To configure a security appliance in unauthenticated NAT/Route Mode, enter the following commands for the appropriate security appliance:

5-series security appliances (including Juniper NetScreen-5GT):

```
set interface trust ip ip-address  
set interface untrust ip ip-address
```

Juniper NetScreen-SSG-5 and -20 Set interface eth0/0 zone trust

```
set interface eth0/0 ip ip-address  
set interface eth0/0 zone dmz  
set interface eth0/1 ip ip-address  
set interface eth0/0 zone untrust  
set interface eth0/2 ip ip-address
```

Juniper NetScreen-204 and -208:

```
set interface eth1 ip ip-address  
set interface eth2 ip ip-address  
set interface eth3 ip ip-address
```

Juniper NetScreen-SSG-520M and -550M: ...

```
set interface eth0/0 ip ip-address  
set interface eth0/1 ip ip-address  
set interface eth0/2 ip ip-address
```

Juniper NetScreen-500:

```
unset interface mgt ip  
set interface eth1/1 zone trust  
set interface eth1/1 ip ip-address  
set interface eth2/1 zone dmz  
set interface eth2/1 ip ip-address  
set interface eth3/1 zone untrust  
set interface eth3/1 ip ip-address
```

Juniper NetScreen-ISG1000 and ISG2000:

```
unset interface mgt ip  
set interface eth1/1 zone trust  
set interface eth1/1 ip ip-address
```

```
set interface eth1/2 zone dmz
set interface eth1/2 ip ip-address
set interface eth1/3 zone untrust
set interface eth1/3 ip ip-address
```

Juniper NetScreen-5200

```
unset interface mgt ip
set interface eth2/1 zone trust
set interface eth2/1 ip ip-address
set interface eth2/2 zone dmz
set interface eth2/2 ip ip-address
set interface eth2/3 zone untrust
set interface eth2/3 ip ip-address
```

Juniper NetScreen-5400:

```
unset interface mgt ip
set interface eth2/1 zone trust
set interface eth2/1 ip ip-address
set interface eth3/2 zone dmz
set interface eth3/2 ip ip-address
set interface eth2/3 zone untrust
set interface eth2/3 ip ip-address
```

Authenticated NAT/Route Mode

A security appliance can be configured in authenticated NAT/Route Mode using either a Route-based VPN or Policy-based VPN. Both Route-based VPN and Policy-based VPN are supported in authenticated NAT/Route mode.

Only Manual Key is supported in the Evaluated Configuration, i.e. AutoKey cannot be used. 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.

Route-Based VPN

To configure the security appliance with a Route-based VPN in authenticated NAT/Route mode, enter the following commands for the appropriate security appliance:

5-series security appliances (including Juniper NetScreen-5GT):

```
set interface trust ip ip-address  
set interface untrust ip ip-address
```

```
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface untrust
```

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

```
set vrouter trust-vr route 0.0.0.0/0 interface untrust gateway local-  
gateway-ip  
set vrouter trust-vr route local-subnet interface tunnel.1
```

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

```
set policy id id-num top from trust to untrust local-LAN remote-LAN  
any permit log count  
set policy id id-num top from untrust to trust local-LAN remote-LAN  
any permit log count
```

Juniper NetScreen-204 and 208:

```
set interface eth1 ip ip-address  
set interface eth2 ip ip-address  
set interface eth3 ip ip-address
```

```
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface eth3
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-untrust-  
interface-ip outgoing-interface eth3 esp 3des password password-  
string1 auth sha-1 password password-string2  
set vpn configured-vpn-name bind interface tunnel.1
```

```
set vrouter trust-vr route 0.0.0.0/0 interface eth3 gateway local-  
gateway-ip  
set vrouter trust-vr route local-subnet interface tunnel.1
```

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

```
set policy id id-num top from trust to untrust local-LAN remote-LAN  
any permit log count  
set policy id id-num top from untrust to trust local-LAN remote-LAN  
any permit log count
```

Juniper NetScreen-SSG-5 and -20:

```
set interface eth0/0 ip ip-address  
set interface eth0/1 ip ip-address  
set interface eth0/2 ip ip-address
```

```
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface eth0/2
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-untrust-  
interface-ip outgoing-interface eth0/2 esp 3des password password-  
string1 auth sha-1 password password-string2  
set vpn configured-vpn-name bind interface tunnel.1
```

```
set vrouter trust-vr route 0.0.0.0/0 interface eth0/2 gateway local-  
gateway-ip  
set vrouter trust-vr route local-subnet interface tunnel.1
```

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

```
set policy id id-num top from trust to untrust local-LAN remote-LAN  
any permit log count  
set policy id id-num top from untrust to trust local-LAN remote-LAN  
any permit count
```

Juniper NetScreen-500:

```
unset interface mgt ip  
set interface eth1/1 zone trust  
set interface eth1/1 ip ip-address  
set interface eth2/1 zone dmz  
set interface eth2/1 ip ip-address  
set interface eth3/1 zone untrust  
set interface eth3/1 ip ip-address
```

```
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface eth3/1
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-untrust-  
interface-ip outgoing-interface eth3/1 esp 3des password password-  
string1 auth sha-1 password password-string2
```

```
set vpn configured-vpn-name bind interface tunnel.1  
  
set vrouter trust-vr route 0.0.0.0/0 interface eth3/1 gateway local-gateway-ip  
set vrouter trust-vr route local-subnet interface tunnel.1  
  
set address trust local-LAN local-subnet  
set address untrust remote-LAN remote-subnet  
  
set policy id id-num top from trust to untrust local-LAN remote-LAN  
any permit log count  
set policy id id-num top from untrust to trust local-LAN remote-LAN  
any permit log count
```

Juniper NetScreen-SSG-520M and -550M:

```
unset interface mgt ip  
set interface e0/0 zone trust  
set interface e0/0 ip ip-address  
set interface eth0/1 zone dmz  
set interface eth0/1 ip ip-address  
set interface eth0/2 zone untrust  
set interface eth0/2 ip ip-address  
  
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface eth0/2  
  
set vpn vpn-name manual local-spi remote-spi gateway remote-untrust-interface-ip  
outgoing-interface eth0/2 esp 3des password password-string1 auth sha-1 password password-string2  
set vpn configured-vpn-name bind interface tunnel.1  
  
set vrouter trust-vr route 0.0.0.0/0 interface eth0/2 gateway local-gateway-ip  
set vrouter trust-vr route local-subnet interface tunnel.1  
  
set address trust local-LAN local-subnet  
set address untrust remote-LAN remote-subnet  
  
set policy id id-num top from trust to untrust local-LAN remote-LAN  
any permit log count  
set policy id id-num top from untrust to trust local-LAN remote-LAN  
any permit log count
```

Juniper NetScreen-ISG1000 and ISG2000:

```
unset interface mgt ip
set interface eth1/1 zone trust
set interface eth1/1 ip ip-address
set interface eth1/2 zone dmz
set interface eth1/2 ip ip-address
set interface eth1/3 zone untrust
set interface eth1/3 ip ip-address
```

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface eth1/3
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-untrust-
interface-ip outgoing-interface eth1/3 esp 3des password password-
string1 auth sha-1 password password-string2
set vpn configured-vpn-name bind interface tunnel.1
```

```
set vrouter trust-vr route 0.0.0.0/0 interface eth1/3 gateway local-
gateway-ip
set vrouter trust-vr route local-subnet interface tunnel.1
```

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

```
set policy id id-num top from trust to untrust local-LAN remote-LAN
any permit log count
set policy id id-num top from untrust to trust local-LAN remote-LAN
any permit log count
```

Juniper NetScreen-5200:

```
unset interface mgt ip
set interface eth2/1 zone trust
set interface eth2/1 ip ip-address
set interface eth2/2 zone dmz
set interface eth2/2 ip ip-address
set interface eth2/3 zone untrust
set interface eth2/3 ip ip-address
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface eth2/3
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-untrust-
interface-ip outgoing-interface eth2/3 esp 3des password password-
string1 auth sha-1 password password-string2
set vpn configured-vpn-name bind interface tunnel.1
```

set vrouter trust-vr route 0.0.0.0/0 interface eth2/3 gateway local-gateway-ip

set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN 1 local-subnet

set address untrust remote-LAN remote-subnet

set policy id id-num top from trust to untrust local-LAN remote-LAN any permit log count

set policy id id-num top from untrust to trust local-LAN remote-LAN any permit log count

Juniper NetScreen-5400:

unset interface mgt ip

set interface eth2/1 zone trust

set interface eth2/1 ip ip-address

set interface eth3/2 zone dmz

set interface eth3/2 ip ip-address

set interface eth2/3 zone untrust

set interface eth2/3 ip ip-address

set interface tunnel.1 zone untrust

set interface tunnel.1 ip unnumbered interface eth2/3

set vpn vpn-name manual local-spi remote-spi gateway remote-untrust-interface-ip outgoing-interface eth2/3 esp 3des password password-string1 auth sha-1 password password-string2

set vpn configured-vpn-name bind interface tunnel.1

set vrouter trust-vr route 0.0.0.0/0 interface eth2/3 gateway local-gateway-ip

set vrouter trust-vr route local-subnet interface tunnel.1

set address trust local-LAN local-subnet

set address untrust remote-LAN remote-subnet

set policy id id-num top from trust to untrust local-LAN remote-LAN any permit log count

set policy id id-num top from untrust to trust local-LAN remote-LAN any permit log count

Policy-Based VPN

To configure the security appliance with a Policy-based VPN in authenticated NAT/Route mode, enter the following commands for the appropriate security appliance:

5-series security appliances (including Juniper NetScreen-5GT):

```
set interface trust ip ip-address  
set interface untrust ip ip-address
```

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

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

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

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

Juniper NetScreen-204 and 208:

i

```
set interface eth1 ip ip-address  
set interface eth2 ip ip-address  
set interface eth3 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-  
outbound-interface outgoing-interface eth3 esp aes128 password  
password-string1 auth sha-1 password password-string2  
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface eth3 gateway local-  
gateway-ip
```

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

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

Juniper NetScreen-SSG-5 and -20:

```
set interface eth0/0 ip ip-address  
set interface eth0/1 ip ip-address  
set interface eth0/2 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-  
outbound-interface outgoing-interface eth0/2 esp aes128 password  
password-string1 auth sha-1 password password-string2  
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface eth0/2 gateway local-  
gateway-ip
```

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

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

Juniper NetScreen-500:

```
unset interface mgt ip  
set interface eth1/1 zone trust  
set interface eth1/1 ip ip-address  
set interface eth2/1 zone dmz  
set interface eth2/1 ip ip-address  
set interface eth3/1 zone untrust  
set interface eth3/1 ip ip-address
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-  
outbound-interface outgoing-interface eth3/1 esp aes128 password  
password-string1 auth sha-1 password password-string2  
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface eth3/1 gateway local-  
gateway-ip
```

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

set address untrust remote-LAN *remote-subnet*

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

Juniper NetScreen-SSG-520M, -550M:

unset interface mgt ip
set interface eth0/0 zone trust
set interface eth0/0 ip *ip-address*
set interface eth0/1 zone dmz
set interface eth0/1 ip *ip-address*
set interface eth0/2 zone untrust
set interface eth0/2 ip *ip-address*

set vpn *vpn-name* **manual local-spi remote-spi gateway remote-**
outbound-interface outgoing-interface eth0/2 esp aes128 password
password-string1 auth sha-1 password password-string2
set vpn *configured-vpn-name* **bind zone untrust-tun**

set vrouter trust-vr route 0.0.0.0/0 interface eth0/2 gateway local-
gateway-ip

set address trust local-LAN *local-subnet*
set address untrust remote-LAN *remote-subnet*

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

Juniper NetScreen-ISG1000 and ISG2000:

unset interface mgt ip
set interface eth1/1 zone trust
set interface eth1/1 ip *ip-address*
set interface eth1/2 zone dmz
set interface eth1/2 ip *ip-address*
set interface eth1/3 zone untrust
set interface eth1/3 ip *ip-address*

set vpn *vpn-name* **manual local-spi remote-spi gateway remote-**
outbound-interface outgoing-interface eth1/3 esp aes128 password
password-string1 auth sha-1 password password-string2

```
set vpn configured-vpn-name bind zone untrust-tun  
  
set vrouter trust-vr route 0.0.0.0/0 interface eth1/3 gateway local-gateway-ip  
  
set address trust local-LAN local-subnet  
set address untrust remote-LAN remote-subnet  
  
set policy id id-num top from trust to untrust local-LAN remote-LAN  
any tunnel vpn configured-vpn-name log  
set policy id id-num top from untrust to trust remote-LAN local-LAN  
any tunnel vpn configured-vpn-name log
```

Juniper NetScreen-5200 :

```
unset interface mgt ip  
set interface eth2/1 zone trust  
set interface eth2/1 ip ip-address  
set interface eth2/2 zone dmz  
set interface eth2/2 ip ip-address  
set interface eth2/3 zone untrust  
set interface eth2/3 ip ip-address  
set interface tunnel.1 zone untrust  
set interface tunnel.1 ip unnumbered interface eth2/3  
  
set vpn vpn-name manual local-spi remote-spi gateway remote-outbound-interface outgoing-interface eth2/3 esp aes128 password password-string1 auth sha-1 password password-string2  
set vpn configured-vpn-name bind zone untrust-tun  
  
set vrouter trust-vr route 0.0.0.0/0 interface eth2/3 gateway local-gateway-ip  
  
set address trust local-LAN local-subnet  
set address untrust remote-LAN remote-subnet  
  
set policy id id-num top from trust to untrust local-LAN remote-LAN  
any tunnel vpn configured-vpn-name log  
set policy id id-num top from untrust to trust remote-LAN local-LAN  
any tunnel vpn configured-vpn-name log
```

Juniper NetScreen-5400:

```
unset interface mgt ip  
set interface eth2/1 zone trust  
set interface eth2/1 ip ip-address
```

```
set interface eth3/2 zone dmz
set interface eth3/2 ip ip-address
set interface eth2/3 zone untrust
set interface eth2/3 ip ip-address
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface eth2/3
```

```
set vpn vpn-name manual local-spi remote-spi gateway remote-
outbound-interface outgoing-interface eth2/3 esp aes128 password
password-string1 auth sha-1 password password-string2
set vpn configured-vpn-name bind zone untrust-tun
```

```
set vrouter trust-vr route 0.0.0.0/0 interface eth2/3 gateway local-
gateway-ip
```

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

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

Authenticated Transparent Mode

In Transparent Authenticated mode, only Policy-based VPN is supported. To configure a security appliance with a Policy-based VPN in authenticated Transparent Mode, enter the following commands for the appropriate security appliance: After the commands have been entered, the configuration must be saved using a save command and then the device reset.

5-series security appliances (including Juniper NetScreen-5GT):

```
unset interface trust ip
set interface trust zone v1-trust
set interface untrust zone v1-untrust
set interface vlan1 ip ip-address
```

```
set address v1-trust local_lan local-subnet
set address v1-untrust peer_lan remote-subnet
```

```
set vpn vpn-name manual local-spi-value remote-spi-value gateway  
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256  
password password-string1 auth sha-1 password password-string2
```

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

```
set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan  
any tunnel vpn configured-vpn-name log  
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan  
any tunnel vpn configured-vpn-name log  
save  
reset
```

Juniper NetScreen-204 and 208:

```
unset interface eth1 ip  
unset interface eth1 zone  
unset interface eth2 zone  
unset interface eth3 zone  
set interface eth1 zone v1-trust  
set interface eth2 zone v1-dmz  
set interface eth3 zone v1-untrust  
set interface vlan1 ip ip-address
```

```
set address v1-trust local_lan local-subnet  
set address v1-untrust peer_lan remote-subnet
```

```
set vpn vpn-name manual local-spi-value remote-spi-value gateway  
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256  
password password-string1 auth sha-1 password password-string2
```

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

```
set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan  
any tunnel vpn configured-vpn-name log  
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan  
any tunnel vpn configured-vpn-name log  
save  
reset
```

Juniper NetScreen-SSG-5 and -20:

```
unset interface eth0/0 ip
unset interface eth0/0 zone
unset interface eth0/1 zone
unset interface eth0/2 zone
set interface eth0/0 zone v1-trust
set interface eth0/1 zone v1-dmz
set interface eth0/2 zone v1-untrust
set interface vlan1 ip ip-address
```

```
set address v1-trust local_lan local-subnet
set address v1-untrust peer_lan remote-subnet
```

```
set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256
password password-string1 auth sha-1 password password-string2
```

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

```
set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan
any tunnel vpn configured-vpn-name log
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan
any tunnel vpn configured-vpn-name log
save
reset
```

Juniper NetScreen-500:

```
unset interface mgt ip
unset interface eth1/1 zone
unset interface eth1/2 zone
unset interface eth2/1 zone
unset interface eth2/2 zone
unset interface eth3/1 zone
unset interface eth3/2 zone
set interface eth1/1 zone v1-trust
set interface eth2/1 zone v1-dmz
set interface eth3/1 zone v1-untrust
set interface vlan1 ip ip-address
```

```
set address v1-trust local_lan local-subnet
set address v1-untrust peer_lan remote-subnet
```

```
set vpn vpn-name manual local-spi-value remote-spi-value gateway  
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256  
password password-string1 auth sha-1 password password-string2
```

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

```
set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan  
any tunnel vpn configured-vpn-name log  
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan  
any tunnel vpn configured-vpn-name log  
save  
reset
```

Juniper NetScreen-SSG-520M, -550M:

```
unset interface mgt ip  
unset interface eth0/0 zone  
unset interface eth0/1 zone  
unset interface eth0/2 zone  
unset interface eth0/3 zone
```

```
set interface eth0/0 zone v1-trust  
set interface eth0/1 zone v1-dmz  
set interface eth0/2 zone v1-untrust  
set interface vlan1 ip ip-address
```

```
set address v1-trust local_lan local-subnet  
set address v1-untrust peer_lan remote-subnet
```

```
set vpn vpn-name manual local-spi-value remote-spi-value gateway  
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256  
password password-string1 auth sha-1 password password-string2
```

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

```
set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan  
any tunnel vpn configured-vpn-name log  
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan  
any tunnel vpn configured-vpn-name log  
save  
reset
```

Juniper NetScreen-ISG1000 and ISG2000:

```
unset interface mgt ip  
set interface eth1/1 zone v1-trust  
set interface eth1/2 zone v1-dmz  
set interface eth1/3 zone v1-untrust  
set interface vlan1 ip ip-address  
  
set address v1-trust local_lan local-subnet  
set address v1-untrust peer_lan remote-subnet  
  
set vpn vpn-name manual local-spi-value remote-spi-value gateway  
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256  
password password-string1 auth sha-1 password password-string2  
  
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway local-  
gateway-ip  
  
set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan  
any tunnel vpn configured-vpn-name log  
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan  
any tunnel vpn configured-vpn-name log  
save  
reset
```

Juniper NetScreen-5200 :

```
unset interface mgt ip  
set interface eth2/1 zone v1-trust  
set interface eth2/2 zone v1-dmz  
set interface eth2/3 zone v1-untrust  
set interface vlan1 ip ip-address  
  
set address v1-trust local_lan local-subnet  
set address v1-untrust peer_lan remote-subnet  
  
set vpn vpn-name manual local-spi-value remote-spi-value gateway  
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256  
password password-string1 auth sha-1 password password-string2  
  
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway local-  
gateway-ip
```

```
set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan
any tunnel vpn configured-vpn-name log
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan
any tunnel vpn configured-vpn-name log
save
reset
```

Juniper NetScreen-5400:

```
unset interface mgt ip
set interface eth2/1 zone v1-trust
set interface eth3/2 zone v1-dmz
set interface eth2/3 zone v1-untrust
set interface vlan1 ip ip-address

set address v1-trust local_lan local-subnet
set address v1-untrust peer_lan remote-subnet

set vpn vpn-name manual local-spi-value remote-spi-value gateway
remote-vlan-interface-ip outgoing-zone v1-untrust esp aes256
password password-string1 auth sha-1 password password-string2

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

set policy id id-num top from v1-trust to v1-untrust local_lan peer_lan
any tunnel vpn configured-vpn-name log
set policy id id-num top from v1-untrust to v1-trust peer_lan local_lan
any tunnel vpn configured-vpn-name log
save
reset
```

Restricting Remote Access

To place a security appliance into a mode consistent with that specified in *Juniper Networks Security Appliances Security Target EAL4*, management access must be limited to the locally connected console port. Security appliances are not shipped in this mode by default.

To limit management access to the console port, the interface that is by default in the **V1-Trust** or **Trust** security zone needs to have management access turned

off. See the interface commands in the *Juniper Networks NetScreen CLI Reference Guide, Version 5.4.0* for more information.

All other interfaces have management access turned off by default, so no action is necessary to turn management off.

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

unset interface *interface-name* manage

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

Juniper NetScreen-5GT:	unset interface trust manage
Juniper NetScreen-204:	unset interface ethernet1 manage
Juniper NetScreen-208:	unset interface ethernet1 manage
Juniper NetScreen-SSG-5:	unset interface ethernet0/0 manage
Juniper NetScreen-SSG-20:	unset interface ethernet0/0 manage
Juniper NetScreen-500:	unset interface ethernet1/1 manage
Juniper NetScreen-SSG-520M:	unset interface ethernet0/0 manage
Juniper NetScreen-SSG-550M:	unset interface ethernet0/0 manage
Juniper NetScreen ISG-1000:	unset interface ethernet1/1 manage
Juniper NetScreen ISG-2000:	unset interface ethernet1/1 manage
Juniper NetScreen-5200:	unset interface ethernet2/1 manage
Juniper NetScreen-5400:	unset interface ethernet2/1 manage

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

The following command is applied for all models (including Juniper NetScreen-5GT, 204, 208, SSG-5, SSG-20, SSG-520M, SSG-550M, 500, ISG-1000, ISG-2000, 5200, and 5400):

unset interface vlan1 manage

Disabling Internal Commands

- In order for the security appliances' commands to be consistent with those that are certified for Common Criteria EAL4, the security appliance administrator must disable internal commands. Internal commands are used for troubleshooting and debugging purposes and are not documented.

To disable internal commands, you must run the following command:

set common-criteria no-internal-commands

To use internal commands (i.e. 'debug flow basic' and 'get dbuf stream', 'debug ids sat') for troubleshooting and debugging purposes, internal commands must be enabled by using the following command:

unset common-criteria no-internal-commands

Note: Use the internal commands 'debug ids sat' is for ISG-1000, ISG-2000, NS-5200 and NS-5400

Configuring Syslog

You must configure a Syslog server as a backup for security audit information and for long-term audit log information storage. This will help prevent a loss in security audit information. See *Chapter 2, "Monitoring NetScreen Devices," in Volume 3 of the NetScreen Concepts & Examples manual* for more information on how to set up and configure a Syslog server to work with security appliances.

The specific commands required to set up a Syslog server are listed below:

```
set syslog config ip-address facilities local0 local0  
set syslog config ip-address port 514  
set syslog config ip-address log traffic  
set syslog enable  
set log module system level level-name destination syslog
```

where

ip-address is the actual IP address of the Syslog server
level-name is the severity level of the log

Note: You must enter the set log command once for each message level. The options for level-name are listed below:

```
emergency  
alert  
critical  
error  
warning  
notification  
information  
debugging
```

Configuring Audit Loss Mitigation

There are cases where more auditable events can occur than the security appliance is able to write to a syslog server. To be compliant with Common Criteria requirements, the security appliance must stop further auditable events from occurring until the audit trail is able to handle more traffic. An authorized administrator must enable the following command:

```
set log audit-loss-mitigation
```

Logging Permitted Packets

- To log permitted packets passing through the device enable logging option on all authenticated and/or unauthenticated 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 NetScreen 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 5.0 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	Juniper NetScreen -5GT	Juniper NetScreen SSG-5 &20	Juniper NetScreen -204, 208
<i>alarm-threshold</i>	512	512	1024
<i>Q-size</i>	512	512	10240
<i>src-threshold</i>	512	512	4000
<i>dst-threshold</i>	512	512	40000

Platforms Platform Screening Values	Juniper NetScreen – SSG-520 & 550	Juniper NetScreen -500	Juniper NetScreen -- ISG1000 & 2000
<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 Platform Screening Values	Juniper NetScreen-5200	Juniper NetScreen-5400
<i>alarm-threshold</i>	1024	1024
<i>Q-size</i>	10240	10240
<i>src-threshold</i>	4000	4000
<i>dst-threshold</i>	40000	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.

Screen function only generate alarm without dropping packet: OFF

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

```
unset zone untrust screen tear-drop  
unset zone untrust screen syn-flood  
unset zone untrust screen ping-death  
unset zone untrust screen ip-filter-src  
unset zone untrust screen land
```

The following will be displayed when the security zone has no screening options 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
```

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

When security appliance in Transparent mode (including Transparent Authenticated mode), 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 Unauthenticated and Nat/Route Authenticated mode). 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 NetScreen CLI Reference Guide, Version 5.4.0* for more information.

For instance, when the security 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 security zones that are configured and used.

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 5-series products including Juniper NetScreen-5GT and Secure Services Group products -- SSG 5 and SSG 20 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 NetScreen CLI Reference Guide, Version 5.4.0* for more information on how to set and unset policies.

To disable this default policy on the Juniper NetScreen-5GT, SSG 5 and SSG 20 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 the following:

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

where,

pol-id is 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 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 in configured in default (Layer 3 NAT/Route) mode, the following commands need to be executed:

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

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

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

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 would 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 may 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. The following command is used to create a host or network address in a security zone.

```
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
```

Once the source and destination addresses have been configured, the policy with counting and logging enabled can be configured using the following command.

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

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 through 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 count
```

where,

trust-HostA and *untr-NetworkB* are, respectively, host and network addresses 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 count

For more information, refer to *“Reordering Policies” in Chapter 7, “Policies,” in Volume 2 of the Juniper Concepts and Examples manual.*

Configuring IP Spoofing Protection

In general, IP spoofing is typically blocked by the screen option “ip-spoofing” as indicated above in the section, “Configuring Screen Options”. This includes **Intrazone** configurations where the VPN traffic is on the same zone as the decrypted traffic. However depending on the configuration implemented (especially **Interzone**), the following additional steps are required to be adequately protected against IP spoofing attacks.

The following guidance for Unauthenticated NAT/Route mode should be applied in addition to the guidance provided in the previous section “Setting a Policy to Permit Traffic”. However the following guidance for Authenticated NAT/Route mode and Authenticated Transparent mode should supplement the guidance provided in the previous section “Setting a Policy to Permit Traffic”.

Unauthenticated NAT/Route Mode

The use of the **ip-spoofing** parameter to the **set zone** command does not prevent spoofing attacks, masquerading as a host on the loopback network, via clear traffic in NAT/Route non-Authenticated mode.

To prevent NAT/Route non-Authenticated loopback ip-spoof attacks, the policy governing the traffic should be drop traffic from the loopback source address. For example:

```
set policy id 51 top from untrust to trust untrust_loopback any any deny log  
set policy id 50 top from trust to untrust trust_loopback any any deny log
```

where, *trust_loopback* and *untrust_loopback* is 127.0.0.0/8

Authenticated NAT/Route Mode & Authenticated Transparent Mode

When operating in Authenticated NAT/Route mode or Authenticated Transparent mode, the “ip-spoofing” screen option is bypassed. Therefore a set of addresses and policies need to be defined to allow only traffic permitted, excluding spoofed IP addresses. In the example below, a grouping of addresses x.x.x.1-254 are defined for both the internal and external networks. The following example is presented for an Authenticated NAT/Route mode configuration, however it can

also be applied for the Authenticated Transparent mode configuration. If used for Authenticated Transparent mode, **trust** should be changed to **v1-trust** and **untrust** should be changed to **v1-untrust**.

Security Appliance #1:

```
set address trust Trust_LAN_1 x.x.x.127/25
set address trust Trust_LAN_2 x.x.x.191/26
set address trust Trust_LAN_3 x.x.x.223/27
set address trust Trust_LAN_4 x.x.x.239/28
set address trust Trust_LAN_5 x.x.x.247/29
set address trust Trust_LAN_6 x.x.x.251/30
set address trust Trust_LAN_7 x.x.x.253/31
set address untrust side_2_1 x.x.x.127/25
set address untrust side_2_2 x.x.x.191/26
set address untrust side_2_3 x.x.x.223/27
set address untrust side_2_4 x.x.x.239/28
set address untrust side_2_5 x.x.x.247/29
set address untrust side_2_6 x.x.x.251/30
set address untrust side_2_7 x.x.x.253/31
set group address trust Trust_LAN add Trust_LAN_1
set group address trust Trust_LAN add Trust_LAN_2
set group address trust Trust_LAN add Trust_LAN_3
set group address trust Trust_LAN add Trust_LAN_4
set group address trust Trust_LAN add Trust_LAN_5
set group address trust Trust_LAN add Trust_LAN_6
set group address trust Trust_LAN add Trust_LAN_7
set group address untrust side_2 add side_2_1
set group address untrust side_2 add side_2_2
set group address untrust side_2 add side_2_3
set group address untrust side_2 add side_2_4
set group address untrust side_2 add side_2_5
set group address untrust side_2 add side_2_6
set group address untrust side_2 add side_2_7
```

```
set policy id 0 from untrust to trust side_2 Trust_LAN any permit log
set policy id 1 from trust to untrust Trust_LAN side_2 any permit log
```

Security Appliance #2:

```
set address trust Trust_LAN_1 x.x.x.127/25
set address trust Trust_LAN_2 x.x.x.191/26
set address trust Trust_LAN_3 x.x.x.223/27
set address trust Trust_LAN_4 x.x.x.239/28
set address trust Trust_LAN_5 x.x.x.247/29
set address trust Trust_LAN_6 x.x.x.251/30
```

```
set address trust Trust_LAN_7 x.x.x.253/31
set address untrust side_1_1 x.x.x.127/25
set address untrust side_1_2 x.x.x.191/26
set address untrust side_1_3 x.x.x.223/27
set address untrust side_1_4 x.x.x.239/28
set address untrust side_1_5 x.x.x.247/29
set address untrust side_1_6 x.x.x.251/30
set address untrust side_1_7 x.x.x.253/31
set group address trust Trust_LAN add Trust_LAN_1
set group address trust Trust_LAN add Trust_LAN_2
set group address trust Trust_LAN add Trust_LAN_3
set group address trust Trust_LAN add Trust_LAN_4
set group address trust Trust_LAN add Trust_LAN_5
set group address trust Trust_LAN add Trust_LAN_6
set group address trust Trust_LAN add Trust_LAN_7
set group address untrust side_1 add side_1_1
set group address untrust side_1 add side_1_2
set group address untrust side_1 add side_1_3
set group address untrust side_1 add side_1_4
set group address untrust side_1 add side_1_5
set group address untrust side_1 add side_1_6
set group address untrust side_1 add side_1_7
```

```
set policy id 0 from untrust to trust side_1 Trust_LAN any permit log
set policy id 1 from trust to untrust Trust_LAN side_1 any permit log
```

where, *Trust_LAN* is the internal address;

where, *side_1* and *side_2* are the external addresses; and

where, x.x.x is the first three values of the IP address for your network

Saving the Applied Configuration

The configuration should be saved to ensure 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 becomes misconfigured in a way that may lead to the security appliance to reach an inoperable or insecure state, the

following command should be executed 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, the following command should be executed:

exec config rollback

The remaining portion of this page was intentionally left blank

Evaluated Configuration Usage Guidance

- When the Security appliance is operating in Layer 2 (Authenticated Transparent) mode, 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 (Authenticated or Unauthenticated NAT/Route) mode. In Layer 3 mode, ARP packets are not passed through the device, but the packets will 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.
- The CLI is the only administration interface allowed in the evaluated configuration of the security appliances for Common Criteria EAL 4. A VT-100 terminal or a device that can emulate a VT-100 terminal is required to locally connect to the security appliances and access the CLI. The CLI only grants authorized administrators with access to issue any commands.
- 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.
- security appliances deployed for EAL4 conformance are assumed to be placed into environments where the threat of malicious attacks that are aimed at discovering exploitable vulnerabilities is considered low.
- 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
- Juniper Networks security appliances provide the functionality to block the download of HTTP components such as ActiveX components, Java components, executable files, and zip files. However, the evaluated configuration only

supports the blocking of executable and zip files. While the inclusion of ActiveX and Java blocking does not invalidate the evaluated configuration, these functionalities were not tested as part of the evaluation performed.

When an executable or zip file is blocked as a result of the command below, the file requested for download is replaced with an arbitrary file in place of the actual blocked file. The name of the replacement file is identical to the blocked file, but the replacement file contains text explaining that the file requested was blocked. In some internet browsers, such as Internet Explorer and Mozilla, this arbitrary file is opened within the browser and displays the text indicating the block within the browser window. While other browsers, such as Conqueror, prompt you to save the file first.

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 will show 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 Not Included in the Evaluated Configuration

The following commands along with their parameters are not included in the Common Criteria EAL4 evaluated configuration.

Command	Parameter
<ul style="list-style-type: none"> • address 	<ul style="list-style-type: none"> • fqdn
<ul style="list-style-type: none"> • admin 	<ul style="list-style-type: none"> • auth server • manager-ip • port • privilege • ssh • scs • telnet port
<ul style="list-style-type: none"> • alias 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • All 	<ul style="list-style-type: none"> • There is no parameter the command
<ul style="list-style-type: none"> • auth 	<ul style="list-style-type: none"> • default
<ul style="list-style-type: none"> • auth-server 	<ul style="list-style-type: none"> • account-type • backup1 backup2 • ldap • radius • secureid • timeout • type
<ul style="list-style-type: none"> • bgp 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • clock 	<ul style="list-style-type: none"> • ntp
<ul style="list-style-type: none"> • console 	<ul style="list-style-type: none"> • disable
<ul style="list-style-type: none"> • flow 	<ul style="list-style-type: none"> • allow-dns-reply • gre-in-tcp-mss • gre-out-tcp-mss • hub-n-spoke-mip • mac-flooding • no-tcp-seq-check
<ul style="list-style-type: none"> • ike 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • ike-cookie 	<ul style="list-style-type: none"> • All the parameters associated with the command

Command	Parameter
<ul style="list-style-type: none"> • interface 	<ul style="list-style-type: none"> • manage-ip • manage <ul style="list-style-type: none"> • ident-reset • nsmgmt • snmp • ssh • ssl • telnet • web • protocol • vip • vlan trunk • webauth • webauth-ip
<ul style="list-style-type: none"> • ippool 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • l2tp 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • Lcd 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • Log 	<ul style="list-style-type: none"> • destination • level
<ul style="list-style-type: none"> • modem 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • Nrtp 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • nsmgmt 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • Nsrp 	<ul style="list-style-type: none"> • active-active transparent
<ul style="list-style-type: none"> • ntp 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • ospf commands 	<ul style="list-style-type: none"> • All that associated with the command
<ul style="list-style-type: none"> • Pki 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • policy 	<ul style="list-style-type: none"> • default-permit-all • l2tp • schedule
<ul style="list-style-type: none"> • proxy-id 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • RIP commands 	<ul style="list-style-type: none"> • All that associated with the command
<ul style="list-style-type: none"> • Sa 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • sa-filter 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • sa-statistics 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • save 	<ul style="list-style-type: none"> • all-virtual-system
<ul style="list-style-type: none"> • scp 	<ul style="list-style-type: none"> • All the parameters associated with the command (i.e. enable or no parameter)
<ul style="list-style-type: none"> • snmp 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • Ssh 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • Ssl 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • timer 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • traffic-shaping 	<ul style="list-style-type: none"> • All the parameters associated with the command

Command	Parameter
<ul style="list-style-type: none"> • user 	<ul style="list-style-type: none"> • Dialup users (for using Manual Key VPNs) • Authentication users (for using network connections) • IKE users (for using AutoKey IKE VPNs) • L2TP users (for using L2TP tunnels) • XAUTH users
<ul style="list-style-type: none"> • Vpn 	<ul style="list-style-type: none"> • auto • sec-level
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • vsys 	<ul style="list-style-type: none"> • All the parameters associated with the command
<ul style="list-style-type: none"> • xauth 	<ul style="list-style-type: none"> • All the parameters associated with the command

The remaining portion of this page was intentionally left blank

Evaluated Configuration Examples

The following examples are provided to demonstrate the set of commands that are required to configure a security appliance within the evaluated configuration.

The following examples are based on NS-500 model.

Unauthenticated NAT/Route Mode

Security Appliance #1:

```
set common-criteria no-internal-commands
set clock 07/29/2005 12:25
set admin password restrict length 8
set admin name RootAdmin
set admin password RootPass
unset interface mgt ip
set interface eth1/1 zone trust
set interface eth1/1 ip 192.168.100.1/24
unset interface eth1/1 manage
set interface eth3/1 zone untrust
set interface eth3/1 ip 10.155.38.15/24
set address trust trust_lan 192.168.100.1/24
set address untrust untrust_lan 10.155.38.15/24
set policy id 0 from untrust to trust untrust_lan trust_lan any permit log count
set policy id 1 from trust to untrust trust_lan untrust_lan any permit log count
set policy id 98 from untrust to trust any any any deny log count
set policy id 99 from trust to untrust any any any deny log count
set syslog config 192.168.100.100 facilities local0 local0
set syslog config 192.168.100.100 port 514
set syslog config 192.168.100.100 log traffic
set syslog enable
set log module system level emergency destination syslog
set log module system level alert destination syslog
set log module system level critical destination syslog
set log module system level error destination syslog
set log module system level warning destination syslog
set log audit-loss-mitigation
set firewall log-self
set zone trust screen block-frag
set zone trust screen component-block
set zone trust screen fin-no-ack
```

set zone trust screen icmp-flood
set zone trust screen icmp-fragment
set zone trust screen icmp-large
set zone trust screen ip-bad-option
set zone trust screen ip-loose-src-route
set zone trust screen ip-record-route
set zone trust screen ip-security-opt
set zone trust screen ip-spoofing
set zone trust screen ip-spoofing drop-no-rpf-route
set zone trust screen ip-stream-opt
set zone trust screen ip-strict-src-route
set zone trust screen ip-sweep
set zone trust screen ip-timestamp-opt
set zone trust screen land
set zone trust screen limit-session
set zone trust screen mal-url code-red
set zone trust screen ping-death
set zone trust screen syn-ack-ack-proxy
set zone trust screen syn-fin
set zone trust screen syn-flood
set zone trust screen syn-frag
set zone trust screen tcp-no-flag
set zone trust screen tear-drop
set zone trust screen udp-flood
set zone trust screen unknown-protocol
set zone trust screen winnuke
set zone untrust screen block-frag
set zone untrust screen component-block
set zone untrust screen fin-no-ack
set zone untrust screen icmp-flood
set zone untrust screen icmp-fragment
set zone untrust screen icmp-large
set zone untrust screen ip-bad-option
set zone untrust screen ip-loose-src-route
set zone untrust screen ip-record-route
set zone untrust screen ip-security-opt
set zone untrust screen ip-spoofing
set zone untrust screen ip-spoofing drop-no-rpf-route
set zone untrust screen ip-stream-opt
set zone untrust screen ip-strict-src-route
set zone untrust screen ip-sweep
set zone untrust screen ip-timestamp-opt
set zone untrust screen land
set zone untrust screen limit-session
set zone untrust screen mal-url code-red
set zone untrust screen ping-death

```
set zone untrust screen syn-ack-ack-proxy
set zone untrust screen syn-fin
set zone untrust screen syn-flood
set zone untrust screen syn-frag
set zone untrust screen tcp-no-flag
set zone untrust screen tear-drop
set zone untrust screen udp-flood
set zone untrust screen unknown-protocol
set zone untrust screen winnuke
save
save config to last-known-good
```

Authenticated NAT/Route Mode

Security Appliance #1:

```
set common-criteria no-internal-commands
set clock 07/29/2005 12:25
set admin password restrict length 8
set admin name RootAdmin
set admin password RootPass
unset interface mgt ip
set interface eth1/1 zone trust
set interface eth1/1 ip 10.1.1.1/24
unset interface eth1/1 manage
set interface eth3/1 zone untrust
set interface eth3/1 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface eth3/1
set address trust Trust_LAN_1 10.1.1.127/25
set address trust Trust_LAN_2 10.1.1.191/26
set address trust Trust_LAN_3 10.1.1.223/27
set address trust Trust_LAN_4 10.1.1.239/28
set address trust Trust_LAN_5 10.1.1.247/29
set address trust Trust_LAN_6 10.1.1.251/30
set address trust Trust_LAN_7 10.1.1.253/31
set address untrust side_2_1 10.2.2.127/25
set address untrust side_2_2 10.2.2.191/26
set address untrust side_2_3 10.2.2.223/27
set address untrust side_2_4 10.2.2.239/28
set address untrust side_2_5 10.2.2.247/29
set address untrust side_2_6 10.2.2.251/30
set address untrust side_2_7 10.2.2.253/31
set group address trust Trust_LAN add Trust_LAN_1
```

```
set group address trust Trust_LAN add Trust_LAN_2
set group address trust Trust_LAN add Trust_LAN_3
set group address trust Trust_LAN add Trust_LAN_4
set group address trust Trust_LAN add Trust_LAN_5
set group address trust Trust_LAN add Trust_LAN_6
set group address trust Trust_LAN add Trust_LAN_7
set group address untrust side_2 add side_2_1
set group address untrust side_2 add side_2_2
set group address untrust side_2 add side_2_3
set group address untrust side_2 add side_2_4
set group address untrust side_2 add side_2_5
set group address untrust side_2 add side_2_6
set group address untrust side_2 add side_2_7
set vpn 1-to-2 manual 3020 3030 gateway 2.2.2.2 outgoing-interface eth3/1 esp 3des
password asdlk24234 auth sha-1 password PNAS134a
set vpn 1-to-2 bind interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface eth3/1 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set policy id 0 from untrust to trust side_2 Trust_LAN any permit log count
set policy id 1 from trust to untrust Trust_LAN side_2 any permit log count
set policy id 98 from untrust to trust any any any deny log count
set policy id 99 from trust to untrust any any any deny log count
set syslog config 10.1.1.10 facilities local0 local0
set syslog config 10.1.1.10 port 514
set syslog config 10.1.1.10 log traffic
set syslog enable
set log module system level emergency destination syslog
set log module system level alert destination syslog
set log module system level critical destination syslog
set log module system level error destination syslog
set log module system level warning destination syslog
set log audit-loss-mitigation
set firewall log-self
set zone trust screen block-frag
set zone trust screen component-block
set zone trust screen fin-no-ack
set zone trust screen icmp-flood
set zone trust screen icmp-fragment
set zone trust screen icmp-large
set zone trust screen ip-bad-option
set zone trust screen ip-loose-src-route
set zone trust screen ip-record-route
set zone trust screen ip-security-opt
set zone trust screen ip-spoofing
set zone trust screen ip-spoofing drop-no-rpf-route
set zone trust screen ip-stream-opt
```

```
set zone trust screen ip-strict-src-route
set zone trust screen ip-sweep
set zone trust screen ip-timestamp-opt
set zone trust screen land
set zone trust screen limit-session
set zone trust screen mal-url code-red
set zone trust screen ping-death
set zone trust screen syn-ack-ack-proxy
set zone trust screen syn-fin
set zone trust screen syn-flood
set zone trust screen syn-frag
set zone trust screen tcp-no-flag
set zone trust screen tear-drop
set zone trust screen udp-flood
set zone trust screen unknown-protocol
set zone trust screen winnuke
set zone untrust screen block-frag
set zone untrust screen component-block
set zone untrust screen fin-no-ack
set zone untrust screen icmp-flood
set zone untrust screen icmp-fragment
set zone untrust screen icmp-large
set zone untrust screen ip-bad-option
set zone untrust screen ip-loose-src-route
set zone untrust screen ip-record-route
set zone untrust screen ip-security-opt
set zone untrust screen ip-spoofing
set zone untrust screen ip-spoofing drop-no-rpf-route
set zone untrust screen ip-stream-opt
set zone untrust screen ip-strict-src-route
set zone untrust screen ip-sweep
set zone untrust screen ip-timestamp-opt
set zone untrust screen land
set zone untrust screen limit-session
set zone untrust screen mal-url code-red
set zone untrust screen ping-death
set zone untrust screen syn-ack-ack-proxy
set zone untrust screen syn-fin
set zone untrust screen syn-flood
set zone untrust screen syn-frag
set zone untrust screen tcp-no-flag
set zone untrust screen tear-drop
set zone untrust screen udp-flood
set zone untrust screen unknown-protocol
set zone untrust screen winnuke
save
```

save config to last-known-good

Security Appliance #2:

```
set common-criteria no-internal-commands
set clock 07/29/2005 12:25
set admin password restrict length 8
set admin name RootAdmin
set admin password RootPass
set common-criteria no-internal-commands
unset interface mgt ip
set interface eth1/1 zone trust
set interface eth1/1 ip 10.2.2.1/24
unset interface eth1/1 manage
set interface eth3/1 zone untrust
set interface eth3/1 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface eth3/1
set address trust Trust_LAN_1 10.2.2.127/25
set address trust Trust_LAN_2 10.2.2.191/26
set address trust Trust_LAN_3 10.2.2.223/27
set address trust Trust_LAN_4 10.2.2.239/28
set address trust Trust_LAN_5 10.2.2.247/29
set address trust Trust_LAN_6 10.2.2.251/30
set address trust Trust_LAN_7 10.2.2.253/31
set address untrust side_1_1 10.1.1.127/25
set address untrust side_1_2 10.1.1.191/26
set address untrust side_1_3 10.1.1.223/27
set address untrust side_1_4 10.1.1.239/28
set address untrust side_1_5 10.1.1.247/29
set address untrust side_1_6 10.1.1.251/30
set address untrust side_1_7 10.1.1.253/31
set group address trust Trust_LAN add Trust_LAN_1
set group address trust Trust_LAN add Trust_LAN_2
set group address trust Trust_LAN add Trust_LAN_3
set group address trust Trust_LAN add Trust_LAN_4
set group address trust Trust_LAN add Trust_LAN_5
set group address trust Trust_LAN add Trust_LAN_6
set group address trust Trust_LAN add Trust_LAN_7
set group address untrust side_1 add side_1_1
set group address untrust side_1 add side_1_2
set group address untrust side_1 add side_1_3
set group address untrust side_1 add side_1_4
set group address untrust side_1 add side_1_5
set group address untrust side_1 add side_1_6
set group address untrust side_1 add side_1_7
```

```
set vpn 2-to-1 manual 3030 3020 gateway 1.1.1.1 outgoing-interface e3/1 esp 3des
password asdlk24234 auth sha-1 password PNAS134a
set vpn 2-to-1 bind interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface e3/1 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set policy id 0 from untrust to trust side_1 Trust_LAN any permit log count
set policy id 1 from trust to untrust Trust_LAN side_1 any permit log count
set policy id 98 from untrust to trust any any any deny log count
set policy id 99 from trust to untrust any any any deny log count
set syslog config 10.2.2.9 facilities local0 local0
set syslog config 10.2.2.9 port 514
set syslog config 10.2.2.9 log traffic
set syslog enable
set log module system level emergency destination syslog
set log module system level alert destination syslog
set log module system level critical destination syslog
set log module system level error destination syslog
set log module system level warning destination syslog
set log audit-loss-mitigation
set firewall log-self
set zone trust screen block-frag
set zone trust screen component-block
set zone trust screen fin-no-ack
set zone trust screen icmp-flood
set zone trust screen icmp-fragment
set zone trust screen icmp-large
set zone trust screen ip-bad-option
set zone trust screen ip-loose-src-route
set zone trust screen ip-record-route
set zone trust screen ip-security-opt
set zone trust screen ip-spoofing
set zone trust screen ip-spoofing drop-no-rpf-route
set zone trust screen ip-stream-opt
set zone trust screen ip-strict-src-route
set zone trust screen ip-sweep
set zone trust screen ip-timestamp-opt
set zone trust screen land
set zone trust screen limit-session
set zone trust screen mal-url code-red
set zone trust screen ping-death
set zone trust screen syn-ack-ack-proxy
set zone trust screen syn-fin
set zone trust screen syn-flood
set zone trust screen syn-frag
set zone trust screen tcp-no-flag
set zone trust screen tear-drop
```

```
set zone trust screen udp-flood
set zone trust screen unknown-protocol
set zone trust screen winnuke
set zone untrust screen block-frag
set zone untrust screen component-block
set zone untrust screen fin-no-ack
set zone untrust screen icmp-flood
set zone untrust screen icmp-fragment
set zone untrust screen icmp-large
set zone untrust screen ip-bad-option
set zone untrust screen ip-loose-src-route
set zone untrust screen ip-record-route
set zone untrust screen ip-security-opt
set zone untrust screen ip-spoofing
set zone untrust screen ip-spoofing drop-no-rpf-route
set zone untrust screen ip-stream-opt
set zone untrust screen ip-strict-src-route
set zone untrust screen ip-sweep
set zone untrust screen ip-timestamp-opt
set zone untrust screen land
set zone untrust screen limit-session
set zone untrust screen mal-url code-red
set zone untrust screen ping-death
set zone untrust screen syn-ack-ack-proxy
set zone untrust screen syn-fin
set zone untrust screen syn-flood
set zone untrust screen syn-frag
set zone untrust screen tcp-no-flag
set zone untrust screen tear-drop
set zone untrust screen udp-flood
set zone untrust screen unknown-protocol
set zone untrust screen winnuke
save
save config to last-known-good
```

Authenticated Transparent Mode

Security Appliance #1:

```
set common-criteria no-internal-commands
set clock 07/29/2005 12:25
set admin password restrict length 8
set admin name RootAdmin
set admin password RootPass
```

```
unset interface mgt ip
unset interface eth1/1 ip
unset interface eth1/1 zone
unset interface eth1/2 ip
unset interface eth1/2 zone
unset interface eth2/1 ip
unset interface eth2/1 zone
unset interface eth2/2 ip
unset interface eth2/2 zone
unset interface eth3/1 ip
unset interface eth3/1 zone
unset interface eth3/2 ip
unset interface eth3/2 zone
set interface eth1/1 zone v1-trust
unset interface eth1/1 manage
set interface eth3/1 zone v1-untrust
set interface vlan1 ip 1.1.1.1/24
unset interface vlan1 manage
set address v1-trust local_lan_1 1.1.1.127/25
set address v1-trust local_lan_2 1.1.1.191/26
set address v1-trust local_lan_3 1.1.1.223/27
set address v1-trust local_lan_4 1.1.1.239/28
set address v1-trust local_lan_5 1.1.1.247/29
set address v1-trust local_lan_6 1.1.1.251/30
set address v1-trust local_lan_7 1.1.1.253/31
set address v1-untrust peer_lan_1 2.2.2.127/25
set address v1-untrust peer_lan_2 2.2.2.191/26
set address v1-untrust peer_lan_3 2.2.2.223/27
set address v1-untrust peer_lan_4 2.2.2.239/28
set address v1-untrust peer_lan_5 2.2.2.247/29
set address v1-untrust peer_lan_6 2.2.2.251/30
set address v1-untrust peer_lan_7 2.2.2.253/31
set group address v1-trust local_lan add local_lan_1
set group address v1-trust local_lan add local_lan_2
set group address v1-trust local_lan add local_lan_3
set group address v1-trust local_lan add local_lan_4
set group address v1-trust local_lan add local_lan_5
set group address v1-trust local_lan add local_lan_6
set group address v1-trust local_lan add local_lan_7
set group address v1-untrust peer_lan add peer_lan_1
set group address v1-untrust peer_lan add peer_lan_2
set group address v1-untrust peer_lan add peer_lan_3
set group address v1-untrust peer_lan add peer_lan_4
set group address v1-untrust peer_lan add peer_lan_5
set group address v1-untrust peer_lan add peer_lan_6
set group address v1-untrust peer_lan add peer_lan_7
```

```
set vpn vpn1 manual 3020 3030 gateway 2.2.2.2 outgoing-zone v1-untrust esp aes256
password asdlk24234 auth sha-1 password PNAS134a
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250
set policy id 1 from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn vpn1 log
set policy id 2 from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn vpn1 log
set policy id 98 from untrust to trust any any any deny log count
set policy id 99 from trust to untrust any any any deny log count
set syslog config 1.1.1.10 facilities local0 local0
set syslog config 1.1.1.10 port 514
set syslog config 1.1.1.10 log traffic
set syslog enable
set log module system level emergency destination syslog
set log module system level alert destination syslog
set log module system level critical destination syslog
set log module system level error destination syslog
set log module system level warning destination syslog
set log audit-loss-mitigation
set firewall log-self
set zone v1-trust screen block-frag
set zone v1-trust screen component-block
set zone v1-trust screen fin-no-ack
set zone v1-trust screen icmp-flood
set zone v1-trust screen icmp-fragment
set zone v1-trust screen icmp-large
set zone v1-trust screen ip-bad-option
set zone v1-trust screen ip-loose-src-route
set zone v1-trust screen ip-record-route
set zone v1-trust screen ip-security-opt
set zone v1-trust screen ip-spoofing
set zone v1-trust screen ip-stream-opt
set zone v1-trust screen ip-strict-src-route
set zone v1-trust screen ip-sweep
set zone v1-trust screen ip-timestamp-opt
set zone v1-trust screen land
set zone v1-trust screen limit-session
set zone v1-trust screen mal-url code-red
set zone v1-trust screen ping-death
set zone v1-trust screen syn-ack-ack-proxy
set zone v1-trust screen syn-fin
set zone v1-trust screen syn-flood
set zone v1-trust screen syn-frag
set zone v1-trust screen tcp-no-flag
set zone v1-trust screen tear-drop
set zone v1-trust screen udp-flood
set zone v1-trust screen unknown-protocol
set zone v1-trust screen winnuke
```

```
set zone v1-untrust screen block-frag
set zone v1-untrust screen component-block
set zone v1-untrust screen fin-no-ack
set zone v1-untrust screen icmp-flood
set zone v1-untrust screen icmp-fragment
set zone v1-untrust screen icmp-large
set zone v1-untrust screen ip-bad-option
set zone v1-untrust screen ip-loose-src-route
set zone v1-untrust screen ip-record-route
set zone v1-untrust screen ip-security-opt
set zone v1-untrust screen ip-spoofing
set zone v1-untrust screen ip-stream-opt
set zone v1-untrust screen ip-strict-src-route
set zone v1-untrust screen ip-sweep
set zone v1-untrust screen ip-timestamp-opt
set zone v1-untrust screen land
set zone v1-untrust screen limit-session
set zone v1-untrust screen mal-url code-red
set zone v1-untrust screen ping-death
set zone v1-untrust screen syn-ack-ack-proxy
set zone v1-untrust screen syn-fin
set zone v1-untrust screen syn-flood
set zone v1-untrust screen syn-frag
set zone v1-untrust screen tcp-no-flag
set zone v1-untrust screen tear-drop
set zone v1-untrust screen udp-flood
set zone v1-untrust screen unknown-protocol
set zone v1-untrust screen winnuke
save
save config to last-known-good
reset
```

Security Appliance #2:

```
set common-criteria no-internal-commands
set clock 07/29/2005 12:25
set admin password restrict length 8
set admin name RootAdmin
set admin password RootPass
unset interface mgt ip
unset interface eth1/1 ip
unset interface eth1/1 zone
unset interface eth1/2 ip
unset interface eth1/2 zone
unset interface eth2/1 ip
unset interface eth2/1 zone
```

```
unset interface eth2/2 ip
unset interface eth2/2 zone
unset interface eth3/1 ip
unset interface eth3/1 zone
unset interface eth3/2 ip
unset interface eth3/2 zone
set interface eth1/1 zone v1-trust
set interface eth3/1 zone v1-untrust
set interface vlan1 ip 2.2.2.2/24
set address v1-trust local_lan_1 2.2.2.127/25
set address v1-trust local_lan_2 2.2.2.191/26
set address v1-trust local_lan_3 2.2.2.223/27
set address v1-trust local_lan_4 2.2.2.239/28
set address v1-trust local_lan_5 2.2.2.247/29
set address v1-trust local_lan_6 2.2.2.251/30
set address v1-trust local_lan_7 2.2.2.253/31
set address v1-untrust peer_lan_1 1.1.1.127/25
set address v1-untrust peer_lan_2 1.1.1.191/26
set address v1-untrust peer_lan_3 1.1.1.223/27
set address v1-untrust peer_lan_4 1.1.1.239/28
set address v1-untrust peer_lan_5 1.1.1.247/29
set address v1-untrust peer_lan_6 1.1.1.251/30
set address v1-untrust peer_lan_7 1.1.1.253/31
set group address v1-trust local_lan add local_lan_1
set group address v1-trust local_lan add local_lan_2
set group address v1-trust local_lan add local_lan_3
set group address v1-trust local_lan add local_lan_4
set group address v1-trust local_lan add local_lan_5
set group address v1-trust local_lan add local_lan_6
set group address v1-trust local_lan add local_lan_7
set group address v1-untrust peer_lan add peer_lan_1
set group address v1-untrust peer_lan add peer_lan_2
set group address v1-untrust peer_lan add peer_lan_3
set group address v1-untrust peer_lan add peer_lan_4
set group address v1-untrust peer_lan add peer_lan_5
set group address v1-untrust peer_lan add peer_lan_6
set group address v1-untrust peer_lan add peer_lan_7
set vpn vpn1 manual 3030 3020 gateway 1.1.1.1 outgoing-zone v1-untrust esp aes256
password asdlk24234 auth sha-1 password PNas134a
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 2.2.2.250
set policy id 1 from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn vpn1 log
set policy id 2 from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn vpn1 log
set policy id 98 from untrust to trust any any any deny log count
set policy id 99 from trust to untrust any any any deny log count
set syslog config 2.2.2.9 facilities local0 local0
set syslog config 2.2.2.9 port 514
```

```
set syslog config 2.2.2.9 log traffic
set syslog enable
set log module system level emergency destination syslog
set log module system level alert destination syslog
set log module system level critical destination syslog
set log module system level error destination syslog
set log module system level warning destination syslog
set log audit-loss-mitigation
set firewall log-self
set zone v1-trust screen block-frag
set zone v1-trust screen component-block
set zone v1-trust screen fin-no-ack
set zone v1-trust screen icmp-flood
set zone v1-trust screen icmp-fragment
set zone v1-trust screen icmp-large
set zone v1-trust screen ip-bad-option
set zone v1-trust screen ip-loose-src-route
set zone v1-trust screen ip-record-route
set zone v1-trust screen ip-security-opt
set zone v1-trust screen ip-spoofing
set zone v1-trust screen ip-stream-opt
set zone v1-trust screen ip-strict-src-route
set zone v1-trust screen ip-sweep
set zone v1-trust screen ip-timestamp-opt
set zone v1-trust screen land
set zone v1-trust screen limit-session
set zone v1-trust screen mal-url code-red
set zone v1-trust screen ping-death
set zone v1-trust screen syn-ack-ack-proxy
set zone v1-trust screen syn-fin
set zone v1-trust screen syn-flood
set zone v1-trust screen syn-frag
set zone v1-trust screen tcp-no-flag
set zone v1-trust screen tear-drop
set zone v1-trust screen udp-flood
set zone v1-trust screen unkown-protocol
set zone v1-trust screen winnuke
set zone v1-untrust screen block-frag
set zone v1-untrust screen component-block
set zone v1-untrust screen fin-no-ack
set zone v1-untrust screen icmp-flood
set zone v1-untrust screen icmp-fragment
set zone v1-untrust screen icmp-large
set zone v1-untrust screen ip-bad-option
set zone v1-untrust screen ip-loose-src-route
set zone v1-untrust screen ip-record-route
```

```
set zone v1-untrust screen ip-security-opt
set zone v1-untrust screen ip-spoofing
set zone v1-untrust screen ip-stream-opt
set zone v1-untrust screen ip-strict-src-route
set zone v1-untrust screen ip-sweep
set zone v1-untrust screen ip-timestamp-opt
set zone v1-untrust screen land
set zone v1-untrust screen limit-session
set zone v1-untrust screen mal-url code-red
set zone v1-untrust screen ping-death
set zone v1-untrust screen syn-ack-ack-proxy
set zone v1-untrust screen syn-fin
set zone v1-untrust screen syn-flood
set zone v1-untrust screen syn-frag
set zone v1-untrust screen tcp-no-flag
set zone v1-untrust screen tear-drop
set zone v1-untrust screen udp-flood
set zone v1-untrust screen unknown-protocol
set zone v1-untrust screen winnuke
save
save config to last-known-good
reset
```

The remaining portion of this page was intentionally left blank