

NetScreen Concept & Examples

ScreenOS Reference Guide

Volume 6: Virtual Systems



ScreenOS 4.0.0
P/N 093-0524-000
Rev. F

Copyright Notice

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

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

NetScreen Technologies, Inc.
350 Oakmead Parkway
Sunnyvale, CA 94085 U.S.A.
www.netscreen.com

FCC Statement

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

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

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

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

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

Disclaimer

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

Contents

Preface	iii	Dedicated Interfaces.....	12
Conventions	iv	Shared Interfaces.....	12
WebUI Navigation Conventions	iv	Importing and Exporting Physical Interfaces	15
Example: Objects > Addresses > List > New	iv	Example: Importing a Physical Interface	
CLI Conventions.....	v	to a Virtual System.....	15
Dependency Delimiters.....	v	Example: Exporting a Physical Interface	
Nested Dependencies	v	from a Virtual System.....	16
Availability of CLI Commands and Features	vi	VLAN-Based Traffic Classification	17
NetScreen Documentation	vii	VLANs.....	18
Chapter 1 Virtual Systems	1	Defining Subinterfaces and VLAN Tags.....	19
Creating a Vsys Object	3	Example: Defining Three Subinterfaces	
Example: Creating Vsys Objects and Vsys		and VLAN Tags	21
Admins.....	3	Communicating between VLANs.....	24
Virtual Routers	6	Example: InterVLAN Communication	24
Zones	7	IP-Based Traffic Classification	28
Interfaces.....	7	Example: Configuring IP-Based Traffic	
Traffic Sorting	9	Classification.....	30
Traffic Destined for the NetScreen Device	9	Logging On as a Vsys Admin	33
Through Traffic	10	Example: Logging On and Changing Your	
Dedicated and Shared Interfaces.....	12	Password	33
		Index.....	IX-I

Preface

You can logically partition a single NetScreen security system into multiple virtual systems to provide multi-tenant services. Each virtual system (vsys) is a unique security domain and can be managed by its own administrators (called “virtual system administrators” or “vsys admins”) who can individualize their security domain by setting their own address books, user lists, custom services, VPNs, and policies.

Volume 6, “Virtual Systems” describes virtual systems, dedicated and shared interfaces, and VLAN-based and IP-based traffic classification. This volume also describes how to create a vsys (you must have root-level administrator privilege) and define vsys admins.

CONVENTIONS

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

WebUI Navigation Conventions

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

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

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

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

CLI Conventions

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

Dependency Delimiters

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

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

Nested Dependencies

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

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

The delimiters [and] surround the entire clause. Consequently, you can omit **feature_1**, **feature_2**, and **feature_3**, and still execute the command successfully. However, because the { and } delimiters surround **feature_2** and **feature_3**, you must include either **feature_2** or **feature_3** if you include **feature_1**. Otherwise, you cannot successfully execute the command.

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

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

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

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

Availability of CLI Commands and Features

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

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

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

NETSCREEN DOCUMENTATION

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

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

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

techpubs@netscreen.com

Virtual Systems

You can logically partition a single NetScreen security system¹ into multiple virtual systems to provide multi-tenant services. Each virtual system (vsys) is a unique security domain and can have its own administrators (called “virtual system administrators” or “vsys admins”) who can individualize their security domain by setting their own address books, user lists, custom services, VPNs, and policies (although only a root-level administrator can set firewall security options, create virtual system administrators, and define interfaces and subinterfaces).

Note: For more information on the various levels of administration that NetScreen supports, see “Levels of Administration” on page 3-27.

NetScreen virtual systems support two kinds of traffic classifications: VLAN-based and IP-based, both of which can function exclusively or concurrently. This chapter discusses the following concepts and implementation of virtual systems:

- “Creating a Vsys Object” on page 3
 - “Virtual Routers” on page 6
 - “Zones” on page 7
 - “Interfaces” on page 7
- “Traffic Sorting” on page 9
 - “Traffic Destined for the NetScreen Device” on page 9
 - “Through Traffic” on page 10
 - “Dedicated and Shared Interfaces” on page 12
 - “Importing and Exporting Physical Interfaces” on page 15

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

- “VLAN-Based Traffic Classification” on page 17
 - “VLANs” on page 18
 - “Defining Subinterfaces and VLAN Tags” on page 19
 - “Communicating between VLANs” on page 24
- “IP-Based Traffic Classification” on page 28
- “Logging On as a Vsys Admin” on page 33

CREATING A VSYS OBJECT

The root administrator or root-level read/write admin must complete the following tasks to create a vsys object:

- Define a virtual system
- (Optional) Define one or more vsys admins²

After creating a vsys object, the root-level admin needs to perform other configurations to make it a functional vsys. He must configure subinterfaces or interfaces for the vsys, and possibly shared virtual routers and shared security zones. The subsequent configurations depend on whether the vsys is intended to support VLAN-based or IP-based traffic classifications, or a combination of both. After completing these configurations, the root-level administrator can then exit the virtual system and allow a vsys admin, if defined, to log on and begin configuring addresses, users, services, VPNs, and policies.

Example: Creating Vsys Objects and Vsys Admins

In this example, as a root-level admin, you create three vsys objects: vsys1, vsys2, vsys3. For vsys1, you create vsys admin Alice with password wLEaS1v1³. For vsys2, you create vsys admin Bob with password pjF56Ms2. For vsys3, there is no vsys admin.

Note: Vsys names, admin names, and passwords are case-sensitive. Vsys “abc” is different from vsys “ABC.”

After you create a vsys through the WebUI, you remain at the root level. Entering the newly created vsys requires a separate step:

Vsys: Click **Enter** (for the virtual system you want to enter).

The WebUI pages of the vsys you have entered appear, with the name of the vsys above the central display area—Vsys:*Name*.

-
2. A root-level administrator can define one vsys admin with read-write privileges and one vsys admin with read-only privileges per vsys.
 3. Only a root-level administrator can create a vsys admin's profile (user name and password). Because the NetScreen device uses the user name to determine the vsys to which a user belongs, a vsys admin cannot change his or her user name. However, a vsys admin can (and should) change his or her password.

When you create a vsys through the CLI, you immediately enter the system that you have just created. (To enter an existing vsys from the root level, use the **enter vsys name_str** command.) When you enter a vsys, note that the CLI command prompt changes to include the name of the system in which you are now issuing commands.

WebUI

1. Vsys > New: Enter the following, and then click **OK**:
 - VSYS Name: vsys1
 - VSYS Admin Name: Alice
 - VSYS Admin Password: wIEaS1v1
 - Confirm Password: wIEaS1v1
2. Vsys > New: Enter the following, and then click **OK**:
 - VSYS Name: vsys2
 - VSYS Admin Name: Bob
 - VSYS Admin Password: pjF56Ms2
 - Confirm Password: pjF56Ms2
3. Vsys > New: Enter the following, and then click **OK**:
 - VSYS Name: vsys3

CLI

1. ns-> set vsys vsys1
2. ns(vsys1)-> set admin name Alice
3. ns(vsys1)-> set admin password wIEaS1v1
4. ns(vsys1)-> save⁴
5. ns(vsys1)-> exit
6. ns-> set vsys vsys2
7. ns(vsys2)-> set admin name Bob
8. ns(vsys2)-> set admin password pjF56Ms2
9. ns(vsys2)-> save
10. ns(vsys2)-> exit
11. ns-> set vsys vsys3
12. ns(vsys3)-> save

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

Virtual Routers

When a root-level admin creates a vsys object, the vsys automatically has the following virtual routers available for its use:

- All shared root-level virtual routers, such as the untrust-vr

In the same way that a vsys and the root system share the Untrust zone, they also share the untrust-vr, and any other virtual routers defined at the root level as sharable.

- Its own virtual router

By default, a vsys-level virtual router is named *vsysname-vr*. You can also customize its name to make it more meaningful. This is a vsys-specific virtual router that, by default, maintains the routing table for the Trust-*vsysname* zone. All vsys-level virtual routers are non-sharable.

You can select any shared virtual router or the vsys-level virtual router as the default virtual router for a vsys. To change the default virtual router, enter a vsys and use the following CLI command: **set vrouter name default-vrouter**.

If you, as a root-level administrator, want all of the vsys zones to be in the untrust-vr routing domain—for example, if all the interfaces bound to the Trust -*vsysname* zone are in Route mode—you can dispense with the *vsysname-vr* by changing the vsys-level security zone bindings from the *vsysname-vr* to the untrust-vr. For more information on virtual routers, see “Routing and Virtual Routers” on page 2-51.

Note: *This release of ScreenOS does not support user-defined virtual routers within a virtual system.*

Zones

When a root-level admin creates a vsys object, the following zones are automatically inherited or created:

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

A vsys shares the Untrust and Null zones with the root system. All other zones in a vsys belong to that vsys.

Note: For information on each of these zone types, see “Zones” on page 2-29.

Interfaces

A vsys can support the following three kinds of interfaces for their Untrust and Trust zones:

Untrust Zone Interface Types

- Dedicated Physical Interface
- Subinterface (with VLAN tagging as a means for trunking* inbound and outbound traffic)
- Shared Interface (physical, subinterface, redundant interface, aggregate interface) with Root System

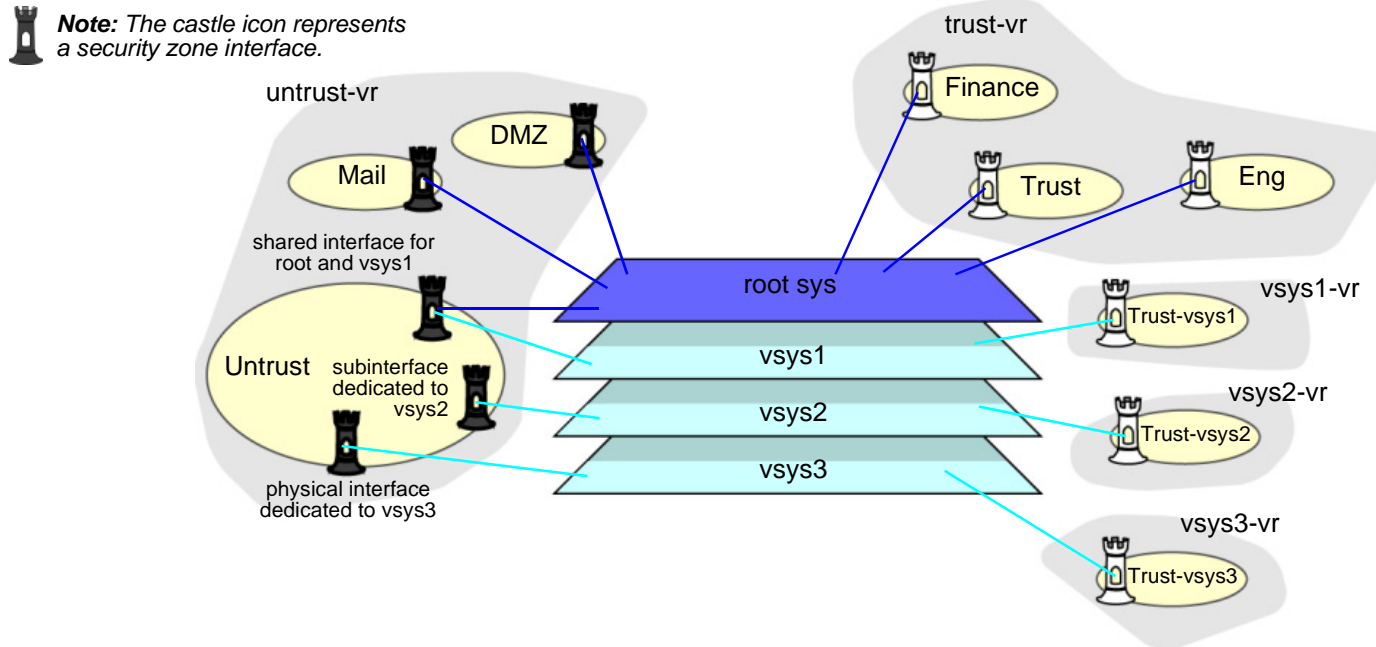
Trust Zone Interface Types

- Dedicated Physical Interface
- Subinterface (with VLAN tagging)
- Shared Physical Interface with Root System (and IP-based traffic classification†)

* For information about VLAN tagging and trunking concepts, see “VLANs” on page 18.

† For more information about IP-based traffic classification, see “IP-Based Traffic Classification” on page 28.

You can bind one, two, or all three of the above interface types to a security zone concurrently. You can also bind multiple interfaces of each type to a zone.



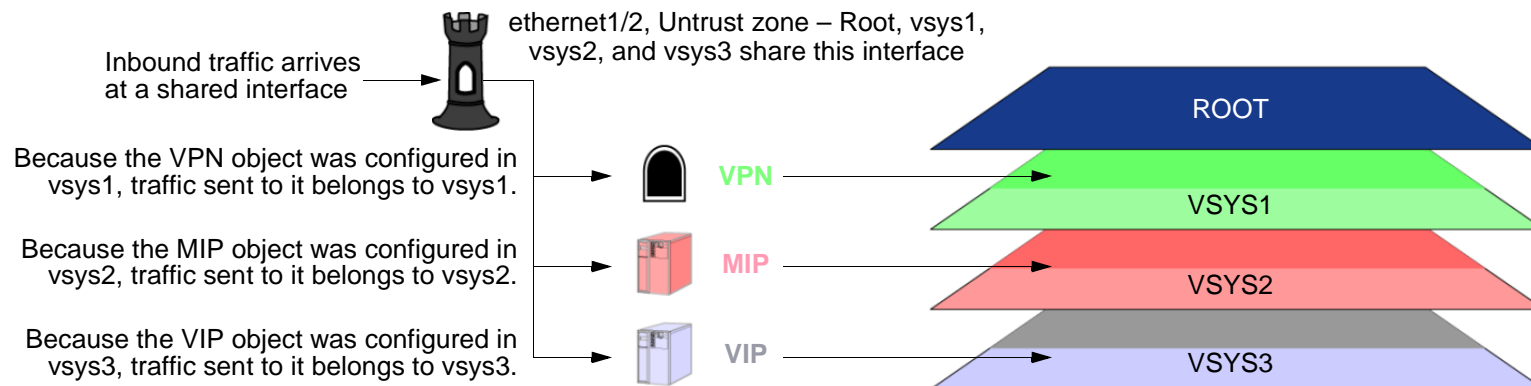
TRAFFIC SORTING

The NetScreen device must sort every packet it receives for delivery to the proper system. A NetScreen device receives two kinds of user traffic, which it sorts in two different ways:

- Traffic destined for an IP address on the device itself, such as encrypted VPN traffic and traffic destined for a MIP or VIP
- Traffic destined for an IP address beyond the device

Traffic Destined for the NetScreen Device

For traffic destined for an object (VPN, MIP, or VIP) on the NetScreen device, the device determines the system to which the traffic belongs through the association of the object with the system in which it was configured.



Inbound traffic can also reach a vsys via VPN tunnels; however, if the outgoing interface is a shared interface, you cannot create an AutoKey IKE VPN tunnel for a vsys and the root system to the same remote site.

Through Traffic

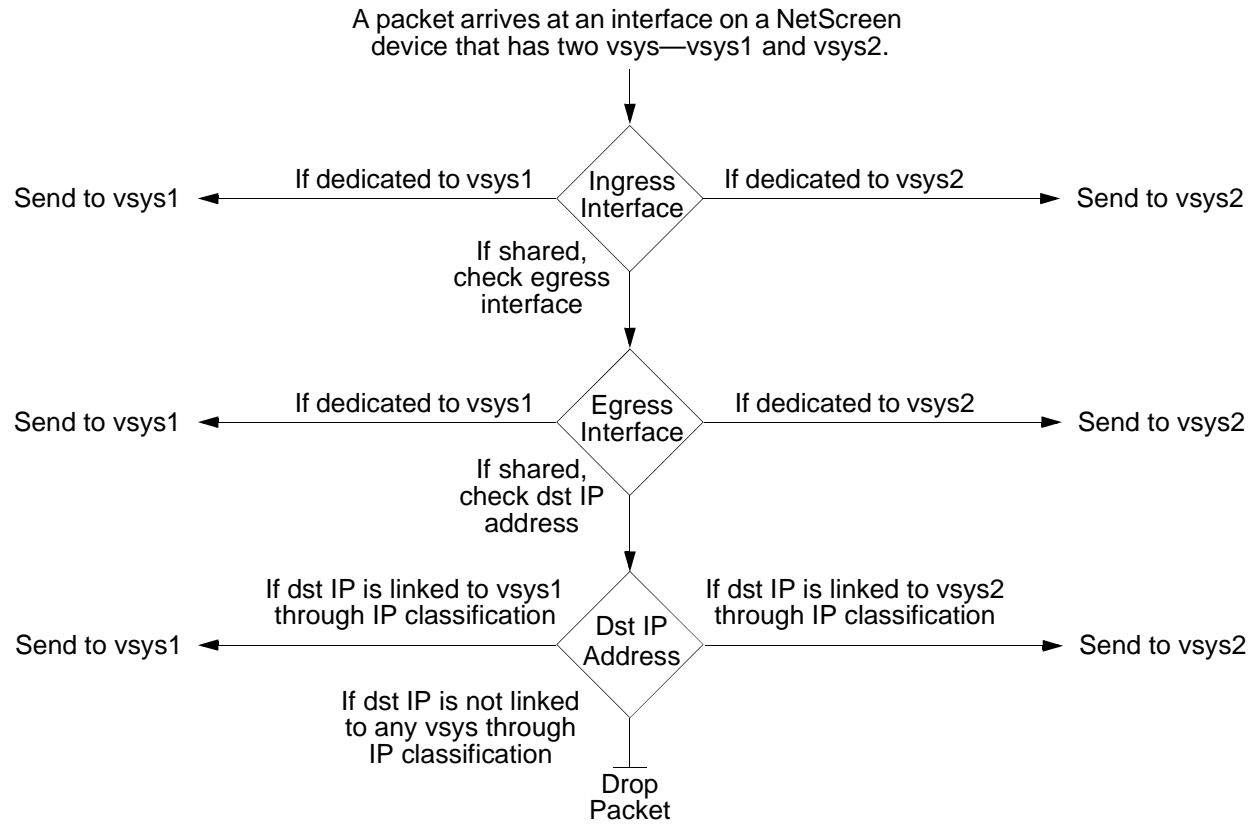
For traffic destined for an IP address beyond the NetScreen device (also known as “through traffic”), the device uses techniques made possible by VLAN-based and IP-based traffic classifications. VLAN-based traffic classification uses VLAN tags⁵ in frame headers to identify the system to which inbound traffic belongs. IP-based traffic classification uses the destination IP address in IP packet headers to identify the system to which inbound traffic belongs.

The procedure that the NetScreen device uses to determine the system to which a packet belongs progresses in the following order:

1. If the ingress interface is a dedicated⁶ interface, the NetScreen device associates the traffic with the system to which the interface is dedicated.
2. If the ingress interface is a shared interface, the NetScreen device checks if the egress interface is shared or dedicated.
3. If the egress interface is dedicated, the NetScreen device associates the traffic with the system to which the interface is dedicated.
4. If both the ingress and egress interfaces are shared, then the NetScreen associates the traffic to the system to which the destination IP address is bound.

5. VLAN tagging requires the use of subinterfaces. A subinterface must be dedicated to a system, in contrast to a shared interface, which is shared by all systems.

6. For more information about shared and dedicated interfaces, see [“Dedicated and Shared Interfaces” on page 12](#).



Dedicated and Shared Interfaces

There are two kinds of interfaces that affect how a NetScreen device can correctly sort inbound traffic to the right system: dedicated and shared.

Dedicated Interfaces

A system—virtual and root—can have multiple interfaces or subinterfaces dedicated exclusively to its own use. Such interfaces are not sharable by other systems. You can dedicate an interface to a system as follows:

- When you configure a physical interface, subinterface, redundant interface, or aggregate interface in the root system and bind it to a non-sharable zone, that interface remains dedicated to the root system.
- When you import a physical or aggregate interface into a vsys and bind it to either the shared Untrust zone or the Trust-*vsys_name* zone, that interface becomes a dedicated interface for that vsys.
- When you configure a subinterface in a vsys, it belongs to that vsys.

Note: When a system has a dedicated subinterface, the NetScreen device must employ VLAN-based traffic classification to properly sort inbound traffic.

Shared Interfaces

A system—virtual and root—can share an interface with another system. For an interface to be sharable, you must configure it at the root level and bind it to a shared zone in a shared virtual router. By default, the predefined untrust-vr is a shared virtual router, and the predefined Untrust zone is a shared zone. Consequently, a vsys can share any root-level physical interface, subinterface, redundant interface, or aggregate interface that you bind to the Untrust zone.

To create a shared interface in a zone other than the Untrust zone, you must define the zone as a shared zone at the root level. To do that, the zone must be in a shared virtual router, such as the untrust-vr or any other root-level virtual router that you define as sharable. Then, when you bind a root-level interface to the shared zone, it automatically becomes a shared interface.

Note: To create a virtual router, you need to obtain a vsys license key, which provides you with the ability to define virtual systems, virtual routers, and security zones for use either in a vsys or in the root system.

A shared virtual router can support both shared and non-sharable root-level security zones. You can define a root-level zone bound to a shared virtual router as sharable or not. Any root-level zone that you bind to a shared virtual router and define as sharable becomes a shared zone, available for use by virtual systems too. Any root-level zone that you bind to a shared virtual router and define as non-sharable remains a dedicated zone for use by the root system alone. If you bind a vsys-level zone to either the virtual router dedicated to that vsys or to a shared virtual router created in the root system, the zone remains a dedicated zone, available for use only by the vsys for which you created it.

A shared zone can support both shared and dedicated interfaces. Any root-level interface that you bind to a shared zone becomes a shared interface, available for use by virtual systems also. Any vsys-level interface that you bind to a shared zone remains a dedicated interface, available for use only by the vsys for which you created it.

A non-sharable zone can only be used by the system in which you created it and can only support dedicated interfaces for that system. All vsys-level zones are non-sharable.

To create a shared interface, you must create a shared virtual router (or use the predefined untrust-vr), create a shared security zone (or use the predefined Untrust zone), and then bind the interface to the shared zone. You must do all three steps in the root system.

The options in the WebUI and CLI are as follows:

1. To create a shared virtual router:

WebUI

Network > Routing > Virtual Routers > New: Select the **Shared and accessible by other vsys** option, and then click **Apply**.

CLI

```
set vrouter name name_str
```

```
set vrouter name_str shared
```

(You cannot modify an existing shared virtual router to make it unshared unless you first delete all virtual systems. However, you can modify a virtual router from unshared to shared at any time.)

2. To create a shared zone, do the following at the root level:

WebUI

Note: At the time of this release, you can only define a shared zone through the CLI.

CLI

```
set zone name name_str
```

```
set zone zone vrouter sharable_vr_name_str
```

```
set zone zone shared
```

3. To create a shared interface, do the following at the root level:

WebUI

Network > Interfaces > New (or Edit for an existing interface): Configure the interface and bind it to a shared zone, and then click **OK**.

CLI

```
set interface interface zone shared_zone_name_str
```

When two or more systems share an interface, the NetScreen device must employ IP-based traffic classification to properly sort inbound traffic. (For more information about IP-based traffic classification, including an example showing how to configure it for several vsys, see [“IP-Based Traffic Classification” on page 28.](#))

Importing and Exporting Physical Interfaces

You can dedicate one or more physical interfaces to a vsys. In effect, you import a physical interface from the root system to a virtual system. After importing a physical interface to a vsys, the vsys has exclusive use of it.

Note: Before you can import an interface to a virtual system, it must be in the Null zone at the root level.

Example: Importing a Physical Interface to a Virtual System

In this example, you import the physical interface ethernet4/1 to vsys1. You bind it to the Untrust zone and assign it the IP address 210.1.1.1/24.

WebUI

1. Vsys: Click **Enter** (for vsys1).
2. Network > Interfaces: Click **Import** (for ethernet4/1).
3. Network > Interfaces > Edit (for ethernet4/1): Enter the following, and then click **OK**:
Zone Name: Untrust-vsys1
IP Address/Netmask: 210.1.1.1/24
4. Click the **Exit Vsys** button (at the bottom of the menu column) to return to the root level.

CLI

1. ns-> enter vsys vsys1
2. ns(vsys1)-> set interface ethernet4/1 import
3. ns(vsys1)-> set interface ethernet4/1 zone untrust-vsys1
4. ns(vsys1)-> set interface ethernet4/1 ip 210.1.1.1/24
5. ns(vsys1)-> save
6. ns(vsys1)-> exit

Example: Exporting a Physical Interface from a Virtual System

In this example, you bind the physical interface ethernet4/1 to the Null zone in vsys1 and assign it the IP address 0.0.0.0/0. Then you export interface ethernet4/1 to the root system.

WebUI

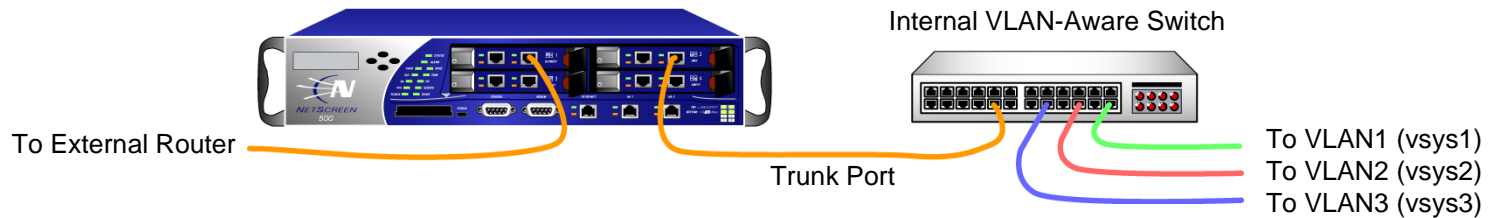
1. Vsys: Click **Enter** (for vsys1).
2. Network > Interfaces > Edit (for ethernet4/1): Enter the following, and then click **OK**:
Zone Name: Null
IP Address/Netmask: 0.0.0.0/0
3. Network > Interfaces: Click **Export** (for ethernet4/1).
Interface ethernet4/1 is now available for use in the root system.
4. Click the **Exit Vsys** button (at the bottom of the menu column) to return to the root level.

CLI

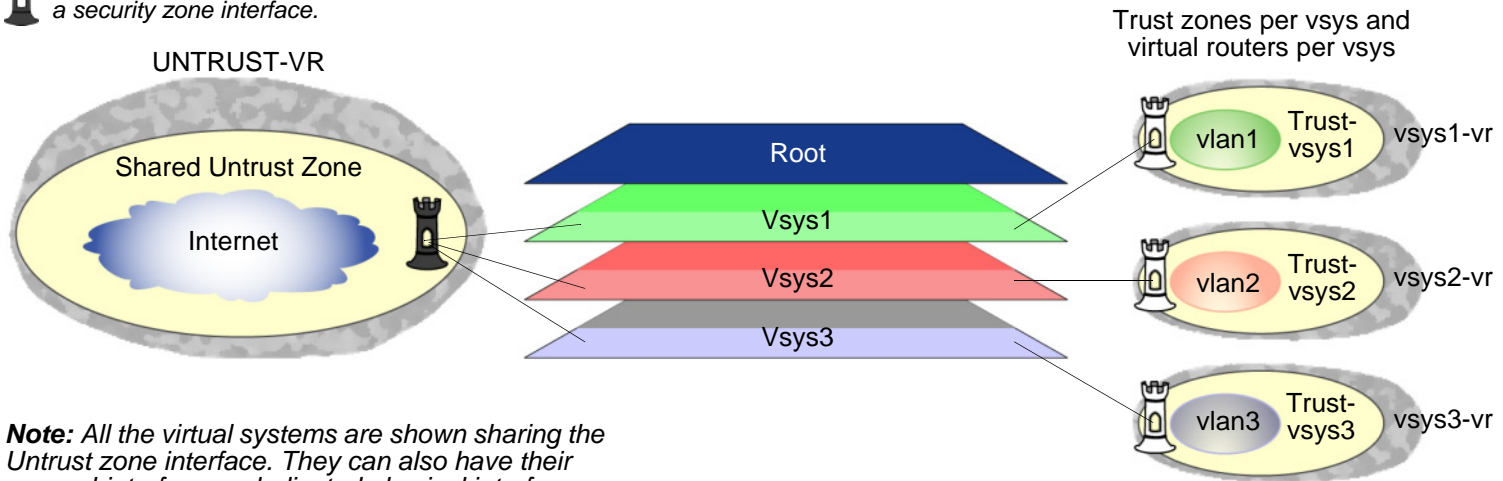
1. ns-> enter vsys vsys1
2. ns(vsys1)-> set interface ethernet4/1 ip 0.0.0.0/0
3. ns(vsys1)-> set interface ethernet4/1 zone null
4. ns(vsys1)-> set interface ethernet4/1 export
5. ns(vsys1)-> save
Interface ethernet4/1 is now available for use in the root system.
6. ns(vsys1)-> exit

VLAN-BASED TRAFFIC CLASSIFICATION

With the VLAN-based traffic classification, a NetScreen device uses VLAN tagging⁷ to direct traffic to various subinterfaces bound to different systems⁸. By default, a vsys has two security zones—a shared Untrust zone and its own Trust zone. Each vsys can share the Untrust zone interface with the root system and with other virtual systems. A vsys can also have its own subinterface or a dedicated physical interface (imported from the root system) bound to the Untrust zone.



Note: The castle icon represents a security zone interface.



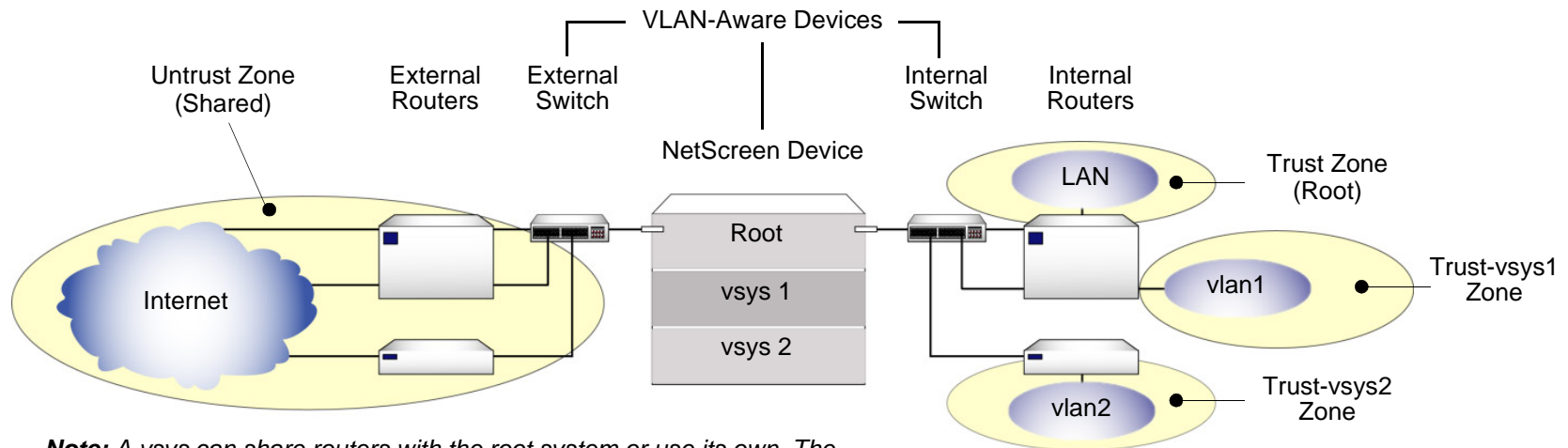
Note: All the virtual systems are shown sharing the Untrust zone interface. They can also have their own subinterface or dedicated physical interface.

7. NetScreen supports VLANs compliant with the IEEE 802.1Q VLAN standard.
8. You can dedicate a physical interface to a virtual system by importing it from the root system to the virtual system. (See [“Importing and Exporting Physical Interfaces” on page 15.](#)) When using physical interfaces, VLAN tagging is unnecessary for traffic on that interface.

VLANs

Each VLAN is bound to a system through a subinterface. If a vsys shares the Untrust zone interface with the root system and has a subinterface bound to its Trust-*vsys_name* zone, the vsys must be associated with a VLAN in the Trust-*vsys_name* zone. If the vsys also has its own subinterface bound to the Untrust zone, the vsys must also be associated with another VLAN in the Untrust zone.

A subinterface stems from a physical interface, which then acts as a trunk port. A trunk port allows a Layer 2 network device to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VLAN identifier (VID) in their frame headers. VLAN trunking allows one physical interface to support multiple logical subinterfaces, each of which must be identified by a unique VLAN tag. The VLAN identifier (tag) on an incoming ethernet frame indicates its intended subinterface—and hence the system—to which it is destined. When you associate a VLAN with an interface or subinterface, the NetScreen device automatically defines the physical port as a trunk port. When using VLANs at the root level in Transparent mode, you must manually define all physical ports as trunk ports with the following CLI command: **set interface vlan1 vlan trunk**.



Note: A vsys can share routers with the root system or use its own. The external and internal switches must be VLAN-aware if the virtual systems have subinterfaces bound to the Untrust and Trust-*vsys_name* zones.

When a *vsys* uses a subinterface (not a dedicated physical interface) bound to the Trust-*vsys_name* zone, the internal switch and internal router in the Trust-*vsys_name* zone must have VLAN-support capabilities. If you create more than one subinterface on a physical interface, then you must define the connecting switch port as a trunk port and make it a member of all VLANs that use it.

When a *vsys* uses a subinterface (not a shared interface or a dedicated physical interface) bound to the shared Untrust zone, the external switch and external router that receives its inbound and outbound traffic must have VLAN-support capabilities. The router tags the incoming frames so that when they reach the NetScreen device, it can direct them to the correct subinterface.

Although a *vsys* cannot be in Transparent mode, because it requires unique interface or subinterface IP addresses, the root system can be in Transparent mode⁹. For the root system to support VLANs while operating in Transparent mode, use the following CLI command to enable the physical interfaces bound to Layer 2 security zones to act as trunk ports: **set interface vlan1 vlan trunk**.

Defining Subinterfaces and VLAN Tags

The Trust-*vsys_name* zone subinterface links a *vsys* to its internal VLAN. The Untrust zone subinterface links a *vsys* to the public WAN, usually the Internet. A subinterface has the following attributes:

- A unique VLAN ID (from 1 to 4095)
- A public or private IP address¹⁰ (the IP address is private by default)
- A netmask for a class A, B, or C subnet
- An associated VLAN

A *vsys* can have a single Untrust zone subinterface and multiple Trust-*vsys_name* zone subinterfaces. If a virtual system does not have its own Untrust zone subinterface, it shares the root level Untrust zone interface. NetScreen devices also support subinterfaces and VLANs at the root level.

9. When the root system is in Transparent mode, it cannot support virtual systems. It can, however, support root-level VLANs while in Transparent mode.

10. For information about public and private IP addresses, see “Public IP Addresses” on page 2-90 and “Private IP Addresses” on page 2-91.

vsys1 shares the Untrust zone interface with the root system. **vsys2** and **vsys100** have their own dedicated subinterfaces bound to the Untrust zone.

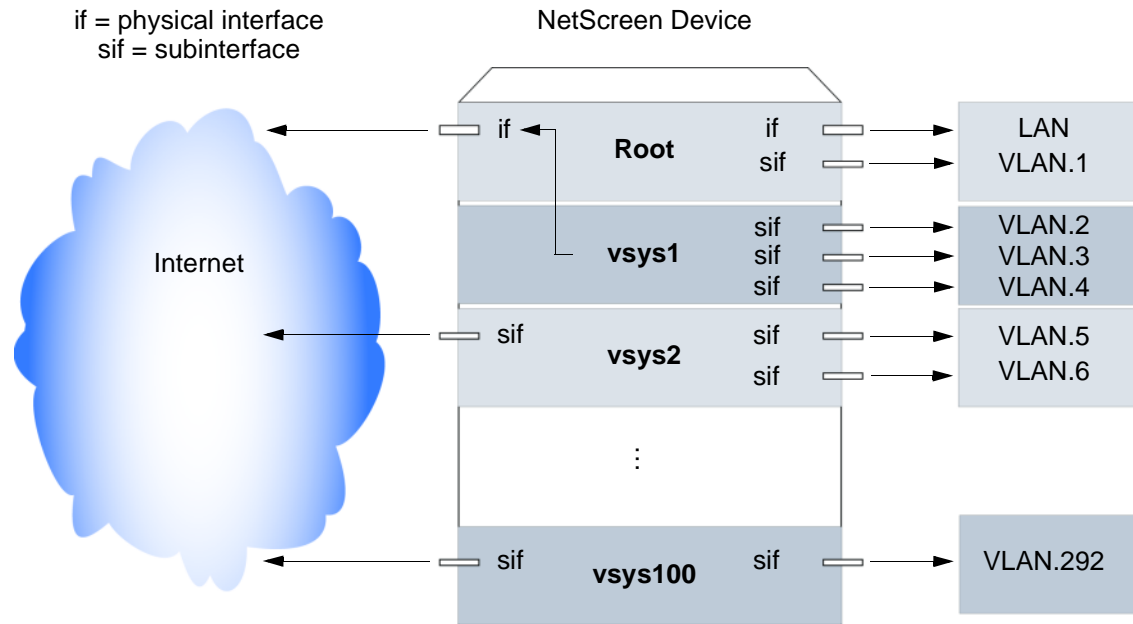
The **root system** has a physical interface and a subinterface bound to its Trust zone.

vsys1 has three subinterfaces bound to its Trust-vsyt1 zone, each leading to a different VLAN.

vsys2 has two subinterfaces bound to its Trust-vsyt2 zone, each leading to a different VLAN.

vsys100 has one subinterface bound to its Trust-vsyt100 zone.

Note: All VLAN IDs must be unique per physical interface.



The NetScreen device supports IEEE 802.1Q-compliant VLAN tags. A tag is an added bit in the Ethernet frame header that indicates membership in a particular VLAN. By binding a VLAN to a vsys, the tag also determines to which vsys a frame belongs, and consequently, which policy is applied to that frame. If a VLAN is not bound to a vsys, policies set in the root system of the NetScreen device are applied to the frame.

A root-level administrator can create a VLAN, assign members to it, and bind it to a vsys. (The assigning of members to a VLAN can be done by several methods—protocol type, MAC address, port number—and is beyond the scope of this document.) The vsys admin, if there is one, then manages the vsys through the creation of addresses, users, services, VPNs, and policies. If there is no vsys admin, then a root-level administrator performs these tasks.

Note: If the root-level admin does not associate a VLAN to a vsys, the VLAN operates within the NetScreen device root system.

There are three tasks that a root-level administrator must perform to create a VLAN for a vsys: Enter a virtual system, define a subinterface, and associate it with a VLAN.

Note: All subnets in a vsys must be disjointed; that is, there must be no overlapping IP addresses among the subnets in the same vsys. For example: Subinterface1 – 10.2.2.1 255.255.255.0 and Subinterface2 – 10.2.3.1 255.255.255.0 are disjointed, and therefore, link to acceptable subnets.

However, subnets with the following subinterfaces overlap, and are unacceptable within the same vsys: subinterface1 – 10.2.2.1 255.255.0.0 and subinterface2 – 10.2.3.1 255.255.0.0.

The address ranges of subnets in different virtual systems can overlap.

Example: Defining Three Subinterfaces and VLAN Tags

In this example, you define subinterfaces and VLAN tags for the three virtual systems that you created in [“Example: Creating Vsys Objects and Vsys Admins” on page 3](#)—vsys1, vsys2, and vsys3. The first two subinterfaces are for two private virtual systems operating in NAT mode, and the third subinterface is for a public virtual system operating in Route mode. The subinterfaces are 10.1.1.1/24, 10.2.2.1/24, and 210.3.3.1/24. You create all three subinterfaces on ethernet3/2.

WebUI

1. Vsys: Click **Enter** (for vsys1).
2. Network > Interfaces > New Sub-IF (for ethernet3/2): Enter the following, and then click **OK**:

Interface Name: ethernet3/2.1

Zone Name: Trust-vsys1

IP Address/Netmask: 10.1.1.1/24

VLAN Tag: 1¹¹

11. You can define virtual systems to operate in Route mode or NAT mode. The default is NAT mode, and thus unnecessary to specify when creating the first two subinterfaces in this example.

3. Vsys: Click **Enter** (for vsys2).
4. Network > Interfaces > New Sub-IF (for ethernet3/2): Enter the following, and then click **OK**:
 - Interface Name: ethernet3/2.2
 - Zone Name: Trust-vsys2
 - IP Address/Netmask: 10.2.2.1/24
 - VLAN Tag: 2
5. Vsys: Click **Enter** (for vsys3).
6. Network > Interfaces > New Sub-IF (for ethernet3/2): Enter the following, and then click **Apply**:
 - Interface Name: ethernet3/2.3
 - Zone Name: Trust-vsys3
 - IP Address/Netmask: 210.3.3.1/24

Select **Interface Mode: Route**, and then click **OK**.
7. Click **Exit Vsys** to return to the root level.

CLI

1. ns-> enter vsys vsys1
2. ns(vsys1)-> set interface ethernet3/2.1 zone trust-vsys1
3. ns(vsys1)-> set interface ethernet3/2.1 ip 10.1.1.1/24 tag 1¹²
4. ns(vsys1)-> save
5. ns(vsys1)-> exit
6. ns-> enter vsys vsys2
7. ns(vsys2)-> set interface ethernet3/2.2 zone trust-vsys2
8. ns(vsys2)-> set interface ethernet3/2.2 ip 10.2.2.1/24 tag 2
9. ns(vsys2)-> save
10. ns(vsys2)-> exit
11. ns-> enter vsys vsys3
12. ns(vsys3)-> set interface ethernet3/2.3 zone trust-vsys3
13. ns(vsys3)-> set interface ethernet3/2.3 ip 210.3.3.1/24 tag 3
14. ns(vsys3)-> set interface ethernet3/2.3 route
15. ns(vsys3)-> save
16. ns(vsys3)-> exit

12. You can define virtual systems to operate in Route mode or NAT mode. The default is NAT mode, and thus unnecessary to specify when creating the first two subinterfaces in this example.

Communicating between VLANs

The members of a VLAN in a vsys have unrestricted communication access with each other. The VLAN members of different vsys cannot communicate with one another unless the participating vsys administrators specifically configure policies allowing the members of their respective systems to do so.

Traffic between root-level VLANs operates within the parameters set by root-level policies. Traffic between virtual system VLANs operates within the parameters set by the participating virtual system policies¹³. Only that traffic allowed to leave the originating virtual system and that traffic allowed to enter the destination virtual system is passed. In other words, the virtual system administrators of both virtual systems must set policies allowing the traffic to flow in the appropriate direction—outgoing and incoming.

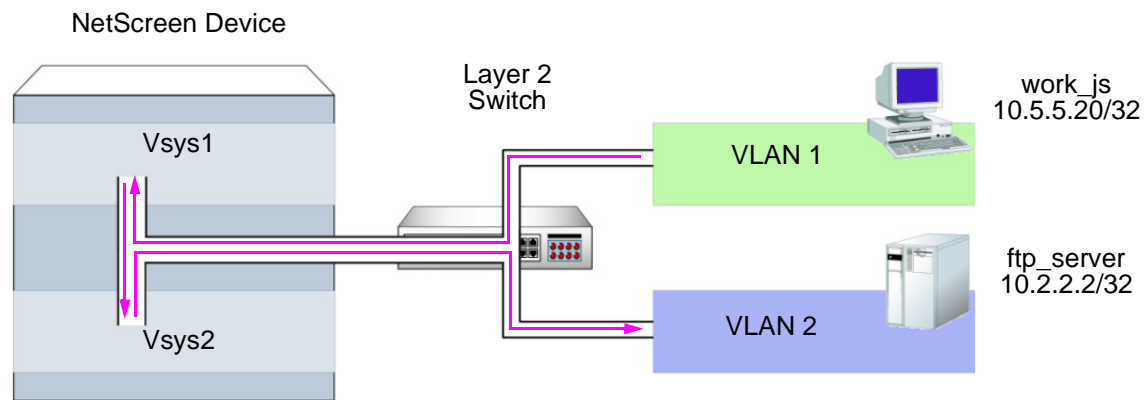
Example: InterVLAN Communication

In this example, you set up two sets of policies to enable traffic between a workstation (work_js with the IP address 10.5.5.20/32) in VLAN 1 and a server (ftp_server with the IP address 10.2.2.2/32) in VLAN 2. The connection is possible if the following two conditions are met:

- The vsys admin for vsys1 has set a policy permitting traffic from the workstation in VLAN 1 to the server in VLAN 2.
- The vsys admin for vsys2 has set a policy permitting traffic from the workstation in VLAN 1 to the server in VLAN 2.

Notice that the network device in front of the internal interface on the NetScreen device is a Layer 2 switch. This forces traffic from VLAN 1 going to VLAN 2 to go through the switch to the NetScreen device for Layer 3 routing. If the network device were a Layer 3 router, traffic between VLAN1 and VLAN2 could pass through the router, bypassing all policies set on the NetScreen device.

13. Policies set in the root system do not affect policies set in virtual systems, and vice versa.



WebUI

Vsys1

1. Objects > Addresses > List > New: Enter the following, and then click **OK**:
Address Name: work_js
IP Address/Domain Name:
IP/Netmask: 10.5.5.20/32
Zone: Trust-vsys1
2. Objects > Addresses > List > New: Enter the following, and then click **OK**:
Address Name: ftp_server
IP Address/Domain Name:
IP/Netmask: 10.2.2.2/32
Zone: Untrust

3. Policies > (From: Trust-vs1, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book: (select), work_js

Destination Address:

Address Book: (select), ftp_server

Service: FTP-Get

Action: Permit

Vsys2

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

Address Name: ftp_server

IP Address/Domain Name: 10.2.2.2

Netmask: 255.255.255.255

Zone: Trust-vs2

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

Address Name: work_js

IP Address/Domain Name:

IP/Netmask: 10.5.5.20/32

Zone: Untrust

3. Policies > (From: Untrust, To: Trust-vsyst2) New: Enter the following, and then click **OK**:

Source Address:

Address Book: (select), work_js

Destination Address:

Address Book: (select), ftp_server

Service: FTP-Get

Action: Permit

CLI

Vsys1

1. set address trust-vsyst1 work_js 10.5.5.20/32
2. set address untrust ftp_server 10.2.2.2/32
3. set policy from trust-vsyst1 to untrust work_js ftp_server ftp-get permit
4. save

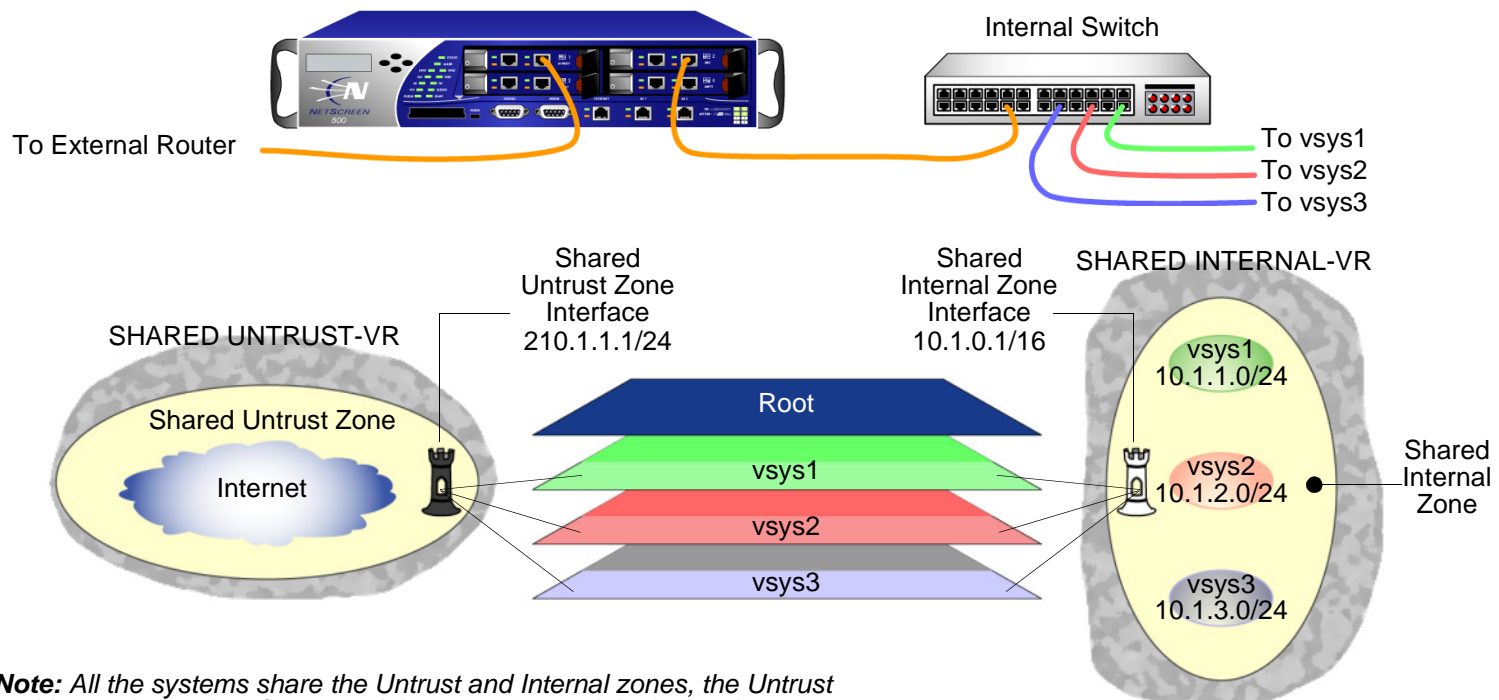
Vsys2

1. set address trust-vsyst2 ftp_server 10.2.2.2/32
2. set address untrust work_js 10.5.5.20/32
3. set policy from untrust to trust-vsyst2 work_js ftp_server ftp-get permit
4. save

IP-BASED TRAFFIC CLASSIFICATION

IP-based traffic classification allows you to use virtual systems without VLANs. Instead of VLAN tags, the NetScreen device uses IP addresses to sort traffic, associating a subnet or range of IP addresses with a particular system—root or vsys. Using IP-based traffic classification exclusively to sort traffic, all systems share the following:

- The untrust-vr and a user-defined internal-vr
- The Untrust zone and a user-defined internal zone
- An Untrust zone interface and a user-defined internal zone interface¹⁴



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

14. Even when using VLAN-based traffic classification for internal traffic, for external traffic all systems use the shared Untrust zone—and, unless a system has a dedicated interface, a shared Untrust zone interface. Using a shared interface on one side and a dedicated interface (with VLAN tagging) on the other constitutes a hybrid approach. VLAN-based and IP-based traffic classification can coexist within the same system or among different systems simultaneously.

To designate a subnet or range of IP addresses to the root system or to a previously created virtual system, you must issue one of the following CLI commands at the root level:

```
set zone zone ip-classification net ip_addr/mask { root | vsys name_str }
```

```
set zone zone ip-classification range ip_addr1-ip_addr2 { root | vsys name_str }
```

Because IP-based traffic classification requires the use of a shared security zone, virtual systems cannot use overlapping internal IP addresses, as is possible with VLAN-based traffic classification. Also, because all the systems share the same internal interface, the operational mode for that interface must be either NAT or Route mode; you cannot mix NAT and Route modes for different systems. In this regard, the addressing scheme of an IP-based approach is not as flexible as that allowed by the more commonly used VLAN-based approach.

Furthermore, sharing virtual routers, security zones, and interfaces is inherently less secure than dedicating an internal virtual router, internal security zone, and internal and external interfaces to each vsys. When all virtual systems share the same interfaces, it is possible for a vsys admin in one vsys to use the **snoop** command to gather information about the traffic activities of another vsys. Also, because IP spoofing is possible on the internal side, NetScreen recommends that you disable the IP spoofing SCREEN option on the shared internal interface. When deciding which traffic classification scheme to use, you must weigh the ease of management offered by the IP-based approach against the increased security and greater addressing flexibility offered by the VLAN-based approach.

Example: Configuring IP-Based Traffic Classification

In this example, you set up IP-based traffic classification for the three virtual systems created in “[Example: Creating Vsys Objects and Vsys Admins](#)” on page 3. You define the trust-vr as sharable. You create a new zone, name it *Internal*, and bind it to the trust-vr. You then make the Internal zone sharable. You bind ethernet3/2 to the shared Internal zone, assign it IP address 10.1.0.1/16, and select NAT mode.

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

The subnets and their respective vsys associations are as follows:

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

WebUI

Virtual Routers, Security Zones, and Interfaces

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

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

Zone Name: Untrust

IP Address/Netmask: 210.1.1.1/24

Route

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet1/2

Gateway IP Address: 210.1.1.250

IP Classification of the Trust Zone

Note: At the time of this writing, you can only configure IP-based traffic classification through the CLI.

CLI

Virtual Routers, Security Zones, and Interfaces

1. set vrouter trust-vr shared
2. set zone name Internal
3. set zone Internal shared
4. set interface ethernet3/2 zone Internal
5. set interface ethernet3/2 ip 10.1.0.1/16
6. set interface ethernet3/2 nat
7. set interface ethernet1/2 zone untrust
8. set interface ethernet1/2 ip 210.1.1.1/24

Route

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

IP Classification of the Trust Zone

10. set zone Internal ip-classification net 10.1.1.0/24 vsys1
11. set zone Internal ip-classification net 10.1.2.0/24 vsys2
12. set zone Internal ip-classification net 10.1.3.0/24 vsys3
13. set zone Internal ip-classification
14. save

LOGGING ON AS A VSYS ADMIN

Whereas a root-level administrator enters a vsys from the root level, a vsys admin enters his or her vsys directly. When a root-level administrator exits a vsys, he or she exits to the root system. When a vsys admin exits a vsys, the connection is immediately severed.

The following example shows how to log on to a vsys as a vsys admin, change your password, and log out.

Example: Logging On and Changing Your Password

In this example, you, as a vsys admin, log on to vsys1 by entering your assigned login name jsmith and password Pd50iH10. You change your password to I6DIs13guh, and then log out.

Note: A vsys admin cannot change his or her login name (user name) because the NetScreen device uses that name, which must be unique among all vsys admins, to route the login connection to the appropriate vsys.

WebUI

Logging On

1. In the URL field in your Web browser, enter the Untrust zone interface IP address for vsys1.
2. When the Network Password dialog box appears, enter the following, and then click **OK**:

User Name: jsmith

Password: Pd50iH10

Changing your Password

3. Configuration > Admin > Administrators: Enter the following, and then click **OK**:

Vsys Admin Old Password: Pd50iH10

Vsys Admin New Password: I6DIs13guh

Confirm New Password: I6DIs13guh

Logging Out

4. Click **Logout**, located at the bottom of the menu column.

CLI

Logging On

1. From a Secure Command Shell (SCS), Telnet, or HyperTerminal session command-line prompt, enter the Untrust zone interface IP address for vsys1.
2. Log on with the following user name and password:
 - User Name: jsmith
 - Password: Pd50iH10

Changing your Password

3. set admin password l6Dls13guh
4. save

Logging Out

5. exit

Index

A

administration
vsys admin 33

C

CLI conventions v
conventions
CLI v
WebUI iv

D

defining
subinterfaces 21

I

IEEE 802.1Q VLAN standard 17
interfaces
dedicated 12, 28
exporting from vsys 16
importing to vsys 15
shared 12, 28
IP-based traffic classification 28

L

logging in
vsys 28, 33

M

MIP
virtual systems 9

P

password
vsys admin 33
ports
trunk 19

S

ScreenOS
virtual systems, VRs 6
virtual systems, zones 7
security zones
See zones
Software
key, vsys 12
subinterfaces 19
configuring (vsys) 19
creating (vsys) 19
defining 21
multiple subinterfaces per vsys 19

T

traffic
classification, IP-based 28
classification, VLAN-based 17
through traffic, vsys sorting 10–11
trunk ports 19
defined 18
manually setting 18

V

VIP
virtual systems 9
virtual system 1–34
admin types 3
admins iii, 1
basic functional requirements 3
changing admin's password 3, 33

creating a vsys object 3
exporting a physical interface 16
importing a physical interface 15
interfaces 7
IP-based traffic classification 28–32
manageability and security 29
MIP 9
overlapping address ranges 21, 29
overlapping subnets 21
shared VR 12
shared zone 12
software key 12
traffic sorting 9–14
Transparent mode 18
VIP 9
VLAN-based traffic classification 17–27
VRs 6
zones 7

VLANs

communicating with another VLAN 24–27
creating 21–23
subinterfaces 19
tag 19, 20
Transparent mode 18, 19
trunking 18
VLAN-based traffic classification 17

VRs

creating a shared VR 13
shared 12

W

WebUI, conventions iv

Z

zones
shared 12
vsys 7

