NetScreen Concepts & Examples

ScreenOS Reference Guide

Volume 7: Virtual Systems

ScreenOS 5.0.0

P/N 093-0930-000

Rev. B

Copyright Notice

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
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

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 7, “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 document contains several types of conventions, which are introduced in the following sections:

CLI Conventions

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  means "set the management options for the ethernet1, ethernet2, or ethernet3 interface".
- Variables appear in *italic.* For example:

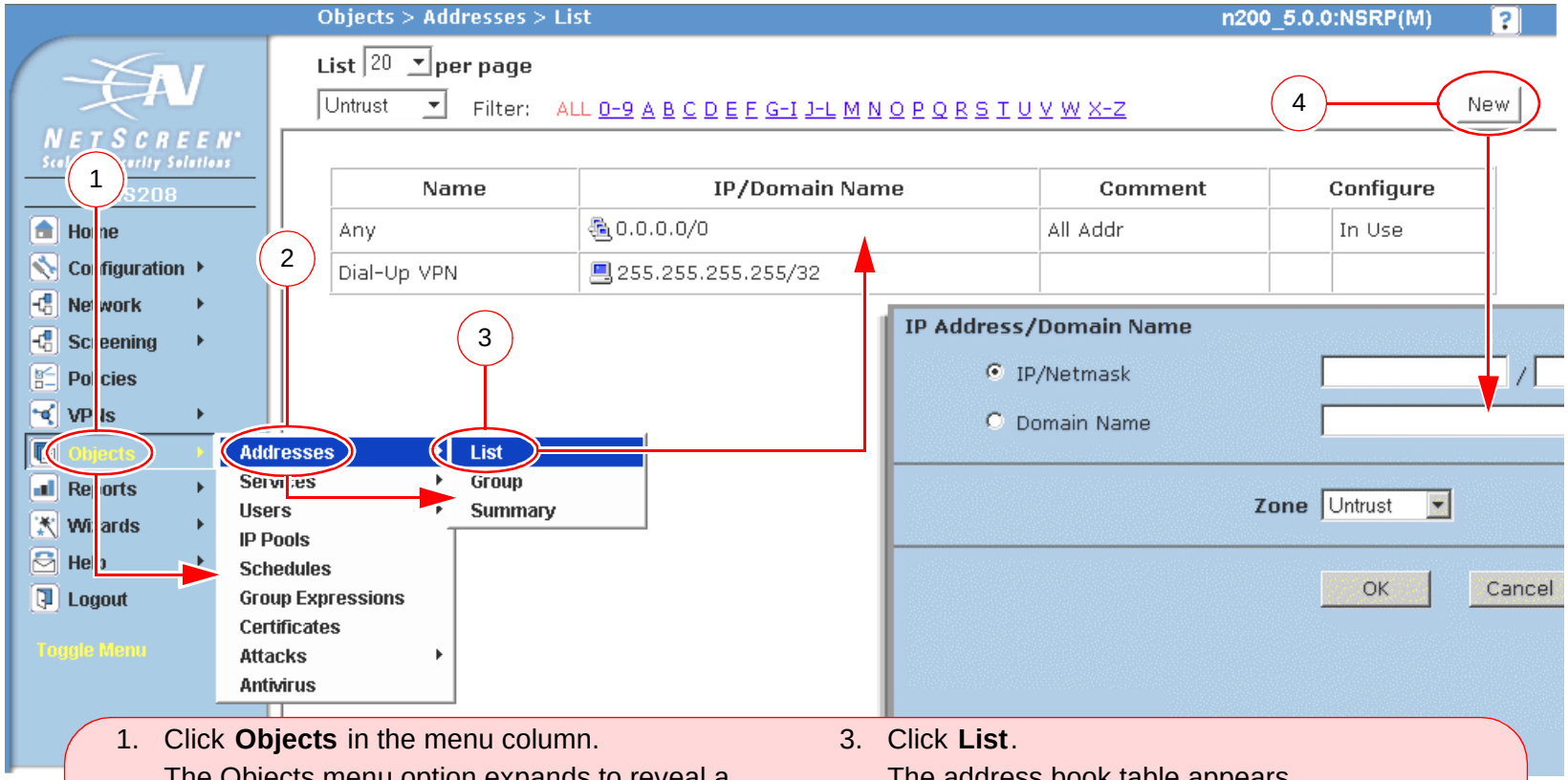
  ```
  set admin user name password
  ```

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: "Use the **get system** command to display the serial number of a NetScreen device."

Note: *When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing* ***set adm u joe j12fmt54*** *is enough to enter the command* ***set admin user joe j12fmt54****. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.*

WebUI Conventions

Throughout this book, a chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links. For example, the path to the address configuration dialog box is presented as **Objects > Addresses > List > New**. This navigational sequence is shown below.



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.
   The new address configuration dialog box appears.

To perform a task with the WebUI, you must first navigate to the appropriate dialog box where you can then define objects and set parameters. The set of instructions for each task is divided into two parts: a navigational path and configuration details. For example, the following set of instructions includes the path to the address configuration dialog box and the settings for you to configure:

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

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.5/32

Zone: Untrust

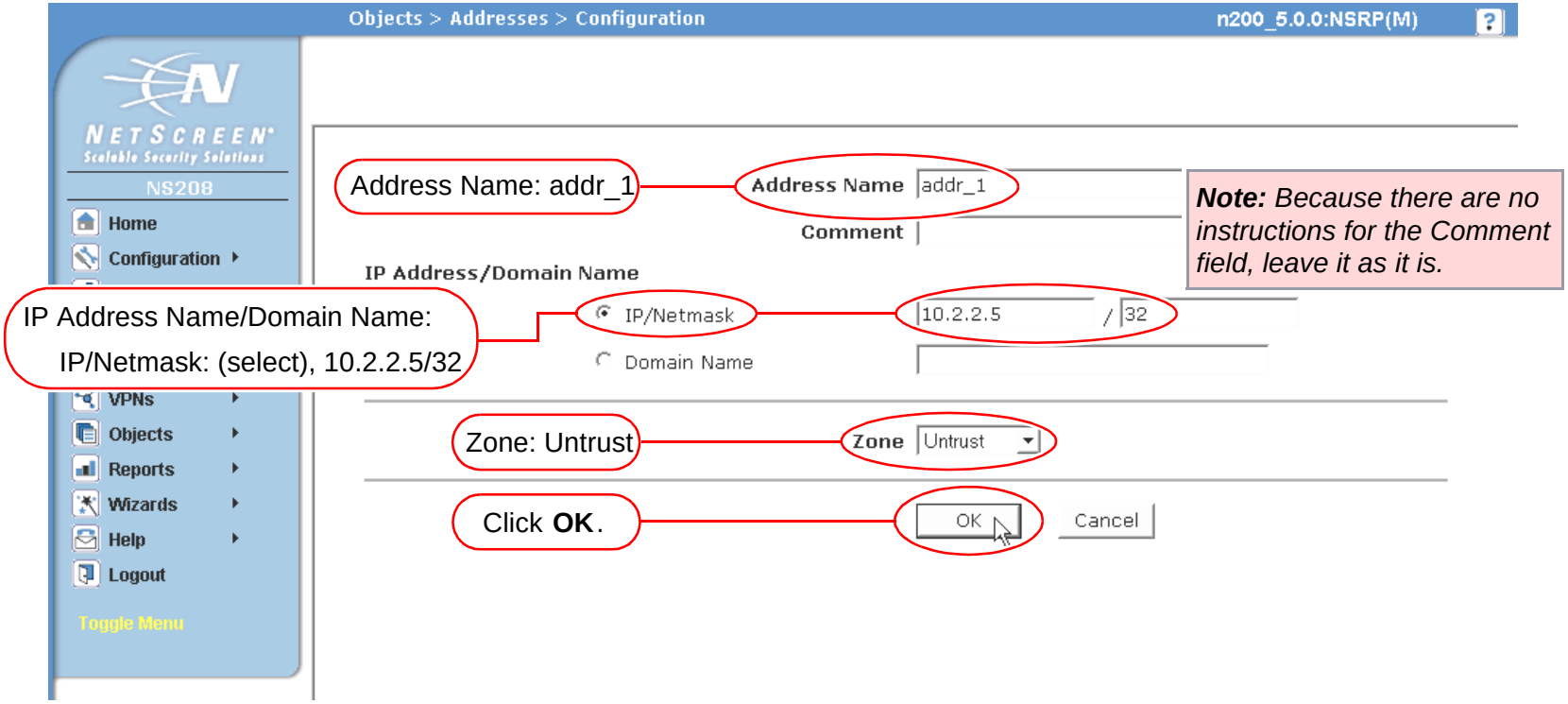


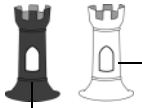
Illustration Conventions

The following graphics make up the basic set of images used in illustrations throughout this book:

Generic NetScreen Device

Virtual Routing Domain

Security Zone



Security Zone Interfaces

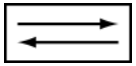
White = Protected Zone Interface (example: Trust Zone)

Black = Outside Zone Interface (example: Untrust Zone)

Tunnel Interface

VPN Tunnel

Router Icon

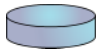


Switch Icon

Local Area Network (LAN) with a Single Subnet

(example: 10.1.1.0/24)

Internet



Dynamic IP (DIP) Pool

Desktop Computer

Laptop Computer

Generic Network Device

(examples: NAT server, Access Concentrator)

Server

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations.

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes ("); for example, **set address trust "local LAN" 10.1.1.0/24**.
- NetScreen trims any spaces leading or trailing text within a set of double quotes; for example, **" local LAN "** becomes **"local LAN"**.
- NetScreen treats multiple consecutive spaces as a single space.
- Name strings are case sensitive, although many CLI key words are case insensitive. For example, **"local LAN"** is different from **"local lan"**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

  Note: *A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your Web browser supports.*

- ASCII characters from 32 (0x20 in hexidecimals) to 255 (0xff), except double quotes ("), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NETSCREEN DOCUMENTATION

To obtain technical documentation for any NetScreen product, visit www.netscreen.com/resources/manuals/.

To obtain the latest software version, visit www.netscreen.com/services/download_soft. Select a category of software product from the dropdown list, then follow the displayed instructions. (You must be a registered user to download NetScreen software.)

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

techpubs@netscreen.com

1

Virtual Systems

You can logically partition a single NetScreen security system[1] 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****-37.*

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:

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.

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 admins[2]
- Select the virtual router that you want the vsys to use for its Trust-*vsysname* zone, Untrust-Tun-*vsysname* zone, and Global-*vsysname* zone

After creating a vsys object, you—as the root-level admin—need to perform other configurations to make it a functional vsys. You 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, you can then exit the virtual system and allow a vsys admin, if defined, to log on and begin configuring addresses, users, services, VPNs, routes, and policies.

Example: Vsys Objects and 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 wIEaS1v1[3]. For vsys2, you create vsys admin Bob with password pjF56Ms2. For vsys3, you do not define a vsys admin. Instead, you accept the admin definition that the NetScreen device automatically generates. In the case of vsys3, the NetScreen device creates the admin “vsys_vsys3” with password “vsys_vsys3”.

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

For vsys1 and vsys2, you use the default virtual router. For vsys3, you choose the sharable root-level untrust-vr.

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.

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*.

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. Vsys1

   Vsys > New: Enter the following, and then click **OK**:

   Vsys Name: vsys1

   Vsys Admin Name: Alice

   Vsys Admin New Password: wIEaS1v1

   Confirm New Password: wIEaS1v1

   Virtual Router:

   Create a default virtual router: (select)

2. Vsys2

   Vsys > New: Enter the following, and then click **OK**:

   Vsys Name: vsys2

   Vsys Admin Name: Bob

   Vsys Admin New Password: pjF56Ms2

   Confirm New Password: pjF56Ms2

   Virtual Router:

   Create a default virtual router: (select)

3. Vsys3

Vsys > New: Enter the following, and then click **OK**:

Vsys Name: vsys3

Virtual Router:

Select an existing virtual router: (select), untrust-vr

CLI

1. Vsys1

```
ns-> set vsys vsys1
ns(vsys1)-> set admin name Alice
ns(vsys1)-> set admin password wIEaS1v1
ns(vsys1)-> save[4]
ns(vsys1)-> exit
```

2. Vsys2

```
ns-> set vsys vsys2
ns(vsys2)-> set admin name Bob
ns(vsys2)-> set admin password pjF56Ms2
ns(vsys2)-> save
ns(vsys2)-> exit
```

3. Vsys3

```
ns-> set vsys vsys3 vrouter share untrust-vr
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 “Virtual Routers” on page **6**-1.

Note: *This release of ScreenOS supports user-defined virtual routers within a virtual system.*

Zones

Each virtual system (vsys) is a unique security domain and can share security zones with the root system and have its own security 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
- Global-*vsys_name* zone

> ***Note:*** *For information on each of these zone types, see "Zones" on page* ***2****-45.*

Each vsys can also support extra user-defined security zones. You can bind these zones to any shared virtual routers defined at the root level or to the virtual router dedicated to that vsys. To create a security zone for a vsys named vsys1, do either of the following:

WebUI

Vsys > Enter (for vsys1)

Network > Zones > New: Enter the following, and then click **OK**:

Zone Name: (type a name for the zone)

Virtual Router Name: (select a virtual router from the drop-down list)

Zone Type: Layer 3

CLI

```
ns-> enter vsys vsys1
ns (vsys1)-> set zone name name_str
ns(vsys1)-> set zone vrouter vrouter
ns(vsys1)-> save
```

The maximum number of security zones that a vsys or the root system can contain is limited only by the number of security zones available at the device level[5]. It is possible for a single vsys to consume all available security zones if the root admin or a root-level read/write admin assigns all of them to that particular vsys. Conversely, if all virtual systems share root-level security zones and do not make use of any user-defined vsys-level zones, then all security zones are available for root-level use.

Interfaces

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

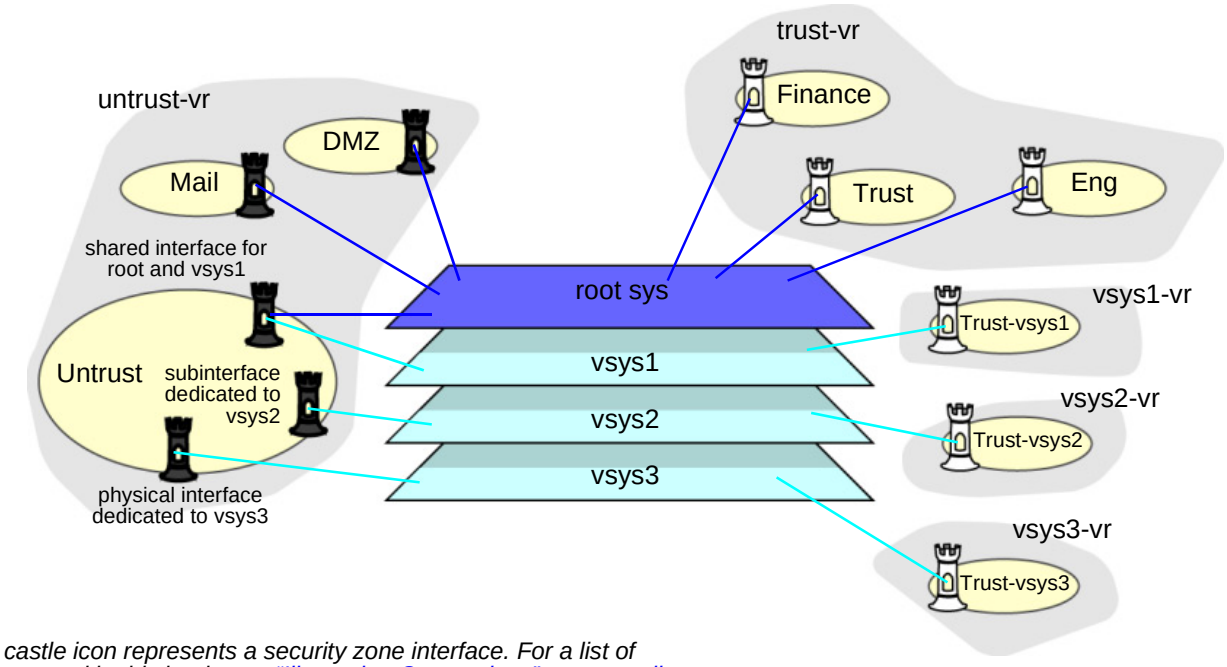
Untrust Zone Interface Types	Trust Zone Interface Types
• Dedicated Physical Interface	• Dedicated Physical Interface
• Subinterface (with VLAN tagging as a means for trunking* inbound and outbound traffic)	• Subinterface (with VLAN tagging)
• Shared Interface (physical, subinterface, redundant interface, aggregate interface) with Root System	• Shared Physical Interface with Root System (and IP-based traffic classification†)

* For information about VLAN tagging and trunking concepts, see "VLANs" on page 22.

† For more information about IP-based traffic classification, see "IP-Based Traffic Classification" on page 33.

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.

5. The total number of user-definable (or "custom") security zones available at the device level is the sum of the number of root-level custom zones—as defined by one or more zone license keys—and the number of custom zones permitted by the vsys license key.



Note: *The castle icon represents a security zone interface. For a list of graphic icons used in this book, see* *"Illustration Conventions" on page vii**.*

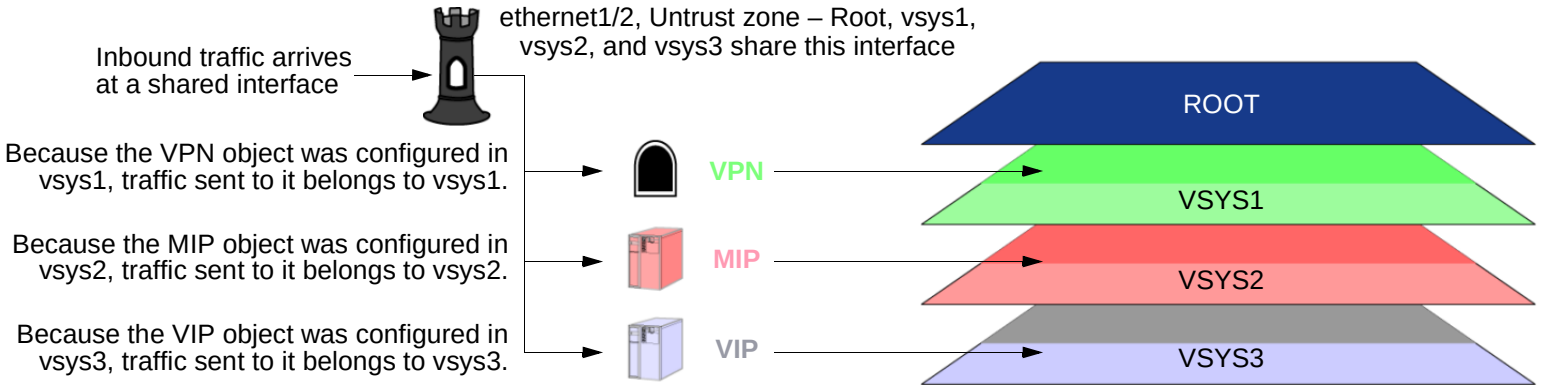
TRAFFIC SORTING

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 tags[6] in frame headers to identify the system to which inbound traffic belongs. IP-based traffic classification uses the source and destination IP address in IP packet headers to identify the system to which traffic belongs. The procedure that the NetScreen device uses to determine the system to which a packet belongs progresses through the following three steps:

1. Ingress Interface/Source IP Traffic Classification

The NetScreen device checks if the ingress interface is a dedicated interface or a shared interface[7].

1. If the ingress interface is dedicated to a vsys (“v-i”, for example), 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 uses IP classification to check if the source IP address is associated with a particular vsys.
   - If the source IP address is not associated with a particular vsys, ingress IP classification fails.
   - If the source IP address is associated with a particular vsys, ingress IP classification succeeds.

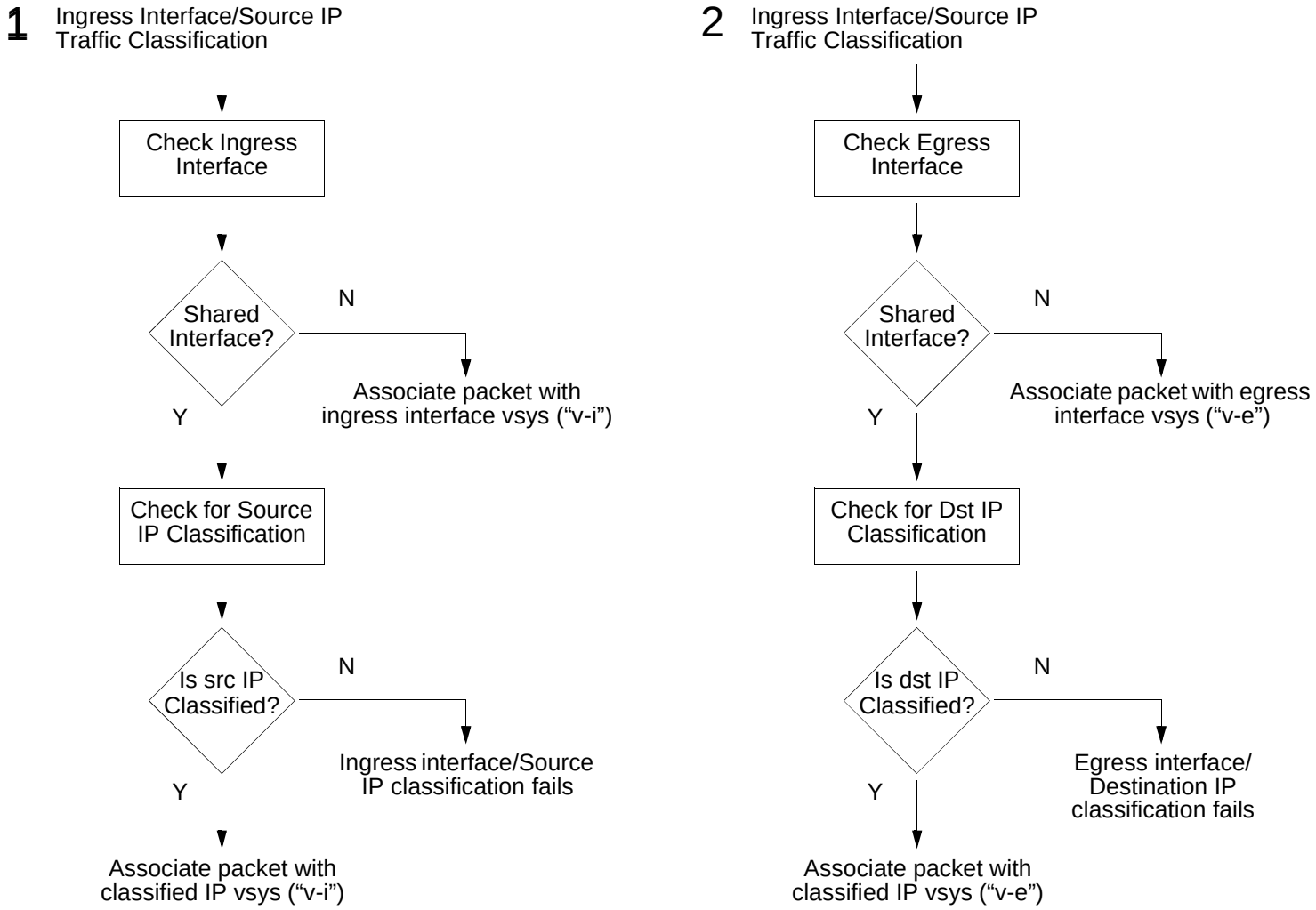
2. Egress Interface/Destination IP Traffic Classification

The NetScreen device checks if the egress interface is shared or dedicated.

1. If the egress interface is dedicated to a vsys (“v-e”, for example), the NetScreen device associates the traffic with the system to which the interface is dedicated.
2. If the egress interface is a shared interface, the NetScreen device uses IP classification to check if the destination IP address is associated with a particular vsys.
   - If the destination IP address is not associated with a particular vsys, egress IP classification fails.
   - If the destination IP address is associated with a particular vsys, egress IP classification succeeds.

6. 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.
7. For more information about shared and dedicated interfaces, see “Dedicated and Shared Interfaces” on page 15.

When a packet arrives at a NetScreen device that has virtual systems, it performs the following steps to associate the packet with a vsys.



3. Vsys Traffic Assignment

Based on the outcome of the ingress interface/source IP (I/S) and egress interface/destination IP (E/D) traffic classifications, the NetScreen device determines the vsys to which traffic belongs.

- If I/S traffic classification succeeds, but E/D traffic classification fails, the NetScreen device uses the policy set and route table for the vsys associated with the ingress interface or source IP address (a vsys named “v-i”, for example).

  I/S traffic classification is particularly useful when permitting outbound traffic from a vsys to a public network such as the Internet.

- If E/D traffic classification succeeds, but I/S traffic classification fails, the NetScreen device uses the policy set and route table for the vsys associated with the egress interface or destination IP address (a vsys named “v-e”, for example).

  E/D traffic classification is particularly useful when permitting inbound traffic to one or more servers in a vsys from a public network such as the Internet.

- If both classification attempts succeed and the associated virtual systems are the same, the NetScreen device uses the policy set and route table for that vsys.

  You can use both I/S and E/D IP traffic classification to permit traffic from specific addresses in one zone to specific addresses in another zone of the same vsys.

- If both classification attempts succeed, the associated virtual systems are different, and the interfaces are bound to the same shared security zone, the NetScreen first uses the policy set and route table for the I/S vsys, and then uses the policy set and route table for the E/D vsys.

  NetScreen supports intrazone intervsys traffic when the traffic occurs in the same shared zone. The NetScreen device first applies the “v-i” policy set and route table, loops the traffic back on the Untrust interface, and then applies the “v-e” policy set and route table. Such intrazone traffic might be common if a single company uses one shared internal zone with different virtual systems for different internal departments and wants to allow traffic between the different departments.

- If both classification attempts succeed, the associated virtual systems are different, and the interfaces are bound to different shared security zones, the NetScreen device drops the packet.

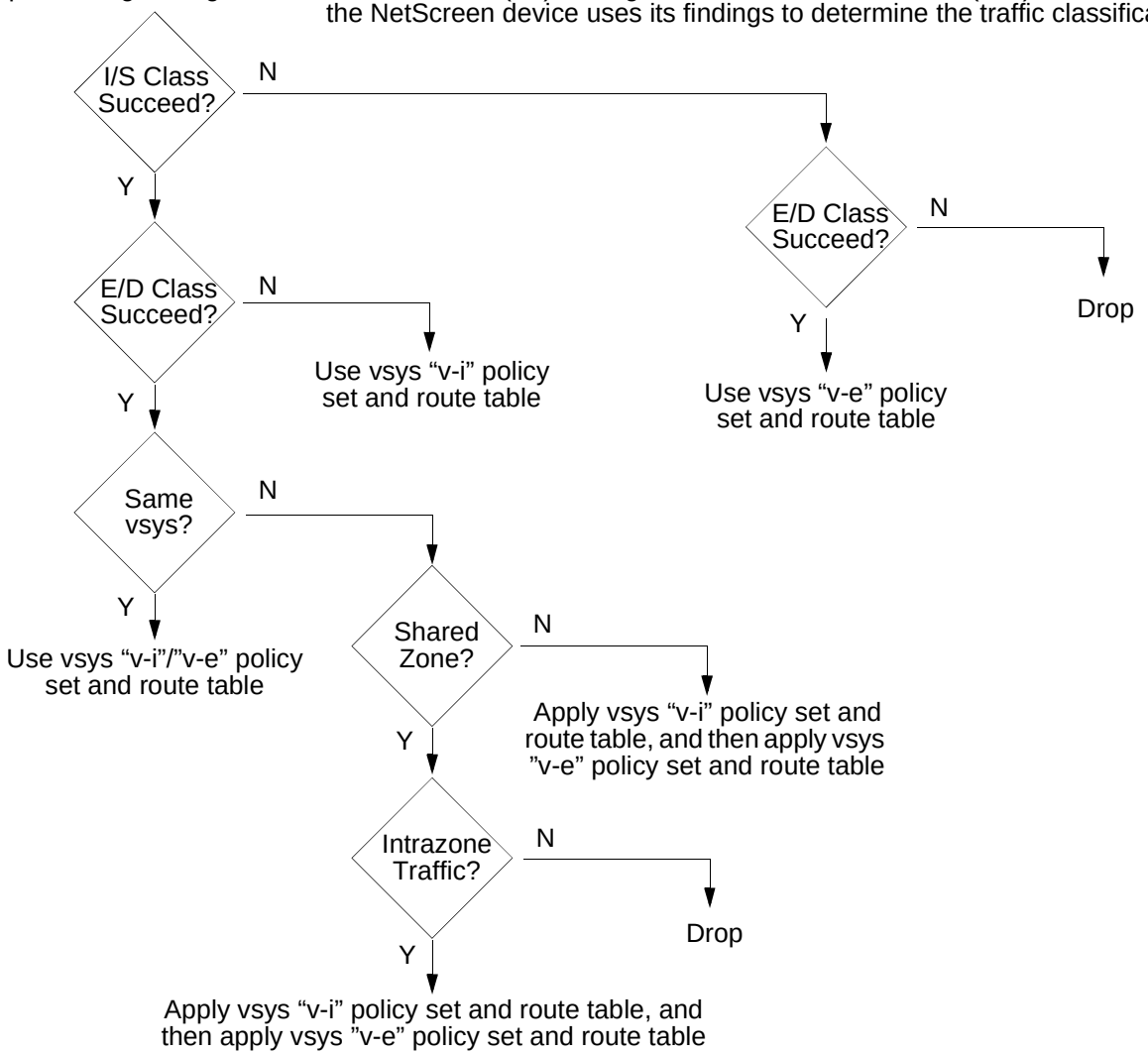
  NetScreen does not support interzone intervsys traffic between shared security zones.

- If both classification attempts succeed, the associated virtual systems are different, and the ingress and egress interfaces are bound to zones dedicated to different virtual systems, the NetScreen device first applies the “v-i” policy set and route table. It then loops the traffic back on the Untrust interface and

applies the “v-e” policy set and route table. (See “Example: InterVsys Communication” on page 28.) NetScreen supports interzone intervsys traffic between dedicated security zones.

– If both classification attempts fail, the NetScreen device drops the packet.

3 After performing the ingress interface/source IP (I/S) and egress interface/destination IP (E/D) classifications, the NetScreen device uses its findings to determine the traffic classification.



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[8]. 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.*

8. For the shared zone option to be available, the NetScreen device must be operating at Layer 3, which means that you must previously assign an IP address to at least one root-level interface.

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 33.)

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—as the root admin—import the physical interface ethernet4/1 to vsys1. You bind it to the Untrust zone and assign it the IP address 1.1.1.1/24.

WebUI

1. Entering Vsys1

   Vsys: Click **Enter** (for vsys1).

2. Importing and Defining the Interface

   Network > Interfaces: Click **Import** (for ethernet4/1).

   Network > Interfaces > Edit (for ethernet4/1): Enter the following, and then click **OK**:

   Zone Name: Untrust

   IP Address/Netmask: 1.1.1.1/24

3. Exiting Vsys1

   Click the **Exit Vsys** button (at the bottom of the menu column) to return to the root level.

CLI

1. Entering Vsys1

```
ns-> enter vsys vsys1
```

2. Importing and Defining the Interface

```
ns(vsys1)-> set interface ethernet4/1 import
ns(vsys1)-> set interface ethernet4/1 zone untrust
ns(vsys1)-> set interface ethernet4/1 ip 1.1.1.1/24
ns(vsys1)-> save
```

3. Exiting Vsys1

```
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. Entering Vsys1

   Vsys: Click **Enter** (for vsys1).

2. Exporting the Interface

   Network > Interfaces > Edit (for ethernet4/1): Enter the following, and then click **OK**:

   Zone Name: Null

   IP Address/Netmask: 0.0.0.0/0

   Network > Interfaces: Click **Export** (for ethernet4/1).

   (Interface ethernet4/1 is now available for use in the root system or in another vsys.)

3. Exiting Vsys1

Click the **Exit Vsys** button (at the bottom of the menu column) to return to the root level.

CLI

1. Entering Vsys1

```
ns-> enter vsys vsys1
```

2. Exporting the Interface

```
ns(vsys1)-> unset interface ethernet4/1 ip
ns(vsys1)-> unset interface ethernet4/1 zone
ns(vsys1)-> unset interface ethernet4/1 import
This command will remove all objects associated with interface, continue? y/[n] y
ns(vsys1)-> save
```

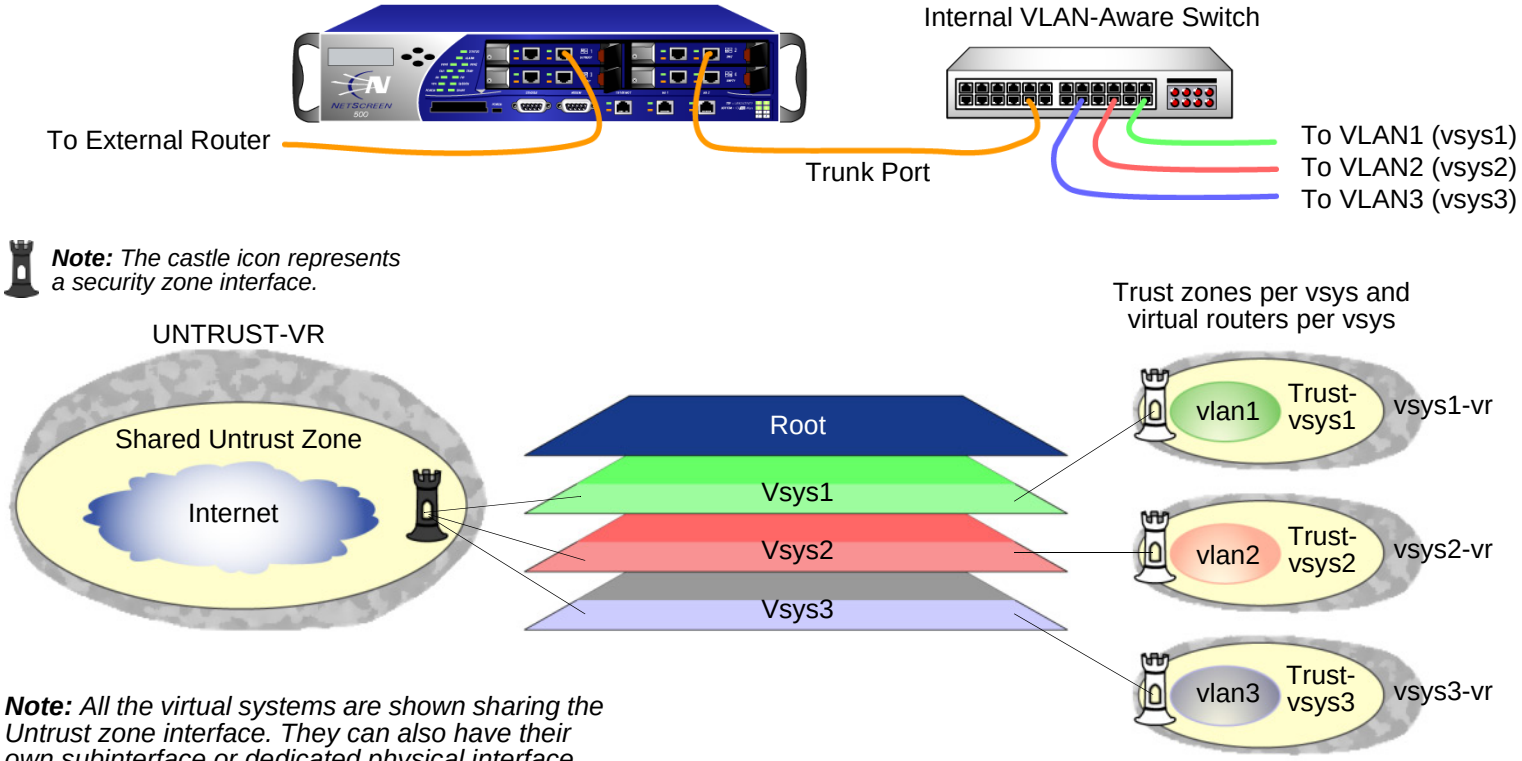
(Interface ethernet4/1 is now available for use in the root system or in another vsys.)

3. Exiting Vsys1

```
ns(vsys1)-> exit
```

VLAN-BASED TRAFFIC CLASSIFICATION

With the VLAN-based traffic classification, a NetScreen device uses VLAN tagging[9] to direct traffic to various subinterfaces bound to different systems[10]. 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.

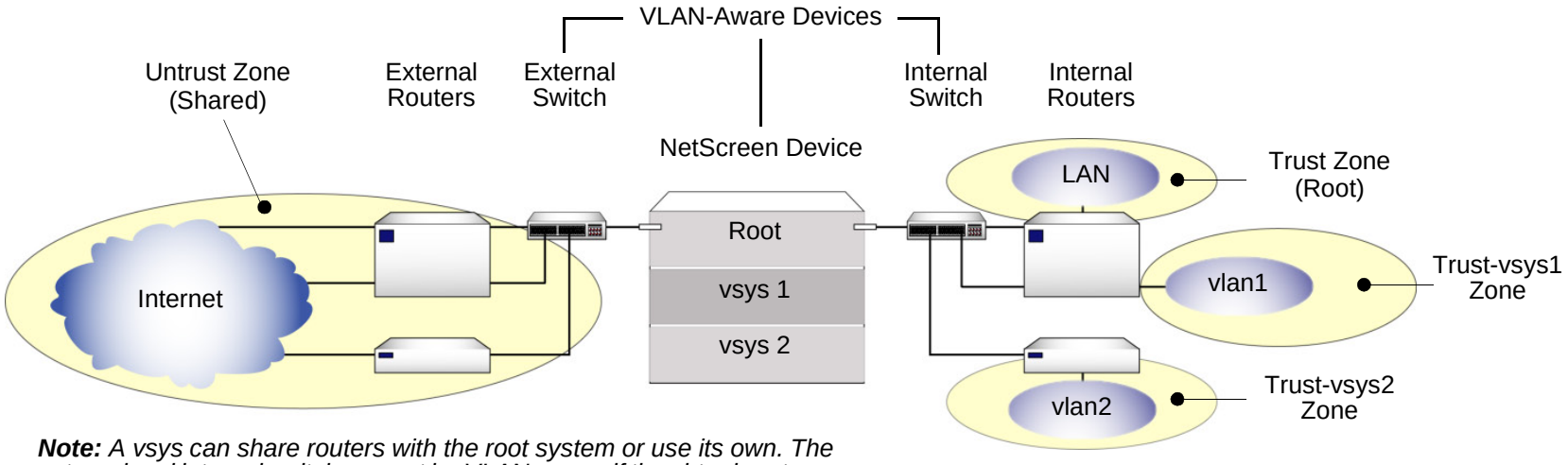


9. NetScreen supports VLANs compliant with the IEEE 802.1Q VLAN standard.
10. You can dedicate a physical interface to a virtual system by importing it from the root system to the virtual system. (See "Importing and Exporting Physical Interfaces" on page 18.) When using physical interfaces, VLAN tagging 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 mode[11]. 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 address[12] (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.

11. When the root system is in Transparent mode, it cannot support virtual systems. It can, however, support root-level VLANs while in Transparent mode.
12. For information about public and private IP addresses, see “Public IP Addresses” on page **2**-77 and “Private IP Addresses” on page **2**-78.

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

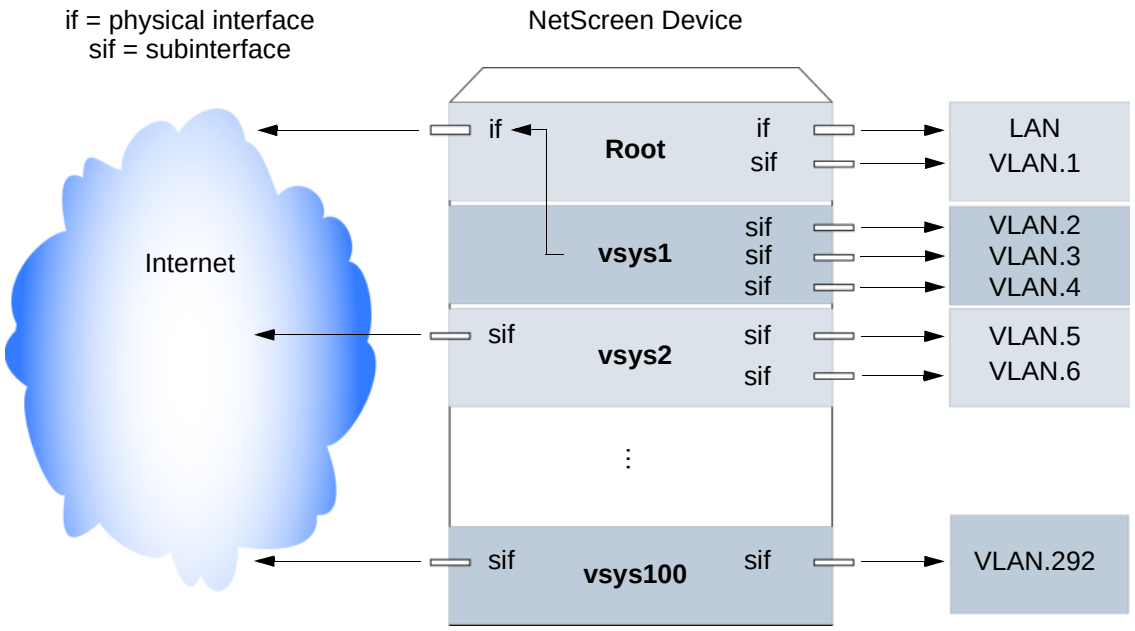
The **root system** has a physical interface and a subinterface bound to its Trust zone.

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

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

vsys100 has one subinterface bound to its Trust-vsys100 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: Vsys Objects and 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 1.3.3.1/24. You create all three subinterfaces on ethernet3/2.

All three virtual systems share the Untrust zone and its interface (ethernet1/1; 1.1.1.1/24) with the root system. The Untrust zone is in the untrust-vr routing domain.

WebUI

1. Vsys1 Subinterface and VLAN Tag

Vsys: Click **Enter** (for vsys1).

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: 1[13]

2. Vsys2 Subinterface and VLAN Tag

Vsys: Click **Enter** (for vsys2).

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

3. Vsys3 Subinterface and VLAN Tag

Vsys: Click **Enter** (for vsys3).

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: 1.3.3.1/24

VLAN Tag: 3

Select **Interface Mode: Route**, and then click **OK**.

Click **Exit Vsys** to return to the root level.

13. 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.

CLI

1. Vsys1 Subinterface and VLAN Tag

```
ns-> enter vsys vsys1
ns(vsys1)-> set interface ethernet3/2.1 zone trust-vsys1
ns(vsys1)-> set interface ethernet3/2.1 ip 10.1.1.1/24 tag 1[14]
ns(vsys1)-> save
ns(vsys1)-> exit
```

2. Vsys2 Subinterface and VLAN Tag

```
ns-> enter vsys vsys2
ns(vsys2)-> set interface ethernet3/2.2 zone trust-vsys2
ns(vsys2)-> set interface ethernet3/2.2 ip 10.2.2.1/24 tag 2
ns(vsys2)-> save
ns(vsys2)-> exit
```

3. Vsys3 Subinterface and VLAN Tag

```
ns-> enter vsys vsys3
ns(vsys3)-> set interface ethernet3/2.3 zone trust-vsys3
ns(vsys3)-> set interface ethernet3/2.3 ip 1.3.3.1/24 tag 3
ns(vsys3)-> set interface ethernet3/2.3 route
ns(vsys3)-> save
ns(vsys3)-> exit
```

14. 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 Virtual Systems

The members of a VLAN in a vsys have unrestricted communication access with each other. The VLAN members of different virtual systems 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 policies[15]. The NetScreen device passes only traffic allowed to leave the originating virtual system and allowed to enter the destination virtual system. In other words, the vsys admins of both virtual systems must set policies allowing the traffic to flow in the appropriate direction—outgoing and incoming.

Example: InterVsys Communication

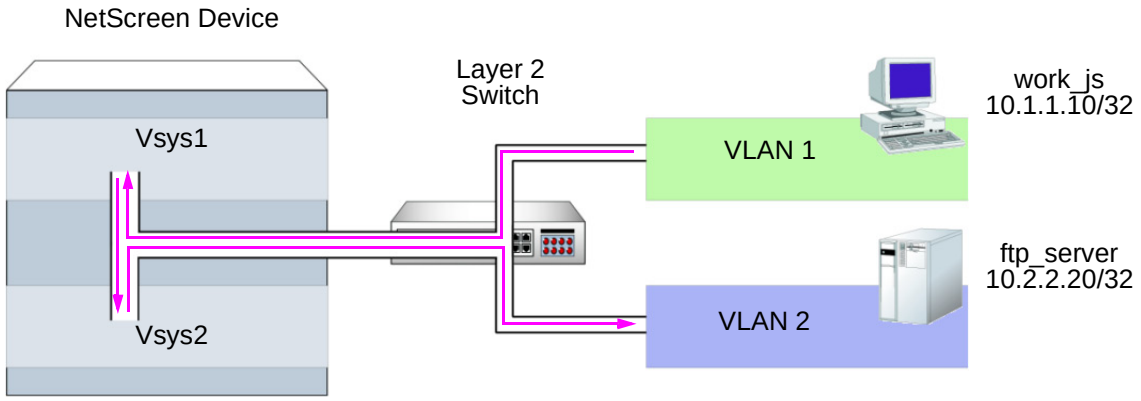
In this example, the admins for vsys1 and vsys2—see "Example: Defining Three Subinterfaces and VLAN Tags" on page 25—set up policies to enable traffic between a workstation (work_js with the IP address 10.1.1.10/32) in VLAN 1 and a server (ftp_server with the IP address 10.2.2.20/32) in VLAN 2. The connection is possible if the following two conditions are met:

- The vsys admin for vsys1 has set a policy permitting traffic from the workstation in Trust-vsys1 to the server in its Untrust zone.
- The vsys admin for vsys2 has set a policy permitting traffic from the workstation in its Untrust zone to the server in Trust-vsys2.

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.

The vsys1 and vsys2 admins also set up the appropriate routes. The shared Untrust zone is in the untrust-vr and the Trust zones in vsys1 and vsys2.

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



WebUI

1. Vsys1

Addresses

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

Address Name: work_js

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.10/32

Zone: Trust-vsys1

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

Address Name: ftp_server

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.20/32

Zone: Untrust

Routes

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.1.1.0/24

Next Hop Virtual Router Name: (select); vsys1-vr

Network > Routing > Routing Entries > vsys1-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Next Hop Virtual Router Name: (select); untrust-vr

Policy

Policies > (From: Trust-vsys1, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), work_js

Destination Address:

Address Book Entry: (select), ftp_server

Service: FTP-Get

Action: Permit

2. Vsys2

Addresses

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

Address Name: ftp_server

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.2/032

Zone: Trust-vsys2

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

Address Name: work_js

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.10/32

Zone: Untrust

Routes

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Next Hop Virtual Router Name: (select); vsys2-vr

Network > Routing > Routing Entries > vsys2-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (select); untrust-vr

Policy

Policies > (From: Untrust, To: Trust-vsys2) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), work_js

Destination Address:

Address Book Entry: (select), ftp_server

Service: FTP-Get

Action: Permit

CLI

1. Vsys1

   Addresses

   ```
   set address trust-vsys1 work_js 10.1.1.10/32
   set address untrust ftp_server 10.2.2.20/32
   ```

   Routes

   ```
   set vrouter untrust-vr route 10.1.1.0/24 vrouter vsys1-vr
   set vrouter vsys1-vr route 0.0.0.0/0 vrouter untrust-vr
   ```

   Policy

   ```
   set policy from trust-vsys1 to untrust work_js ftp_server ftp-get permit
   save
   ```

2. Vsys2

   Addresses

   ```
   set address trust-vsys2 ftp_server 10.2.2.20/32
   set address untrust work_js 10.1.1.10/32
   ```

3. Routes

   ```
   set vrouter untrust-vr route 10.2.2.0/24 vrouter vsys2-vr
   set vrouter vsys2-vr route 0.0.0.0/0 vrouter untrust-vr
   ```

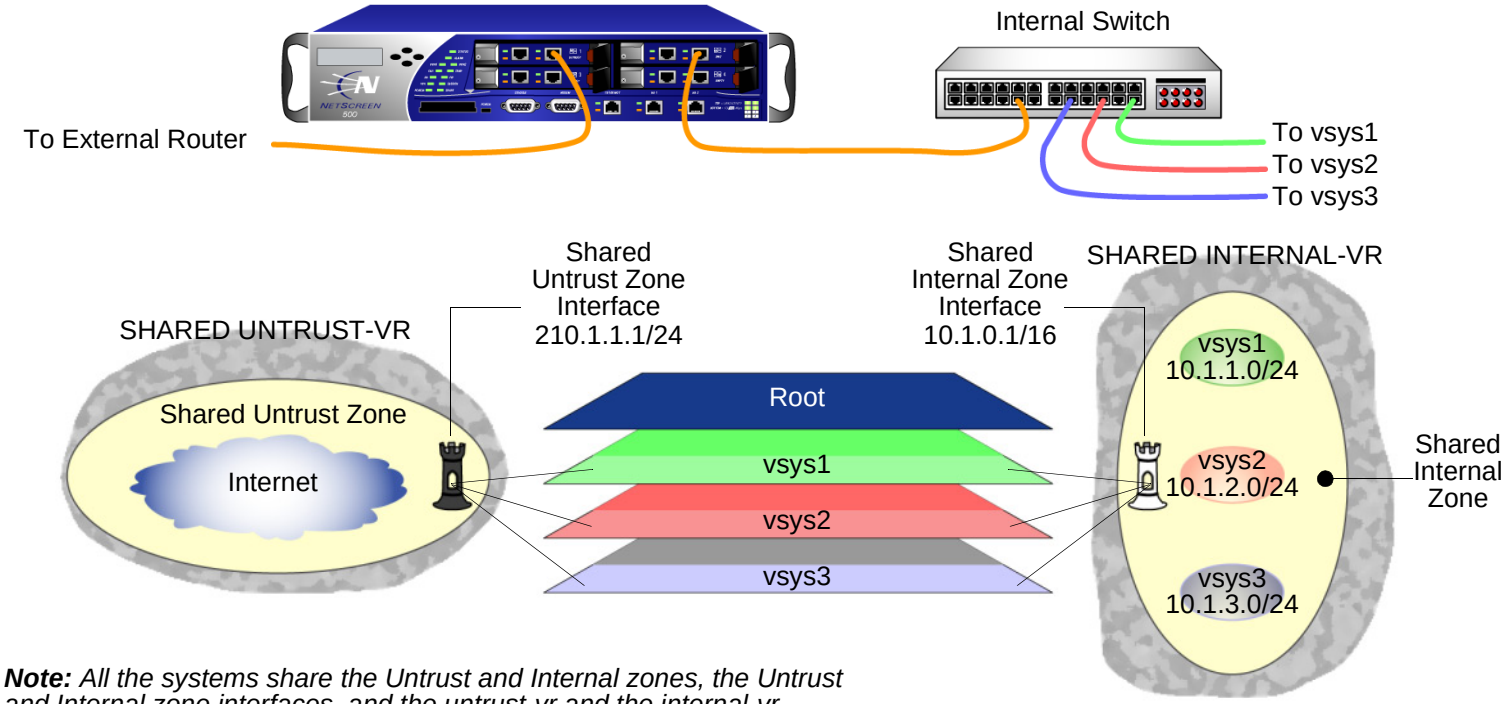
4. Vsys2 Policy

   ```
   set policy from untrust to trust-vsys2 work_js ftp_server ftp-get permit
   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 interface[16]



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

16. 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 do either of the following at the root level:

WebUI

Network > Zones > Edit (for *zone*) > IP Classification: Enter the following, and then click **OK**:

System: (select **root** or ***vsys_name_str***)

Address Type: (select **Subnet** and enter ***ip_addr/mask***, or select **Range** and enter ***ip_addr1*** – ***ip_addr2***)

CLI

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: Vsys Objects and 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

1. Virtual Routers, Security Zones, and Interfaces

Network > Routing > Virtual Routers > Edit (for trust-vr): Select the **Shared and accessible by other vsys** check box, and then click **OK**.

Network > Zones > New: Enter the following, and then click **OK**:

Zone Name: Internal

Virtual Router Name: trust-vr

Zone Type: Layer 3

Network > Zones > Edit (for Internal): Select the **Share Zone** check box, and then click **OK**.

Network > Interfaces > Edit (for ethernet3/2): Enter the following, and then click **OK**:

Zone Name: Internal

IP Address/Netmask: 10.1.0.1/16

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

Zone Name: Untrust

IP Address/Netmask: 210.1.1.1/24

2. Route

Network > Routing > Routing Entries > 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

3. IP Classification of the Trust Zone

Network > Zones > Edit (for Internal) > IP Classification: Enter the following, and then click **OK**:

System: vsys1

Address Type:

Subnet: (select); 10.1.1.0/24

Network > Zones > Edit (for Internal) > IP Classification: Enter the following, and then click **OK**:

System: vsys2

Address Type:

Subnet: (select); 10.1.2.0/24

Network > Zones > Edit (for Internal) > IP Classification: Enter the following, and then click **OK**:

System: vsys3

Address Type:

Subnet: (select); 10.1.3.0/24

Network > Zones > Edit (for Internal): Select the **IP Classification** check box, and then click **OK**.

CLI

1. Virtual Routers, Security Zones, and Interfaces

```
set vrouter trust-vr shared
set zone name Internal
set zone Internal shared
set interface ethernet3/2 zone Internal
set interface ethernet3/2 ip 10.1.0.1/16
set interface ethernet3/2 nat
set interface ethernet1/2 zone untrust
set interface ethernet1/2 ip 210.1.1.1/24
```

2. Route

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

3. IP Classification of the Trust Zone

```
set zone Internal ip-classification net 10.1.1.0/24 vsys1
set zone Internal ip-classification net 10.1.2.0/24 vsys2
set zone Internal ip-classification net 10.1.3.0/24 vsys3
set zone Internal ip-classification
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 I6Dls13guh, 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

1. Logging On

In the URL field in your Web browser, enter the Untrust zone interface IP address for vsys1.

When the Network Password dialog box appears, enter the following, and then click **OK**:

User Name: jsmith

Password: Pd50iH10

2. Changing your Password

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

Vsys Admin Old Password: Pd50iH10

Vsys Admin New Password: I6Dls13guh

Confirm New Password: I6Dls13guh

3. Logging Out

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

CLI

1. Logging On

From a Secure Command Shell (SCS), Telnet, or HyperTerminal session command-line prompt, enter the Untrust zone interface IP address for vsys1.

Log on with the following user name and password:

- User Name: jsmith
- Password: Pd50iH10

2. Changing your Password

```
set admin password I6Dls13guh
save
```

3. Logging Out

```
exit
```

Index