FortiGate VLANs and VDOMs

Version 4.0

Guide

FORTINET

UNIFIED THREAT MANAGEMENT SOLUTIONS

FortiGate VLANs and VDOMs Guide

Version 4.0

21 July 2009

01-40000-83388-20090721

Trademarks

Contents

Introduction

This guide provides detailed information about FortiGate VLANs and VDOMs. It is intended for administrators who need guidance on solutions to suit different network needs and information on basic and advanced configuration of VLANs and VDOMs.

Virtual Local Area Networks (VLANs) and Virtual Domains (VDOMs) multiply the capabilities of your FortiGate unit by using virtualization to partition your resources.

VLANs follow the IEEE 802.1Q standard and increase the number of network interfaces beyond the physical connections on your FortiGate unit.

VDOMs enable your FortiGate unit to split its resources and function as multiple independent units with common administration.

This chapter includes the following topics:

Before you begin

Before you begin using this guide, take a moment to note the following:

- The information in this guide applies to all FortiGate units. All FortiGate models except the FortiGate-30B model support VDOMs, and all FortiGate models support VLANs.
- By default, your FortiGate unit supports a maximum of 10 VDOMs in any combination of NAT/Route and Transparent operating modes. For FortiGate models numbered 3000 and higher, you can purchase a license key to increase the maximum number to 25, 50, 100 or 250 VDOMs.
- This guide uses a FortiGate-800 for examples and procedures. The interface names on some models will vary. For example, some models do not have interfaces labeled external or internal.
- Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This document describes how to implement VLAN technology on FortiGate units operating in both NAT/Route, and Transparent mode. It also describes how to use VDOMs on FortiGate units to provide separate network protection, routing, and VPN configurations.

This document contains the following chapters:

Introduction to VLANs and VDOMs provides an overview of the VLAN and VDOM technologies, some of the concepts and rules for using them. We recommend that you begin with this chapter before attempting to configure your FortiGate unit to use VLANs and VDOMs.

Using VLANs in NAT/Route mode and Using VDOMs in NAT/Route mode provides detailed explanations and basic and advanced examples for configuring these features in your FortiGate unit using the NAT/Route mode.

Inter-VDOM routing describes inter-VDOM routing concepts and scenarios, and gives examples that illustrate them.

Using VLANs and VDOMs in Transparent mode provides detailed explanations, as well as basic and advanced examples for configuring these features in your FortiGate unit using Transparent mode.

Avoiding problems with VLANs explains how to avoid or handle problems that may arise when using VLANs such as asymmetric routing, layer-2 traffic being blocked, and Split Tree Protocol (STP) packet forwarding.

Document conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Cautions, Notes and Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Note: Presents useful information, usually focused on an alternative, optional method, such as a shortcut, to perform a step.

Tip: Highlights useful additional information, often tailored to your workplace activity.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From *Minimum log level*, select *Notification*.

CLI input*	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system settings`
	`comments  : (null)`
	`opmode  : nat`

Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>` `<BODY><H4>You must authenticate to use this service.</H4>`
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com.
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to *VPN* > *IPSEC* > *Auto Key (IKE)*.
Publication	For details, see the *FortiGate Administration Guide*. **Note:** Links typically go to the most recent version. To access earlier releases, go to http://docs.fortinet.com/. This link appears at the bottom of each page of this document.
Global	The chapter or section contains VDOM configuration settings, see "VDOM settings" on page 22.
VDOM	The chapter or section contains Global configuration settings, see "Global settings" on page 25.

* For conventions used to represent command syntax, see "CLI command syntax" on page 10

CLI command syntax

This guide uses the following conventions to describe syntax to use when entering commands in the Command Line Interface (CLI).

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as <address_ipv4>, indicate which data types or string patterns are acceptable value input.

For more information, see the *FortiGate CLI Reference*.

Table 2: Command syntax

Convention	Description
Square brackets [ ]	A non-required word or series of words. For example: [verbose {1 | 2 | 3}] indicates that you may either omit or type both the verbose word and its accompanying option, such as: verbose 3
Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: <retries_int> indicates that you should enter a number of retries, such as 5. Data types include: • <xxx_name>: A name referring to another part of the configuration, such as policy_A. • <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route. • <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as *@example.com to match all email addresses ending in @example.com. • <xxx_fqdn>: A fully qualified domain name (FQDN), such as mail.example.com. • <xxx_email>: An email address, such as admin@mail.example.com. • <xxx_ipv4>: An IPv4 address, such as 192.168.1.99. • <xxx_ipv4range>: An IPv4 address range. • <xxx_v4mask>: A dotted decimal IPv4 netmask, such as 255.255.255.0. • <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0. • <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as 192.168.1.99/24. • <xxx_ipv6>: An IPv6 address. • <xxx_v6mask>: A dotted decimal IPv6 netmask. • <xxx_ipv6mask>: A dotted decimal IPv6 address and netmask separated by a space. • <xxx_str>: A string of characters that is ***not*** another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences • <xxx_int>: An integer number that is ***not*** another data type, such as 15 for the number of minutes.
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].

Table 2: Command syntax

	Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

	Options delimited by spaces	Non-mutually exclusive options. For example:
		`{http https ping snmp ssh telnet}`
		indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
		`ping https ssh`
		Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:
		`ping https snmp ssh`
		If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Fortinet products End User License Agreement

See the *Fortinet products End User License Agreement*.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article What does Fortinet Technical Support require in order to best assist the customer?

Training

Fortinet Training Services provides a variety of training programs to serve the needs of our customers and partners world-wide. Visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

Fortinet documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

Tools and Documentation CD

The documentation for your product is available on the Fortinet Tools and Documentation CD shipped with your product. The documents on this CD are current at shipping time. For the most current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com

Introduction to VLANs and VDOMs

Virtual Local Area Networks (VLANs) and Virtual Domains (VDOMs) multiply the capabilities of your FortiGate unit. Both VDOMs and VLANs can also provide added network security.

Virtual LANs (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs can provide separate firewall policies and, in NAT/Route mode, completely separate configurations for routing and VPN services for each connected network or organization.

This chapter provides an introduction to VLANs and VDOMs and includes the following topics:

Before you begin

Before you begin using this guide, take a moment to note the following:

- The information in this guide applies to all FortiGate units. All FortiGate models except the FortiGate-30B model support VDOMs, and all FortiGate models support VLANs.
- By default, your FortiGate unit supports a maximum of 10 VDOMs in any combination of NAT/Route and Transparent operating modes. For FortiGate models numbered 3000 and higher, you can purchase a license key to increase the maximum number to 25, 50, 100 or 250 VDOMs.
- This guide uses a FortiGate-800 for examples and procedures. The interface names on some models will vary. For example, some models do not have interfaces labeled external or internal.
- Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators and are described in this chapter.

Virtual LANs

A Local Area Network (LAN) is a group of connected computers and devices that are arranged into network broadcast domains. A LAN broadcast domain includes all the computers that receive a packet broadcast from any computer in that broadcast domain. A switch will automatically forward the packets to all of its ports; in contrast, routers do not automatically forward network broadcast packets. This means routers separate broadcast domains. If a network has only switches and no routers, that network is considered one broadcast domain, no matter how large or small it is. Smaller broadcast domains are more efficient because fewer devices receive unnecessary packets. They are more secure as well because a hacker reading traffic on the network will have access to only a small portion of the network instead of the entire network's traffic.

Virtual LANs (VLANs) use ID tags to logically separate a LAN into smaller broadcast domains. Each VLAN is its own broadcast domain. Smaller broadcast domains reduce traffic and increase network security. The IEEE 802.1Q standard defines VLANs. All layer-2 and layer-3 devices along a route must be 802.1Q-compliant to support VLANs along that route. For more information, see "VLAN layer-2 switching" on page 14 and "VLAN layer-3 routing" on page 16.

VLANs reduce the size of the broadcast domains by only forwarding packets to interfaces that are part of that VLAN or part of a VLAN trunk link. Trunk links form switch-to-switch or switch-to-router connections, and forward traffic for all VLANs. This enables a VLAN to include devices that are part of the same broadcast domain, but physically distant from each other.

VLAN ID tags consist of a 4-byte frame extension that switches and routers apply to every packet sent and received in the VLAN. Workstations and desktop computers, which are commonly originators or destinations of network traffic, are not an active part of the VLAN process—all the VLAN tagging and tag removal is done after the packet has left the computer. For more information, see "Rules for VLAN IDs" on page 19.

Any FortiGate unit (without VDOMs enabled) or VDOM can have a maximum of 255 interfaces in Transparent operating mode. In NAT/Route operating mode, the number can range from 255 to 8192 interfaces per VDOM, depending on the FortiGate model. These numbers include VLANs, other virtual interfaces, and physical interfaces. To have more than 255 interfaces configured in Transparent operating mode, you need to configure multiple VDOMs with many interfaces on each VDOM. For more information, see "Increasing the number of VDOMs" on page 65.

One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

Note: This guide uses the term packet to refer to both layer-2 frames and layer-3 packets.

This section contains the following topics:

VLAN layer-2 switching

Ethernet switches are layer-2 devices, and generally are 802.1Q compliant. Layer 2 refers to the second layer of the seven layer Open Systems Interconnect (OSI) basic networking model—the Data Link layer. FortiGate units act as layer-2 switches or bridges when they are in Transparent mode—the units simply tag and forward the VLAN traffic or receive and remove the tags from the packets. A layer-2 device does not inspect incoming packets or change their contents; it only adds or removes tags and routes the packet.

A VLAN can have any number of physical interfaces assigned to it. Multiple VLANs can be assigned to the same physical interface. Typically two or more physical interfaces are assigned to a VLAN, one for incoming and one for outgoing traffic. Multiple VLANs can be configured on one FortiGate unit, including trunk links.

Layer-2 VLAN example

To better understand VLAN operation, let's look at what happens to a data frame on a network that uses VLANs.

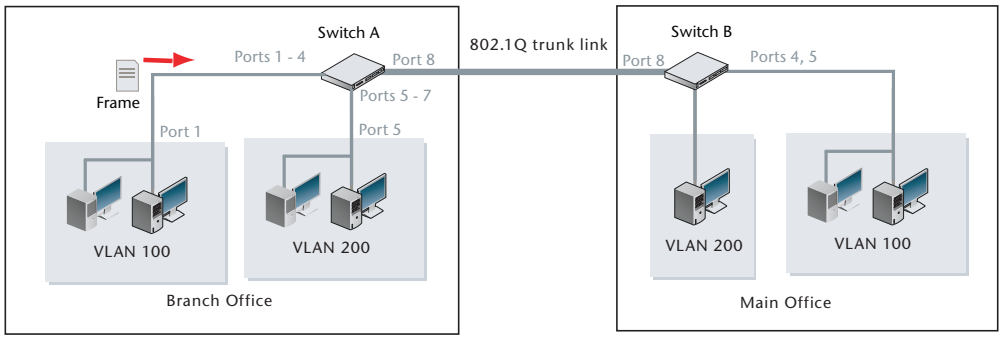
The network topology consists of two 8-port switches that are configured to support VLANs on a network. Both switches are connected through port 8 using an 802.1Q trunk link. Subnet 1 is connected to switch A, and subnet 2 is connected to switch B. The ports on the switches are configured as follows.

Table 3: How ports and VLANs are used on Switch A and B

Switch	Ports	VLAN
A	1 - 4	100
A	5 - 7	200
A & B	8	Trunk link
B	4 - 5	100
B	6	200

Let's follow the steps a data frame follows when it is sent from a computer on subnet 1 that is part of VLAN 100. In this example, switch A is connected to the Branch Office and switch B to the Main Office.

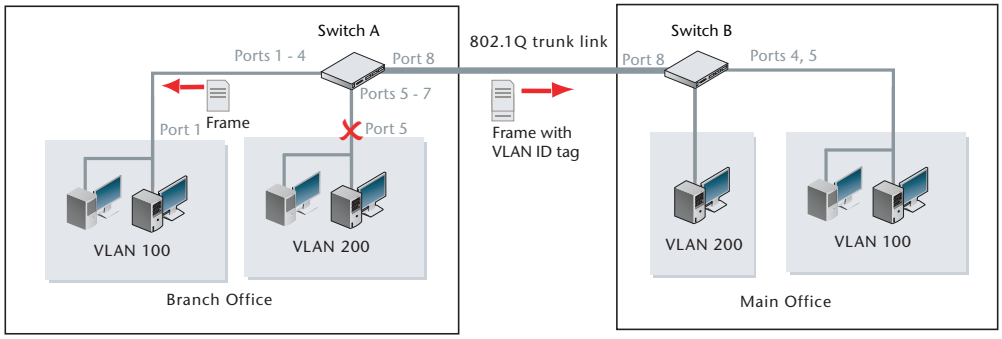
1 A computer on port 1 of switch A sends a data frame over the network.



2 Switch A tags the data frame with a VLAN 100 ID tag upon arrival because port 1 is part of VLAN 100.

3 Switch A forwards the tagged data frame to the other VLAN 100 ports—ports 2 through 4. Switch A also forwards the data frame to the 802.1Q trunk link (port 8) so other parts of the network that may contain VLAN 100 groups will receive VLAN 100 traffic.

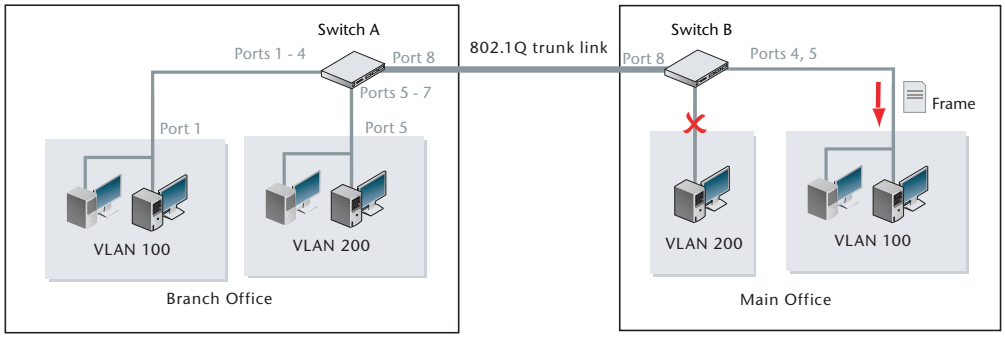
This data frame is not forwarded to the other ports on switch A because they are not part of VLAN 100. This increases security and decreases network traffic.



4 Switch B receives the data frame over the trunk link (port 8).

5 Because there are VLAN 100 ports on switch B (ports 4 and 5), the data frame is forwarded to those ports. As with switch A, the data frame is not delivered to VLAN 200.

If there were no VLAN 100 ports on switch B, the switch would not forward the data frame and it would stop there.



6 The switch removes the VLAN 100 ID tag before it forwards the data frame to an end destination.

The sending and receiving computers are not aware of any VLAN tagging on the data frames that are being transmitted. When any computer receives that data frame, it appears as a normal data frame.

VLAN layer-3 routing

Routers are layer-3 devices. Layer 3 refers to the third layer of the OSI networking model—the Network layer. FortiGate units in NAT/Route mode act as layer-3 devices. As with layer 2, FortiGate units acting as layer-3 devices are 802.1Q-compliant.

The main difference between layer-2 and layer-3 devices is how they process VLAN tags. Layer-2 switches just add, read and remove the tags. They do not alter the tags or do any other high-level actions. Layer-3 routers not only add, read and remove tags but also analyze the data frame and its contents. This analysis allows layer-3 routers to change the VLAN tag if it is appropriate and send the data frame out on a different VLAN.

In a layer-3 environment, the 802.1Q-compliant router receives the data frame and assigns a VLAN ID. The router then forwards the data frame to other members of the same VLAN broadcast domain. The broadcast domain can include local ports, layer-2 devices and layer-3 devices such as routers and firewalls. When a layer-3 device receives the data frame, the device removes the VLAN tag and examines its contents to decide what to do with the data frame. The layer-3 device considers:

- source and destination addresses
- protocol
- port number.

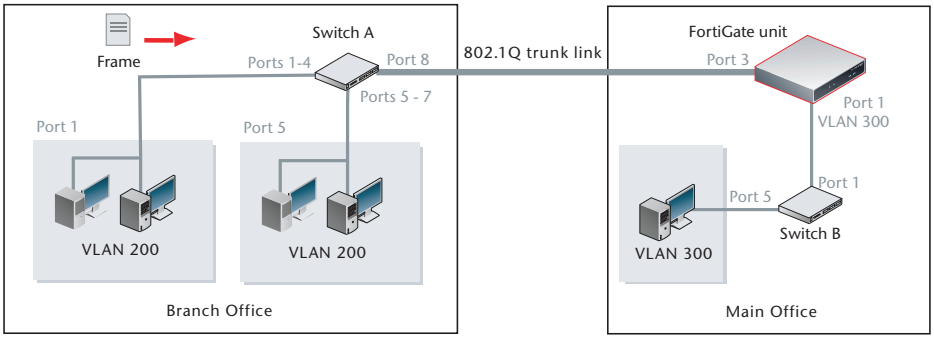
The data frame may be forwarded to another VLAN, sent to a regular non-VLAN-tagged network or just forwarded to the same VLAN as a layer-2 switch would do. Or, the data frame may be discarded if the proper firewall policy has been configured to do so.

Layer-3 VLAN example

In the following example, switch A is connected to the Branch Office subnet, the same as subnet 1 in the layer-2 example. In the Main Office subnet, VLAN 300 is on port 5 of switch B. The FortiGate unit is connected to switch B on port 1 and the trunk link connects the FortiGate unit's port 3 to switch A. The other ports on switch B are unassigned.

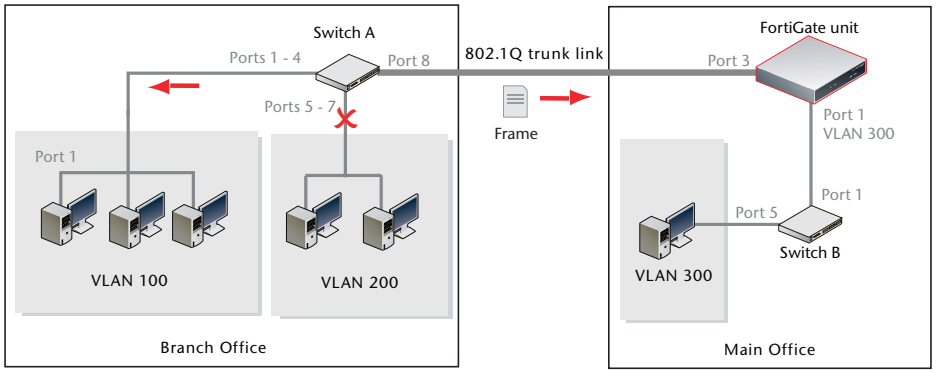
This example explains how traffic can change VLANs—originating on VLAN 100 and arriving at a destination on VLAN 300. Layer-2 switches alone cannot accomplish this, but a layer-3 router can.

1 The VLAN 100 computer at the Branch Office sends the data frame to switch A, where the VLAN 100 tag is added.



2 Switch A forwards the tagged data frame to the FortiGate unit over the 802.1Q trunk link, and to the VLAN 100 interfaces on Switch A.

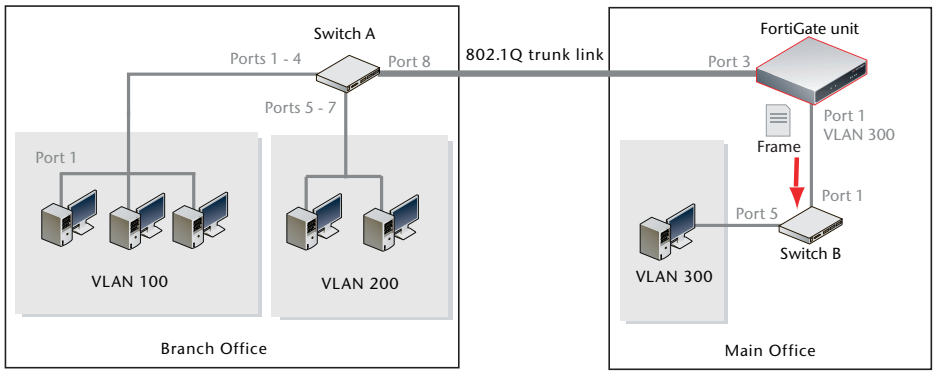
Up to this point everything is the same as in the layer-2 example.



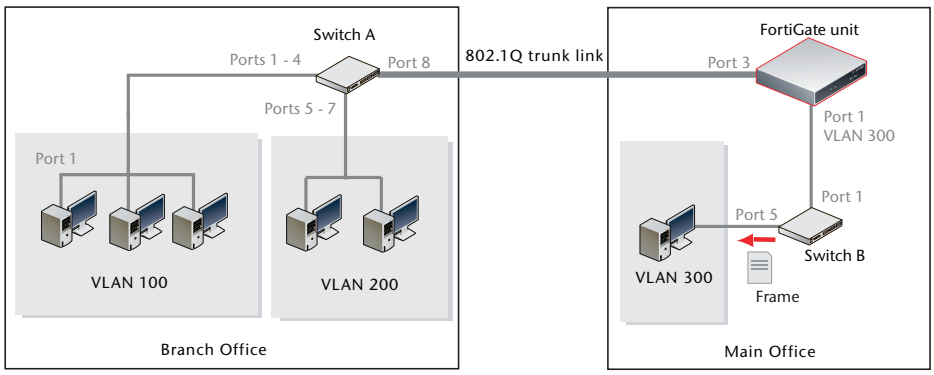
3 The FortiGate unit removes the VLAN 100 tag, and inspects the content of the data frame. The FortiGate unit uses the content to select the correct firewall policy and routing options.

4 The FortiGate unit's firewall policy allows the data frame to go to VLAN 300 in this example. The data frame will be sent to all VLAN 300 interfaces, but in the example there is only one—port 1 on the FortiGate unit. Before the data frame leaves, the FortiGate unit adds the VLAN ID 300 tag to the data frame.

This is the step that layer 2 cannot do. Only layer 3 can retag a data frame as a different VLAN.



5 Switch B receives the data frame, and removes the VLAN ID 300 tag, because this is the last hop, and forwards the data frame to the computer on port 5.



In this example, a data frame arrived at the FortiGate unit tagged as VLAN 100. After checking its content, the FortiGate unit retagged the data frame for VLAN 300. It is this change from VLAN 100 to VLAN 300 that requires a layer-3 routing device, in this case the FortiGate unit. Layer-2 switches cannot perform this change.

Rules for VLAN IDs

Layer-2 switches and layer-3 devices add VLAN ID tags to the traffic as it arrives and remove them before they deliver the traffic to its final destination. Devices such as PCs and servers on the network do not require any special configuration for VLANs.

On a layer-2 switch, you can have only one VLAN subinterface per physical interface, unless that interface is configured as a trunk link. Trunk links can transport traffic for multiple VLANs to other parts of the network.

On a FortiGate unit, you can add multiple VLANs to the same physical interface. However, VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID or have IP addresses on the same subnet. You can add VLAN subinterfaces with the same VLAN ID to different physical interfaces.

Twelve bits of the 4-byte VLAN tag are reserved for the VLAN ID number. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved.

Creating VLAN subinterfaces with the same VLAN ID does not create any internal connection between them. For example a VLAN ID of 300 on port1 and VLAN ID of 300 on port2 are allowed, but they are not connected. Their relationship is the same as between any two FortiGate network interfaces.

For more information on VLANs, see the “Using VLANs in NAT/Route mode”, “Using VLANs and VDOMs in Transparent mode”, and “Avoiding problems with VLANs” chapters.

Virtual Domains

Virtual Domains (VDOMs) provide a way to divide your FortiGate unit and operate it as multiple separate units. You can configure and manage many features such as interfaces, VLAN subinterfaces, zones, firewall policies, routing, antispam, web filter, logging, reporting, and VPN configurations separately for each VDOM. This separation simplifies configuration because you do not have to manage many settings, such as routes or firewall policies, at one time.

One application of this capability is to use a single FortiGate unit to provide routing and network protection for several organizations. Each organization has its own network interfaces (physical or virtual), routing requirements, and network protection rules. By default, communication between organizations is possible only if both allow access to an external network such as the Internet. The chapter, "Using VDOMs in NAT/Route mode" on page 59 provides two examples of this application.

When a packet enters a VDOM, it is confined to that VDOM; you can create firewall policies for connections only between virtual LAN subinterfaces or zones in that VDOM. The security of the FortiGate unit is preserved—the packet never crosses VDOM borders.

The maximum number of VDOMs supported by your FortiGate unit is displayed under *System* > *Status* > *License Information* > *Virtual Domain*. By default, your FortiGate unit supports a maximum of 10 VDOMs in any combination of NAT/Route and Transparent operating modes. For FortiGate models numbered 3000 and higher, you can purchase a license key to increase the maximum number to 25, 50, 100 or 250 VDOMs. For more information, see "Creating, disabling, and deleting VDOMs" on page 63.

This section contains the following topics:

Management VDOM

All management traffic leaves the FortiGate unit through the management VDOM. Management traffic includes all external logging, remote management, and other Fortinet services.

The management VDOM must have access to the Internet, so that various services such as FortiGuard services and network time protocol (NTP) can function properly.

By default, the management VDOM is the root VDOM. However, you can change the management VDOM so management traffic will originate from the new VDOM. For more information, see "Changing the management VDOM" on page 69.

Administration of VDOMs

When VDOMs are enabled, only a super_admin account has access to the global settings and all VDOM settings, and can therefore administer the FortiGate unit and all VDOM accounts. Other, separate administrators for each VDOM can administer only the VDOMs to which they have access. By default the super_admin account is the "admin" account. For more information on global settings, see "Global settings" on page 25.

Caution: Exercise extreme caution when changing super_admin accounts, especially the default "admin" account. Make careful note of administrators and their passwords. You may accidently remove all access to your FortiGate unit and be required to call support to re-gain access. Any configuration changes you have made may also be lost as this process will reset your FortiGate unit to factory default settings.

You can use super_admin accounts to create other non-super_admin administrator accounts and assign them to VDOMs. Each administrator account can configure and manage only the VDOM assigned to that account. VDOM administrators do not have permission to change global properties, as those properties affect all VDOMs and not just the current VDOM.

You can use super_admin accounts to configure read-only or read/write access profiles for all administrators using those profiles. You can configure combinations of access features that include:

- maintenance
- system configuration
- security policies
- logging and reporting
- user authorization
- administrator management
- configuration backup/restore.

This makes it possible for you to have administrators for different services on each VDOM. For example, you can configure one administrator to be responsible for logs and reporting on a VDOM, while another administrator is responsible for security policies on that same VDOM. For more information, see the *FortiGate Administration Guide*.

When you are configuring VDOMs using a super_admin account, the web-based manager shows which VDOM you are currently editing, at the bottom of the left menu with the label *Current VDOM:* followed by the name of the VDOM. To move from within a VDOM to global properties, select << *Global* at the bottom of the left menu options. If you are configuring global properties, there is no VDOM indicator and no << *Global* in the left menu.

For more information on VDOM administration, see “Getting started with VDOMs” on page 60.

Inter-VDOM routing

When VDOM link virtual interfaces are configured with proper firewall policies, traffic can pass between VDOMs without using a physical interface. All this inter-VDOM traffic must pass through firewall policies to ensure security, just like traffic does with all external interface connections.

Using inter-VDOM routing allows you to free up physical interfaces. Another benefit is that the internal interfaces you replace them with are faster and configuration is more flexible. You can also continue to use secure firewall policies.

For more information, see “Inter-VDOM routing” on page 125, and the chapter “Creating VDOM administrators” in the *FortiGate CLI Reference*.

Global and VDOM settings

Settings configured outside of a VDOM are called global settings. Global settings affect the entire FortiGate unit and include areas such as interfaces, HA, maintenance, antivirus, and logging.

Settings configured within a VDOM are called VDOM settings. VDOM settings affect only the specific VDOM you are currently editing and include areas such as operating mode, routing, firewall, VPN, some antivirus, some logging, and reporting.

Generally, system configuration (such as HA settings) is set at the global level, and settings that customize specific behavior and traffic controls (such as firewall and UTM settings) are set at the VDOM level.

Both FortiGate online help and the *FortiGate Administration Guide* include icons that show which chapters and sections are global or VDOM. VDOM and global icons appear in the *FortiGate Administration Guide* to indicate a chapter or section of a chapter is part of the VDOM configuration or the global configuration.

Table 4: Global and VDOM icons

When you select help for a global configuration web-based manager page the help display includes the global icon.	
When you select help for a VDOM configuration web-based manager page, the help display includes the VDOM icon.	

At the CLI level, this distinction is made through the location of a command. Global commands are in the `config global` top level command tree, where VDOM specific commands are in the `config vdom` command tree.

For more information on a configuration settings topic, see chapters with similar names or associated with specific menus in the *FortiGate Administration Guide*.

This section includes:

- VDOM settings
- Global settings

VDOM settings

To configure and use VDOMs, you must enable virtual domains on the *System* > *Status* dashboard, or from the CLI enter `config system global, set vdom-admin`.

The following settings are exclusively part of a virtual domain and are not shared between virtual domains. A regular administrator for the VDOM sees only these settings. The default super_admin account can also access these settings, but must first select which VDOM to configure.

Table 5: Settings available to a VDOM-only administrator (specified VDOM)

Menu	Configuration Settings
System	Zone Web Proxy Routing Table (Transparent mode) Modem Wireless DHCP Operation mode (NAT/Route or Transparent) Management IP (Transparent mode)
Router	Static Dynamic Monitor
Firewall	Policy Address Service Schedule Traffic Shaper Virtual IP Load Balance Protection Profile
UTM	AntiVirus Intrusion Protection Web Filter AntiSpam Data Leak Protection Application Control

Table 5: Settings available to a VDOM-only administrator (specified VDOM)

Menu	Configuration Settings
VPN	IPSec SSL
User	Local Remote Directory Service PKI User Group Options Monitor
Wan Opt. & Cache	Rule Peer Monitor Cache
End Point Control	Endpoints FortiClient Software Detection
Log & Report	Log Config Log Access Content Archive Report Config Report Access

Global settings

The following settings affect all virtual domains on the FortiGate unit. When VDOMs are enabled, only accounts with the default super_admin profile can access global settings.

Table 6: Settings available to a super_admin administrator (VDOMs enabled)

Menu	Configuration Object
System	Physical and virtual interfaces
	DNS settings
	Dead gateway detection
	Host name
	System Time
	Firmware version
	Idle and authentication timeout
	Web-based manager language
	LCD panel PIN, where applicable
	Wireless Settings, where applicable
	VDOM
	Global Resources
	HA configuration
	SNMP configuration
	Replacement messages
	Administrators
	Certificates
	Central Management
	Maintenance
User	Dynamic Profile
UTM	AntiVirus, Quarantine
	AntiVirus, Configuration
	Antivirus, Grayware
Log & Report	Log Configuration

Using VLANs in NAT/Route mode

In NAT/Route mode the FortiGate unit functions as a layer-3 device. In this mode, the unit controls the flow of packets between VLANs, but can also remove VLAN tags from incoming VLAN packets. The FortiGate unit can also forward untagged packets to other networks, such as the Internet.

In NAT/Route mode, the FortiGate unit supports VLAN trunk links with IEEE 802.1Q-compliant switches, or routers. The trunk link transports VLAN-tagged packets between physical subnets or networks. When you add VLAN sub-interfaces to the FortiGate unit physical interfaces, the VLANs have IDs that match the VLAN IDs of packets on the trunk link. The FortiGate unit directs packets with VLAN IDs to sub-interfaces with matching IDs.

You can define VLAN sub-interfaces on all FortiGate physical interfaces. However, if multiple virtual domains are configured on the FortiGate unit, you will have access to only the physical interfaces on your virtual domain. The FortiGate unit can tag packets leaving on a VLAN subinterface. It can also remove VLAN tags from incoming packets and add a different VLAN tag to outgoing packets.

Normally in VLAN configurations, the FortiGate unit's internal interface is connected to a VLAN trunk, and the external interface connects to an Internet router that is not configured for VLANs. In this configuration the FortiGate unit can apply different policies for traffic on each VLAN interface connected to the internal interface, which results in less network traffic and better security.

This section includes:

Before you begin

This chapter and the examples in it include the following assumptions.

- You have not enabled VDOM configuration on your FortiGate unit. If you have enabled it, you will need to navigate to the global or VDOM configuration as needed before following each procedure.
- Examples are based on the FortiGate-800 model. Depending on your FortiGate model, interface names may vary. For example, some models do not have interfaces named internal or external internal.
- This chapter does not explain how to configure the protection profiles for virus scanning, web filtering and spam filtering. For more information, see *FortiGate Administration Guide*.

Configuring your FortiGate unit

In NAT/Route mode, you can access the FortiGate unit's web-based manager (GUI) with a supported web browser that connects to a FortiGate unit interface. The interface must be configured for administrative access. Use HTTPS to access the address of the interface. All FortiGate units have administrative access enabled by default on the default interface. On the FortiGate-800 the default interface is the internal interface. For the examples presented in this chapter, the default interface has an address of 192.168.1.99.

For more information, see the *Quick Start Guide* or the *Installation Guide* that came with your FortiGate unit.

Configuring your FortiGate unit for VLANs includes:

- Adding VLAN subinterfaces
- Configuring firewall policies and routing

Adding VLAN subinterfaces

A VLAN subinterface, sometimes called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.

Adding a VLAN subinterface includes configuring the

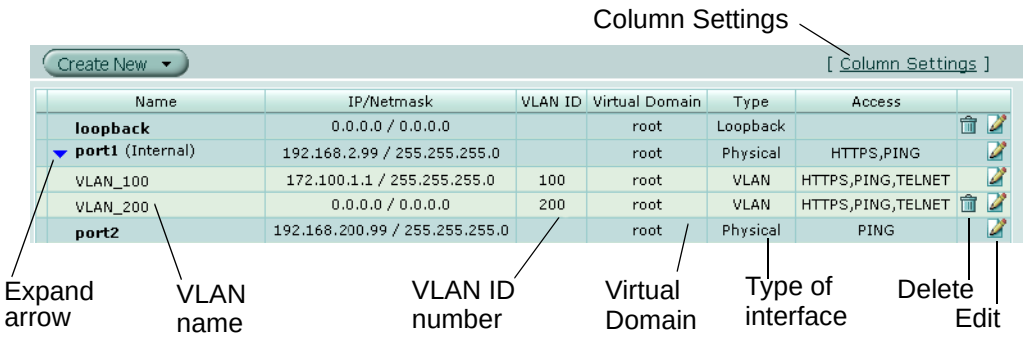
- Physical interface
- IP address and netmask
- VLAN ID
- VDOM.

Physical interface

The term VLAN subinterface correctly implies the VLAN interface is not a complete interface by itself. You add a VLAN subinterface to the physical interface that receives VLAN-tagged packets. The physical interface can belong to a different VDOM than the VLAN, but it must be connected to a network route that is configured for this VLAN. Without that route, the VLAN will not be connected to the network, and VLAN traffic will not be able to access this interface.The traffic on the VLAN is separate from any other traffic on the physical interface.

When you are working with interfaces on your FortiGate unit, we recommend checking the *Column Settings* on the Interface display to make sure the information you need is displayed. Besides customizing this display, you can also re-order the columns to focus on the important information for each interface. When working with VLANs, it is useful to position the *VLAN ID* column close to the IP address. If you are working with VDOMs, including the *Virtual Domain* column as well will help you troubleshoot problems more quickly. To view the Interface display, go to *System* > *Network*.

Figure 1: Organizing columns on the interface display



IP address and netmask

FortiGate unit interfaces cannot have overlapping IP addresses—the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to virtual interfaces such as VLAN subinterfaces. Each VLAN subinterface must be configured with its own IP address and netmask pair. This rule helps prevent a broadcast storm or other similar network problems. For more information on troubleshooting VLAN networking problems, see “Avoiding problems with VLANs” on page 193.

Note: If you are unable to change your existing configurations to prevent IP overlap, enter the CLI command `config system global` and `set ip-overlap enable` to allow IP address overlap. If you enter this command, multiple VLAN interfaces can have an IP address that is part of a subnet used by another interface. This command is recommended for advanced users only.

VLAN ID

The VLAN ID is part of the VLAN tag added to the packets by VLAN switches and routers. The VLAN ID is a number between 1 and 4094 that allow groups of IP addresses with the same VLAN ID to be associated together. VLAN ID 0 is used only for high priority frames, and 4095 is reserved.

All devices along a route must support the VLAN ID of the traffic along that route. Otherwise, the traffic will be discarded before reaching its destination. For example, if your computer is part of VLAN_100 and a co-worker on a different floor of your building is also on the same VLAN_100, you can communicate with each other over VLAN_100, only if all the switches and routers support VLANs and are configured to pass along VLAN_100 traffic properly. Otherwise, any traffic you send your co-worker will be blocked or not delivered.

VDOM

If VDOMs are enabled, each VLAN subinterface must belong to a VDOM. This rule also applies for physical interfaces.

Note: Interface-related CLI commands require a VDOM to be specified, regardless of whether the FortiGate unit has VDOMs enabled.

VLAN subinterfaces on separate VDOMs cannot communicate directly with each other. In this situation, the VLAN traffic must exit the FortiGate unit and re-enter the unit again, passing through firewalls in both directions. This situation is the same for physical interfaces.

A VLAN subinterface can belong to a different VDOM than the physical interface it is part of. This is because the traffic on the VLAN is handled separately from the other traffic on that interface. This is one of the main strengths of VLANs. For more information on VDOMs, see “Creating, disabling, and deleting VDOMs” on page 63.

The following procedure will add a VLAN subinterface called VLAN_100 to the FortiGate internal interface with a VLAN ID of 100. It will have an IP address and netmask of 172.100.1.1/255.255.255.0, and allow HTTPS, PING, and TELNET administrative access. Note that in the CLI, you must enter “`set type vlan`” before setting the vlanid, and that the allowaccess protocols are lower case.

To add a VLAN subinterface in NAT/Route mode - web-based manager

1 If *<<Global* appears in the left menu, select it to enter global configuration.

2 Go to *System* > *Network* > *Interface*.

3 Select *Create New* to add a VLAN subinterface.

4 Enter the following:

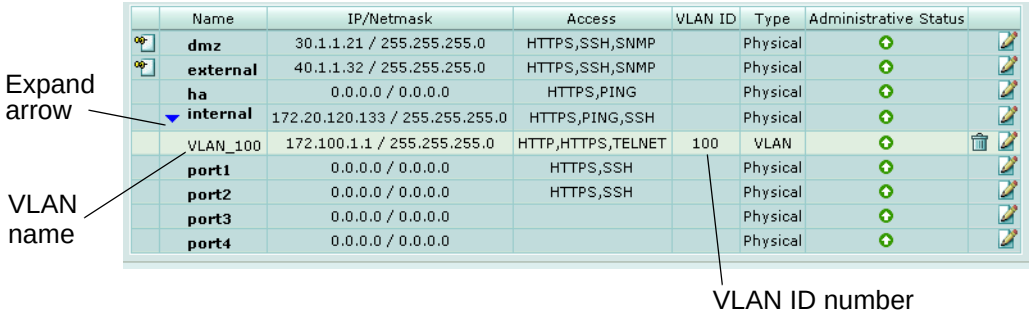
VLAN Name	VLAN_100
Type	VLAN
Interface	internal
VLAN ID	100
Addressing Mode	Manual
IP/Netmask	172.100.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

5 Select *OK*.

To view the new VLAN subinterface, select the expand arrow next to the parent physical interface (the internal interface). This will expand the display to show all VLAN subinterfaces on this physical interface. If there is no expand arrow displayed, there are no subinterfaces configured on that physical interface.

For each VLAN, the list displays the name of the VLAN, and, depending on column settings, its IP address, the Administrative access you selected for it, the VLAN ID number, and which VDOM it belongs to if VDOMs are enabled.

Figure 2: Viewing the new VLAN subinterface



To add a VLAN subinterface in NAT/Route mode - CLI

```
config system interface
  edit VLAN_100
    set interface internal
    set type vlan
    set vlanid 100
    set ip 172.100.1.1 255.255.255.0
    set allowaccess https ping telnet
  next
end
```

Configuring firewall policies and routing

Once you have created a VLAN subinterface on the FortiGate unit, you need to configure firewall policies and routing for that VLAN. Without these, the FortiGate unit will not pass VLAN traffic to its intended destination.

Firewall policies direct traffic through the FortiGate unit between interfaces. Routing directs traffic across the network.

This section includes the following topics:

- Configuring firewall policies
- Configuring routing

Configuring firewall policies

Firewall policies permit communication between the FortiGate unit's network interfaces based on source and destination IP addresses. Without firewall policies, traffic will not pass through the FortiGate unit. Firewall policies also allow you to limit communication at particular times and limit services to specific protocols. Interfaces that communicate with the VLAN interface need firewall policies to permit traffic to pass between them and the VLAN interface.

Each VLAN needs a firewall policy for each of the following connections the VLAN will be using:

- from this VLAN to an external network
- from an external network to this VLAN
- from this VLAN to another VLAN in the same virtual domain on the FortiGate unit
- from another VLAN to this VLAN in the same virtual domain on the FortiGate unit.

The packets on each VLAN are subject to antivirus scans and other UTM measures as they pass through the FortiGate unit.

For more information on firewall policies, see the firewall chapter of the *FortiGate Administration Guide*.

Configuring routing

As a minimum, you need to configure a default static route to a gateway with access to an external network for outbound packets. In more complex cases, you will have to configure different static or dynamic routes based on packet source and destination addresses.

As with firewalls, you need to configure routes for VLAN traffic. VLANs need routing and a gateway configured to send and receive packets outside their local subnet just as physical interfaces do. The type of routing you configure, static or dynamic, will depend on the routing used by the subnet and interfaces you are connecting to. Dynamic routing can be routing information protocol (RIP), border gateway protocol (BGP), open shortest path first (OSPF), or multicast.

If you enable SSH, PING, TELNET, HTTPS and HTTP on the VLAN, you can use those protocols to troubleshoot your routing and test that it is properly configured. Enabling logging on the interfaces and using CLI diag commands such as `diag sniff packet <interface_name>` can also help locate any possible configuration or hardware issues.

Routing and logging are explained in the *FortiGate Administration Guide* and the *FortiGate CLI Reference*.

Example VLAN configuration in NAT/Route mode

In this example two different internal VLAN networks share one interface on the FortiGate unit, and share the connection to the Internet.

This configuration could apply to two departments in a single company, or to different companies. The main point is that the networks can keep their traffic separate while sharing one FortiGate interface.

This section includes the following topics:

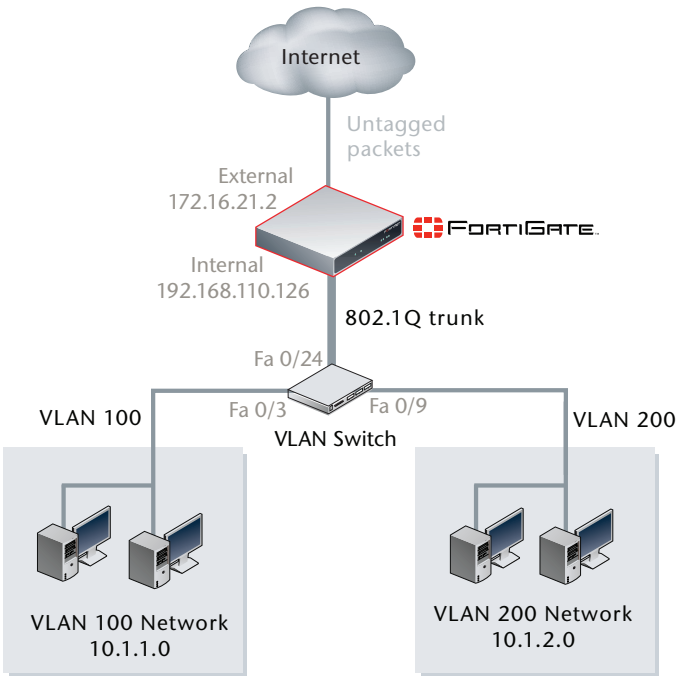
Network topology and assumptions

There are two different internal network VLANs in this example. VLAN_100 is on the 10.1.1.0/255.255.255.0 subnet, and VLAN_200 is on the 10.1.2.0/255.255.255.0 subnet. These VLANs are connected to the VLAN switch, such as a Cisco 2950 Catalyst switch.

The FortiGate internal interface connects to the VLAN switch through an 802.1Q trunk. The internal interface has an IP address of 192.168.110.126 and is configured with two VLAN subinterfaces (VLAN_100 and VLAN_200). The external interface has an IP address of 172.16.21.2 and connects to the Internet. The external interface has no VLAN subinterfaces on it.

Figure 3 shows the configuration for this example.

Figure 3: FortiGate unit with VLANs in NAT/Route mode



When the VLAN switch receives packets from VLAN_100 and VLAN_200, it applies VLAN ID tags and forwards the packets of each VLAN both to local ports and to the FortiGate unit across the trunk link. The FortiGate unit has policies that allow traffic to flow between the VLANs, and from the VLANs to the external network.

This section describes how to configure a FortiGate-800 unit and a Cisco Catalyst 2950 switch for this example network topology. The Cisco configuration commands used in this section are IOS commands. It is assumed that both the FortiGate-800 and the Cisco 2950 switch are installed and connected and that basic configuration has been completed. On the switch, you will need to be able to access the CLI to enter commands. Refer to the manual for your FortiGate model as well as the manual for the switch you select for more information.

It is also assumed that no VDOMs are enabled.

This section includes the following topics:

- Configuring the FortiGate unit
- Configuring the VLAN switch
- Testing the configuration

General configuration steps

The following steps provide an overview of configuring and testing the hardware used in this example. For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configuring the FortiGate unit
   - Configuring the external interface
   - Adding two VLAN subinterfaces to the internal network interface
   - Adding firewall addresses and address ranges for the internal and external networks
   - Adding firewall policies to allow:
     - the VLAN networks to access each other
     - the VLAN networks to access the external network.
2. Configuring the VLAN switch
3. Testing the configuration.

Configuring the FortiGate unit

Configuring the FortiGate unit includes:

- Configuring the external interface
- Adding VLAN subinterfaces
- Adding the firewall addresses
- Adding the firewall policies

Configuring the external interface

The FortiGate unit's external interface will provide access to the Internet for all internal networks, including the two VLANs.

To configure the external interface - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select *Edit* for the external interface.
3. Enter the following information and select *OK*:

Addressing mode	Manual
IP/Netmask	172.16.21.2/255.255.255.0

To configure the external interface - CLI

```
config system interface
  edit external
    set mode static
    set ip 172.16.21.2 255.255.255.0
end
```

Adding VLAN subinterfaces

This step creates the VLANs on the FortiGate unit internal physical interface. The IP address of the internal interface does not matter to us, as long as it does not overlap with the subnets of the VLAN subinterfaces we are configuring on it.

The rest of this example shows how to configure the VLAN behavior on the FortiGate unit, configure the switches to direct VLAN traffic the same as the FortiGate unit, and test that the configuration is correct.

Adding VLAN subinterfaces can be completed through the web-based manager, or the CLI.

To add VLAN subinterfaces - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select *Create New*.
3. Enter the following information and select *OK*:

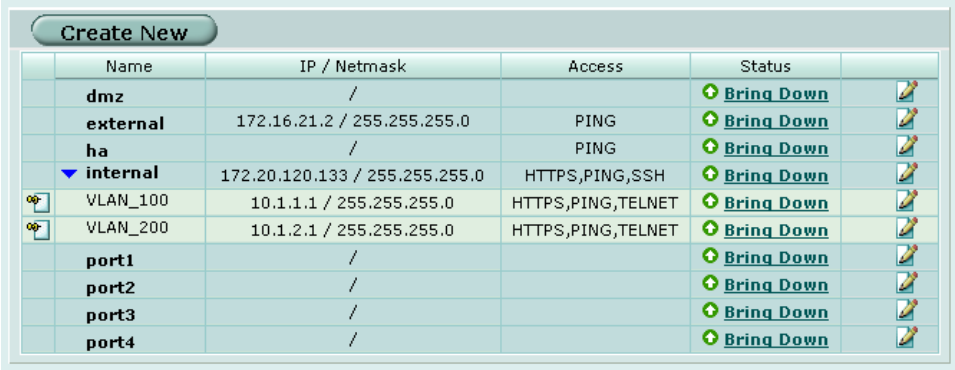
Name	VLAN_100
Interface	internal
VLAN ID	100
Addressing mode	Manual
IP/Netmask	10.1.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

4. Select *Create New*.

5 Enter the following information and select *OK*:

Name	VLAN_200
Interface	internal
VLAN ID	200
Addressing mode	Manual
IP/Netmask	10.1.2.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

Figure 4: VLAN subinterfaces



To add VLAN subinterfaces - CLI

```
config system interface
  edit VLAN_100
    set vdom root
    set interface internal
    set type vlan
    set vlanid 100
    set mode static
    set ip 10.1.1.1 255.255.255.0
    set allowaccess https ping telnet
  next
  edit VLAN_200
    set vdom root
    set interface internal
    set type vlan
    set vlanid 200
    set mode static
    set ip 10.1.2.1 255.255.255.0
    set allowaccess https ping telnet
end
```

Adding the firewall addresses

You need to define the addresses of the VLAN subnets for use in firewall policies. The FortiGate unit provides one default address, “all”, that you can use when a firewall policy applies to all addresses as a source or destination of a packet. However, using “all” is less secure and should be avoided when possible.

In this example, the "_Net" part of the address name indicates a range of addresses instead of a unique address. When choosing firewall address names, keep them informative and unique.

To add the firewall addresses - web-based manager

1 Go to *Firewall* > *Address*.

2 Select *Create New*.

3 Enter the following information and select *OK*:

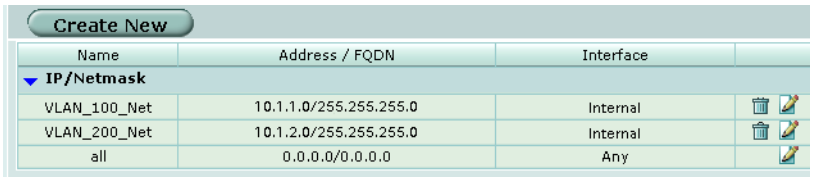
Address Name	VLAN_100_Net
Type	Subnet / IP Range
Subnet / IP Range	10.1.1.0/255.255.255.0

4 Select *Create New*.

5 Enter the following information and select *OK*:

Address Name	VLAN_200_Net
Type	Subnet / IP Range
Subnet / IP Range	10.1.2.0/255.255.255.0

Figure 5: Firewall addresses for VLAN_100 and VLAN_200



To add the firewall addresses - CLI

```
config firewall address
  edit VLAN_100_Net
    set type ipmask
    set subnet 10.1.1.0 255.255.255.0
  next
  edit VLAN_200_Net
    set type ipmask
    set subnet 10.1.2.0 255.255.255.0
end
```

Adding the firewall policies

Once you have assigned addresses to the VLANs, you need to configure firewall policies for them to allow valid packets to pass from one VLAN to another and to the Internet.

Note: You can customize the Firewall Policy display by including some or all columns, and customize the column order onscreen. Due to this feature, firewall policy screenshots may not appear the same as on your screen.

If you do not want to allow all services on a VLAN, you can create a firewall policy for each service you want to allow. This example allows all services.

To add the firewall policies - web-based manager

1 Go to *Firewall* > *Policy*.

2 Select *Create New*.

3 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_100
Source Address	VLAN_100_Net
Destination Interface/Zone	VLAN_200
Destination Address	VLAN_200_Net
Schedule	Always
Service	ANY
Action	ACCEPT

4 Select *Create New*.

5 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200
Source Address	VLAN_200_Net
Destination Interface/Zone	VLAN_100
Destination Address	VLAN_100_Net
Schedule	Always
Service	ANY
Action	ACCEPT

6 Select *Create New*.

7 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_100
Source Address	VLAN_100_Net
Destination Interface/Zone	external
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

8 Select *Create New*.

9 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200
Source Address	VLAN_200_Net
Destination Interface/Zone	external
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

To add the firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_100
    set srcaddr VLAN_100_Net
    set dstintf VLAN_200
    set dstaddr VLAN_200_Net
    set schedule always
    set service ANY
    set action accept
    set status enable
  next
  edit 2
    set srcintf VLAN_200
    set srcaddr VLAN_200_Net
    set dstintf VLAN_100
    set dstaddr VLAN_100_Net
    set schedule always
    set service ANY
    set action accept
    set status enable
  next
  edit 3
    set srcintf VLAN_100
    set srcaddr VLAN_100_Net
    set dstintf external
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set status enable
  next
  edit 4
    set srcintf VLAN_200
    set srcaddr VLAN_200_Net
    set dstintf external
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set status enable
end
```

Configuring the VLAN switch

On the Cisco Catalyst 2950 Catalyst VLAN switch, you need to define VLANs 100 and 200 in the VLAN database, and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

One method to configure a Cisco switch is to connect over a serial connection to the console port on the switch, and enter the commands at the CLI. Another method is to designate one interface on the switch as the management interface and use a web browser to connect to the switch's graphical interface. For details on connecting and configuring your Cisco switch, refer to the installation and configuration manuals for the switch.

The switch used in this example is a Cisco Catalyst 2950 switch. The commands used are IOS commands. Refer to the switch manual for help with these commands.

To configure the VLAN subinterfaces and the trunk interfaces

Add this file to the Cisco switch:

```
!
interface FastEthernet0/3
  switchport access vlan 100
!
interface FastEthernet0/9
  switchport access vlan 200
!
interface FastEthernet0/24
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 100
Port 0/9	VLAN ID 200
Port 0/24	802.1Q trunk

Note: To complete the setup, configure devices on VLAN_100 and VLAN_200 with default gateways. The default gateway for VLAN_100 is the FortiGate VLAN_100 subinterface. The default gateway for VLAN_200 is the FortiGate VLAN_200 subinterface.

Testing the configuration

Use diagnostic commands, such as `tracert`, to test traffic routed through the FortiGate unit and the Cisco switch. Testing includes:

- Testing traffic from VLAN_100 to VLAN_200
- Testing traffic from VLAN_200 to the external network

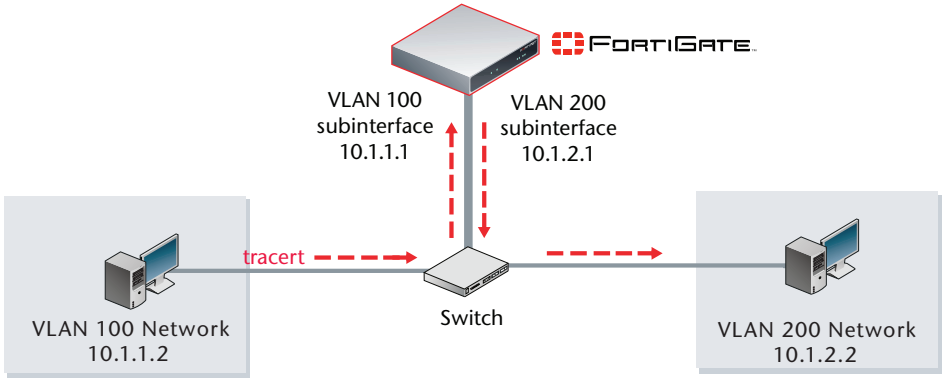
Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between the two internal networks. The route target is a host on VLAN_200.

Access a command prompt on a Windows computer on the VLAN_100 network, and enter the following command:

```
C:\>tracert 10.1.2.2
Tracing route to 10.1.2.2 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.1.1.1
  2   <10 ms   <10 ms   <10 ms  10.1.2.2
Trace complete.
```

Figure 6: Example tracert from VLAN_100 to VLAN_200



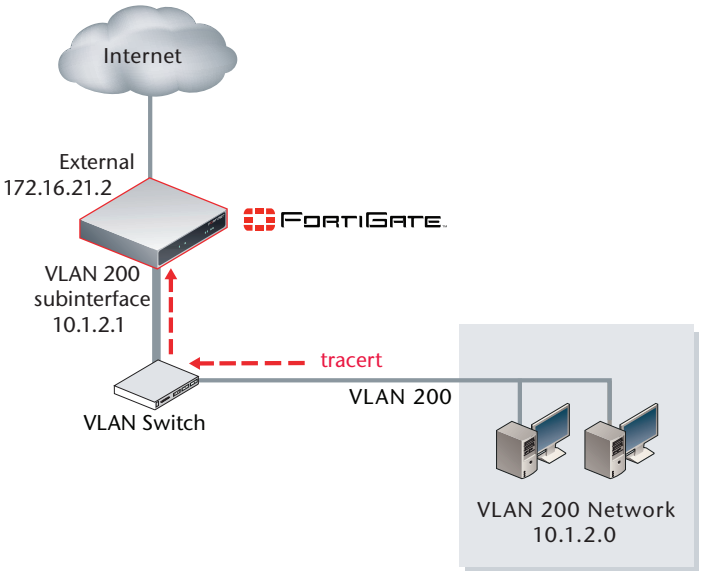
Testing traffic from VLAN_200 to the external network

In this example, a route is traced from an internal network to the external network. The route target is the external network interface of the FortiGate-800 unit.

From VLAN_200, access a command prompt and enter this command:

```
C:\>tracert 172.16.21.2
Tracing route to 172.16.21.2 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.1.2.1
  2   <10 ms   <10 ms   <10 ms  172.16.21.2
Trace complete.
```

Figure 7: Example trace route from VLAN_200 to the external network



Example VLAN configuration in NAT/Route mode (advanced)

In this example, a company called Example Inc. has two networks within the company—one for financial employees and one for everyone else (local users). The financial employees have a number of security policies and procedures that apply only to them and their network. This extra security means that the company has two Internet service providers—one high security (XO ISP) and one normal security (ATT ISP). The high security ISP costs more to use, so all possible traffic will go through the ATT-ISP to save money. Several employees need to access the local users' internal network from outside the company, so a VPN connection is required.

VLANs enable sharing of FortiGate interfaces while keeping traffic separate and enabling separate firewall policies. In general, VLANs enable a more efficient network solution.

This example includes the following sections:

Network topology and assumptions

VLANs are used to help keep the traffic from the two networks, and to keep two ISP connections separate and secure.

Table 7: Network and VLAN configuration details

Network	VLAN ID	IP subnet
Local User	10	192.168.10.0/255.255.255.0
Finance	20	172.100.10.0/255.255.255.0
ATT ISP	30	30.1.1.0/255.255.255.0
XO ISP	40	40.1.1.0/255.255.255.0

The ATT ISP IP address, for the ISP external to the FortiGate unit, is 30.1.1.2, and the IP address for XO ISP is 40.1.1.2.

In this example, a FortiGate unit operates in NAT/Route mode mainly to provide firewall and VLAN services. All traffic from VLANs 10 and 20 come in on the FortiGate unit's internal interface, and all traffic from VLANs 30 and 40 come in on the external interfaces.

The unit is configured with firewall policies that control the flow of traffic between networks. The Finance network is the most secure network. It allows outbound traffic to all other networks, but it does not allow inbound traffic. The Local users network allows outbound traffic to the external networks (ATT ISP and XO ISP), inbound traffic from the Finance network and a single inbound connection from a VPN client on the ATT ISP network.

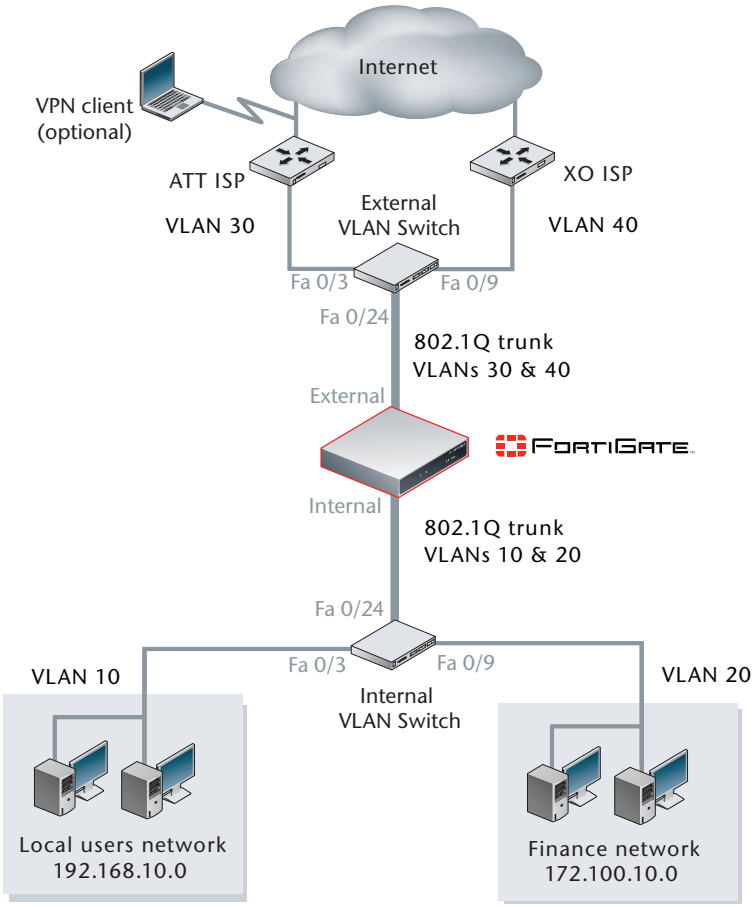
Note: If your network does not use VPN configurations, you can leave out the VPN configuration section of this example. It has been included for completeness, but is not required. If you do use VPN, you will require the FortiClient application.

For easier tracking of IP addresses, all IP addresses assigned to VLAN subinterfaces on the FortiGate unit will end in ".1", as in 30.1.1.1 or 172.100.10.1.

This section describes how to configure a FortiGate unit and two 802.1Q-compliant Cisco switches for the example network topology shown in Figure 8. Other 802.1Q-compliant switches can be used; however their configuration is not included in this example.

No VDOMs are enabled.

Figure 8: Example VLAN topology (FortiGate unit in NAT/Route mode)



General configuration steps

The following steps break down the configuration for this VLAN example into smaller sections, each with a number of smaller procedures. For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configuring FortiGate interfaces and routing
2. Configuring FortiGate firewalls
3. Configuring the VLAN switches
4. Testing the configuration
5. Configuring the FortiGate unit IPSec VPN
6. Configuring the VPN client

Configuring FortiGate interfaces and routing

Configuring the FortiGate unit includes:

- Adding the VLAN subinterfaces
- Adding a default route

Adding the VLAN subinterfaces

VLAN subinterfaces connect the FortiGate unit to the rest of the VLAN network.

Note: When working with many VLANs, it is good to use *Column Settings* to show the VLAN ID and interface type on the interface list screen. This will allow you to identify the interface you are looking for more quickly. Screen shots in this example will include this column.

To add the VLAN subinterfaces - web-based manager

1 Go to *System* > *Network* > *Interface*.

2 Select *Create New*.

3 Enter the following information for the Local users network and select *OK*:

Name	Local-LAN
Interface	internal
VLAN ID	10
Addressing mode	Manual
IP/Netmask	192.168.10.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

4 Select *Create New*.

5 Enter the following information for the Finance network and select *OK*:

Name	Finance
Interface	internal
VLAN ID	20
Addressing mode	Manual
IP/Netmask	172.100.10.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

6 Select *Create New*.

7 Enter the following information for the ATT ISP network and select *OK*:

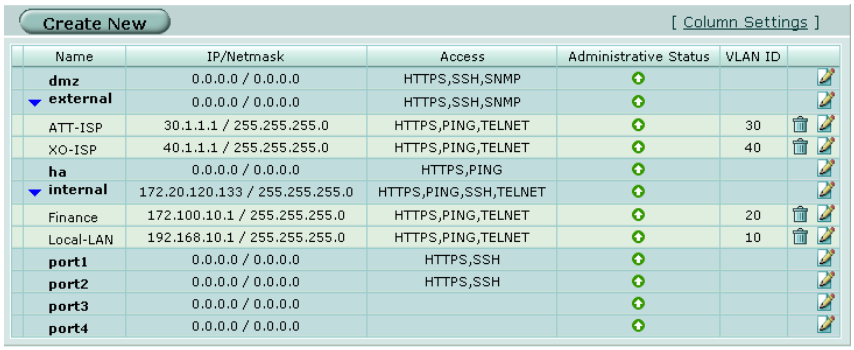
Name	ATT-ISP
Interface	external
VLAN ID	30
Addressing mode	Manual
IP/Netmask	30.1.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

8 Select *Create New*.

9 Enter the following information for the XO ISP network and select *OK*:

Name	XO-ISP
Interface	external
VLAN ID	40
Addressing mode	Manual
IP/Netmask	40.1.1.1/255.255.255.0
Access	HTTPS, PING, TELNET

Figure 9: VLAN 10, 20, 30, and 40 subinterfaces configured



To add the VLAN subinterfaces - CLI

```
config system interface
  edit Local-LAN
    set vdom root
    set interface internal
    set type vlan
    set vlanid 10
    set mode static
    set ip 192.168.10.1 255.255.255.0
    set allowaccess https ping telnet
  next
  edit Finance
    set vdom root
    set interface internal
    set type vlan
    set vlanid 20
    set mode static
    set ip 172.100.10.1 255.255.255.0
    set allowaccess https ping telnet
  next
  edit ATT-ISP
    set vdom root
    set interface external
    set type vlan
    set vlanid 30
    set mode static
    set ip 30.1.1.1 255.255.255.0
    set allowaccess https ping telnet
  next
```

```
    edit XO-ISP
      set vdom root
      set interface external
      set type vlan
      set vlanid 40
      set mode static
      set ip 40.1.1.1 255.255.255.0
      set allowaccess https ping telnet
end
```

Adding a default route

Default routes added to the ISP connections enable internal networks to communicate with external networks.

The default routes for each ISP are weighted differently using the distance metric. This means traffic will use ATT-ISP by default, but if it is unavailable XO-ISP will be used instead.

Note: If you wanted both ISPs to be used interchangeably, i.e. for load balancing by session, three things have to be in place: their distances have to be equal, their priorities have to be equal, and load balancing must be turned on. This is known as equal cost configuration. For more information, see the *FortiGate CLI Reference*.

To add a default route - web-based manager

1. Go to *Router* > *Static* > *Static Route*.
2. Select *Create New*.
3. Enter the following information to add a default route to ATT-ISP for network traffic leaving the external interface, and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	ATT-ISP
Gateway	30.1.1.2
Distance	10

4. Enter the following information to add a secondary default route to XO-ISP for network traffic leaving the external interface, and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	XO-ISP
Gateway	40.1.1.2
Distance	20

To add a default route - CLI

```
config router static
  edit 1
    set dst 0.0.0.0/0
    set device ATT-ISP
    set gateway 30.1.1.2
    set distance 10
  next
  edit 2
    set dst 0.0.0.0/0
    set device XO-ISP
    set gateway 40.1.1.2
    set distance 20
end
```

Configuring FortiGate firewalls

Firewalls need to be in place to allow traffic between interfaces on the FortiGate unit. Firewall addresses make configuration easier.

Firewall policies are needed between XO-ISP and the Finance network, the Finance network and the Local users network, and ATT-ISP and the Local users network.

This section includes the following topics:

- Adding the firewall addresses
- Adding the firewall policies

Adding the firewall addresses

Firewall addresses define the IP addresses and subnets where the firewall policies are applied. Before you can configure firewall policies to control inter-VLAN and VLAN-Internet traffic, you need to assign firewall addresses.

To add the firewall addresses - web-based manager

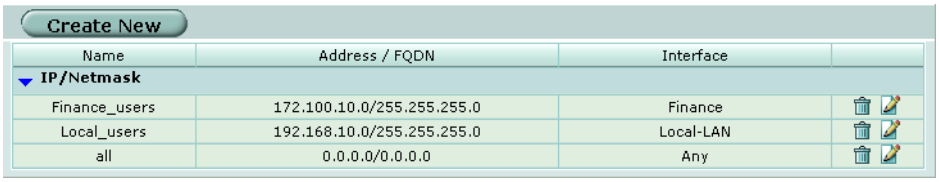
1. Go to *Firewall* > *Address*.
2. Select *Create New*.
3. Enter the following information and select *OK*:

Address Name	Local_users
Type	Subnet / IP Range
Subnet / IP Range	192.168.10.0/255.255.255.0
Interface	Local-LAN

4. Select *Create New*.
5. Enter the following information and select *OK*:

Address Name	Finance_users
Type	Subnet / IP Range
Subnet / IP Range	172.100.10.0/255.255.255.0
Interface	Finance

Figure 10: Firewall addresses for Local_users and Finance_users



To add the firewall addresses - CLI

```
config firewall address
  edit Local_users
    set type ipmask
    set subnet 192.168.10.0 255.255.255.0
  next
  edit Finance_users
    set type ipmask
    set subnet 172.100.10.0 255.255.255.0
end
```

Adding the firewall policies

Firewall policies allow VLAN traffic to move to other VLANs and the Internet. To allow traffic in both directions, you need two policies for each connection, for a total of six configured policies. There are policies to allow traffic between Finance and XO-ISP, XO-ISP and Finance, Finance and Local users, Local users and Finance, Local users and ATT-ISP, and ATT-ISP and Local users.

To add the firewall policies - web-based manager

1. Go to *Firewall* > *Policy*.
2. Select *Create New*.
3. Enter the following information and select *OK*.

   This policy allows the finance network to access the Internet through XO-ISP. Finance does not use ATT-ISP.

Source Interface/Zone	Finance
Source Address	Finance_users
Destination Interface/Zone	XO-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select

4. Select *Create New*.

5 Enter the following information and select *OK*.

This policy allows XO-ISP to access the Finance network.

Source Interface/Zone	XO-ISP
Source Address	all
Destination Interface/Zone	Finance
Destination Address	Finance_users
Schedule	Always
Service	ANY
Action	ACCEPT

6 Select *Create New.*

7 Enter the following information and select *OK*.

This policy allows both internal networks to communicate with each other.

Source Interface/Zone	Finance
Source Address	Finance_users
Destination Interface/Zone	Local-LAN
Destination Address	Local_users
Schedule	Always
Service	ANY
Action	ACCEPT

8 Select *Create New.*

9 Enter the following information and select *OK*.

This policy also allows both internal networks to communicate with each other.

Source Interface/Zone	Local-LAN
Source Address	Local_users
Destination Interface/Zone	Finance
Destination Address	Finance_users
Schedule	Always
Service	ANY
Action	ACCEPT

10 Select *Create New.*

11 Enter the following information and select *OK*.

This policy allows the Local users network to access the Internet through ATT-ISP.

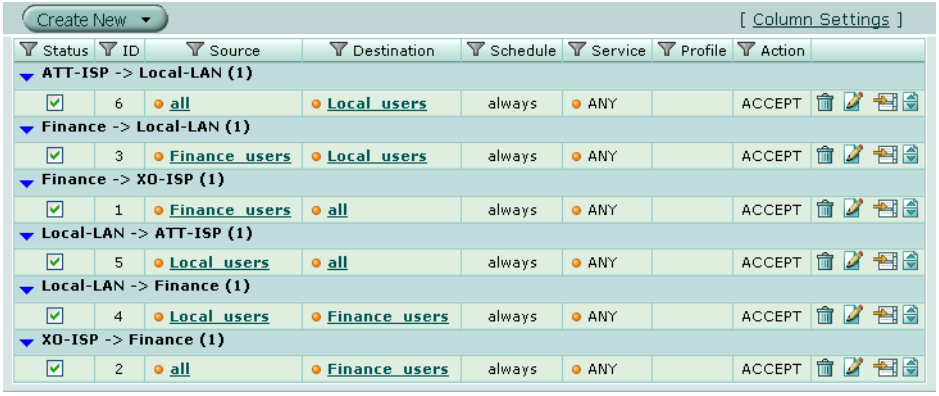
Source Interface/Zone	Local-LAN
Source Address	Local_users
Destination Interface/Zone	ATT-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

12 Select *Create New*.

13 Enter the following information and select *OK*.

Source Interface/Zone	ATT-ISP
Source Address	all
Destination Interface/Zone	Local-LAN
Destination Address	Local_users
Schedule	Always
Service	ANY
Action	ACCEPT

Figure 11: Firewall policies



To add the firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf Finance
    set srcaddr Finance_users
    set dstintf XO-ISP
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set status enable
  next
  edit 2
    set srcintf XO-ISP
    set srcaddr all
    set dstintf Finance
    set dstaddr Finance_users
    set schedule always
    set service ANY
    set action accept
    set status enable
  next
```

```
    edit 3
      set srcintf Finance
      set srcaddr Finance_users
      set dstintf Local-LAN
      set dstaddr Local_users
      set schedule always
      set service ANY
      set action accept
      set status enable
    next
    edit 4
      set srcintf Local-LAN
      set srcaddr Local_users
      set dstintf Finance
      set dstaddr Finance_users
      set schedule always
      set service ANY
      set action accept
      set status enable
    next
    edit 5
      set srcintf Local-LAN
      set srcaddr Local_users
      set dstintf ATT-ISP
      set dstaddr all
      set schedule always
      set service ANY
      set action accept
      set status enable
    end
    edit 6
      set srcintf ATT-ISP
      set srcaddr add
      set dstintf Local-LAN
      set dstaddr Local_users
      set schedule always
      set service ANY
      set action accept
      set status enable
  end
```

Configuring the VLAN switches

You need to configure VLANs 10 and 20 in the VLAN database on the VLAN switch connected to the FortiGate unit's internal interface. Then you need to add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

You need to configure VLANs 30 and 40 in the VLAN database. Then you need to add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

This example uses Cisco IOS commands and a Cisco 2900 series switch.

Configuring the internal VLAN switch

Add this file to the Cisco switch connected to the internal interface:

```
!
interface FastEthernet0/3
switchport access vlan 10
!
interface FastEthernet0/9
switchport access vlan 20
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 10
Port 0/9	VLAN ID 20
Port 0/24	802.1Q trunk

Note: To complete the setup, configure devices on VLAN 10 and VLAN 20 with default gateways. The default gateway for VLAN 10 is the FortiGate VLAN 10 subinterface. The default gateway for VLAN 20 is the FortiGate VLAN 20 subinterface.

Configuring the external VLAN switch

Add this file to the Cisco switch connected to the external interface:

```
!
interface FastEthernet0/3
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 40
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 30
Port 0/9	VLAN ID 40
Port 0/24	802.1Q trunk

Note: To complete the setup, configure devices on VLAN 30 and VLAN 40 with default gateways. The default gateway for VLAN 30 is the FortiGate VLAN 30 subinterface. The default gateway for VLAN 40 is the FortiGate VLAN 40 subinterface.

Testing the configuration

Testing the configuration tests not only the hardware connections, but also the VLAN configurations to ensure all the hardware along a route can successfully pass VLAN traffic as expected.

Use diagnostic commands, such as `tracert`, to test traffic routed through the FortiGate unit and the Cisco switch.

The traffic route tests include:

- Testing traffic from VLAN 20 to VLAN 10
- Testing traffic from VLAN 10 to ATT-ISP

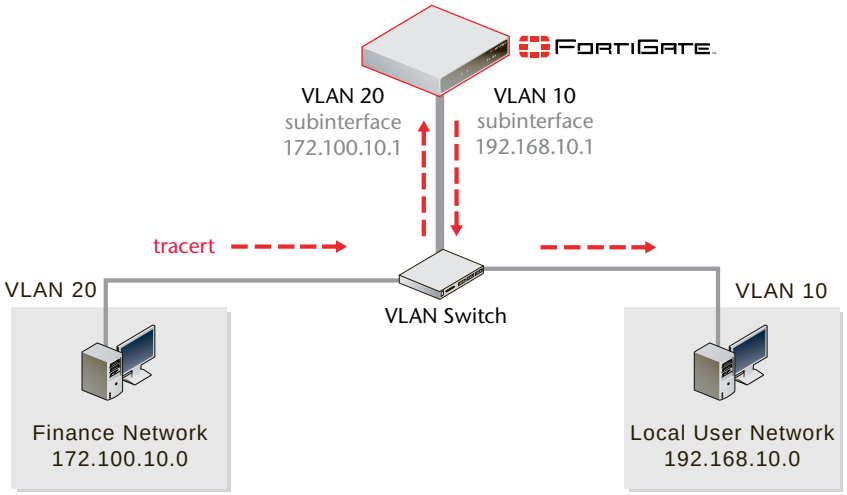
Testing traffic from VLAN 20 to VLAN 10

In this example, a route is traced between the two internal networks. The route target is a host on the Local users network (VLAN 10).

From the Finance network, access a command prompt on a Windows PC and enter this command:

```
C:\>tracert 192.168.10.2
Tracing route to 192.168.10.2 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms 192.168.20.1
  2   <10 ms   <10 ms   <10 ms 192.168.10.2
Trace complete.
```

Figure 12: Example trace route from VLAN 20 to VLAN 10



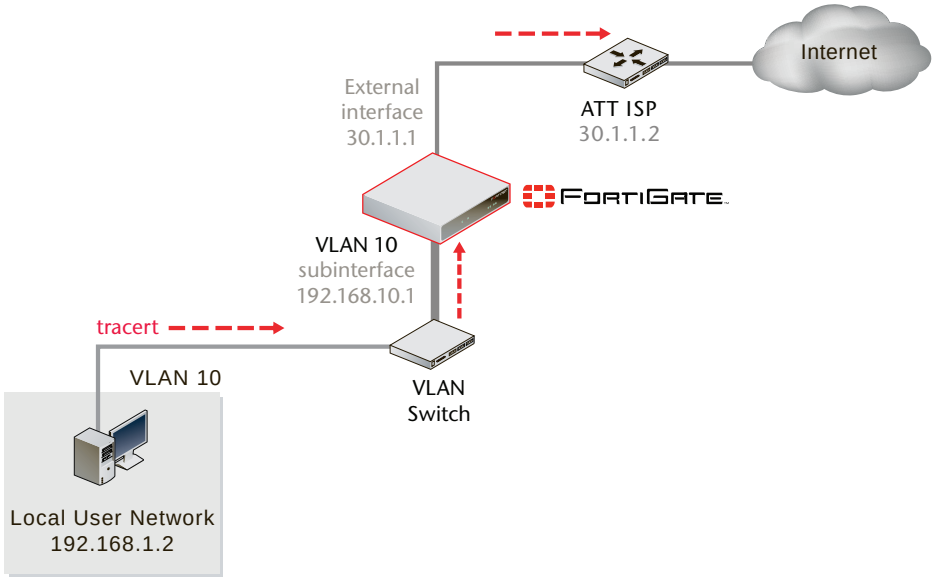
Testing traffic from VLAN 10 to ATT-ISP

In this example, a route is traced from VLAN 10 on an internal network to ATT-ISP on the external network. The route target is the external network interface of the FortiGate unit.

From the Local users network (VLAN 10), access a command prompt on a Windows PC and enter this command:

```
C:\>tracert 30.1.1.2
Tracing route to 30.1.1.2 over a maximum of 30 hops:
  1 <10 ms   <10 ms   <10 ms  192.168.10.1
  2 <10 ms   <10 ms   <10 ms  30.1.1.1
  3 <10 ms   <10 ms   <10 ms  30.1.1.2
Trace complete.
```

Figure 13: Example trace route from VLAN 10 to the external network



Configuring the FortiGate unit IPSec VPN

In this example, one user is allowed to connect to the Local user network through a VPN tunnel from an external dial-up connection. The VPN connection is through ATT-ISP. The FortiGate and Client VPN parts of the network configuration are optional.

For more information on VPN configuration with FortiGate units, see the IPSec VPN User Guide, or the VPN chapter of the *FortiGate Administration Guide* and the *FortiGate CLI Reference*.

This section includes the following topics:

- Configuring the VPN gateway
- Configuring the VPN tunnel
- Adding the encrypt policy

Configuring the VPN gateway

VPN IPSec tunnels are typically built in two phases. The VPN gateway is Phase 1.

Note: To be secure the key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

To configure the VPN gateway - web-based manager

1. Go to *VPN > IPsec > Auto Key (IKE)*.
2. Select *Create Phase 1* and then select *Advanced*.
3. Enter the following information and select *OK*:

Name	Dialup_tunnel
Remote Gateway	Dialup User
Local Interface	ATT-ISP
Mode	Main
Authentication Method	Preshared key
Pre-shared key	Enter “example”. The client must use the same pre-shared key.
Advanced	Advanced values remain at default values.

To configure the VPN gateway - CLI

```
config vpn ipsec phase1
  edit Dialup_tunnel
    set type dynamic
    set mode main
    set authmethod psk
    set psksecret example
end
```

Configuring the VPN tunnel

With the VPN gateway configured, you can configure the VPN tunnel. The VPN tunnel is Phase 2.

To configure the VPN tunnel - web-based manager

1. Go to *VPN > IPsec > Auto Key (IKE)*.
2. Select *Create Phase 2* and then select Advanced.
3. Enter the following information and select *OK*:

Name	Dialup-client
Phase 1	Dialup_tunnel
Advanced	Advanced values remain at default values.

To configure the VPN tunnel - CLI

```
config vpn ipsec phase2
  edit Dialup-client
    set phase1name Dialup_tunnel
  end
```

Adding the encrypt policy

In the encrypt policy, we are using inbound NAT to provide the Local users network IP address. Otherwise we would have to configure a virtual IP (VIP) and assign it to an interface for the VPN client coming in.

To add the encrypt policy - web-based manager

1 Go to *Firewall* > *Policy*.

2 Select *Create New*.

3 Enter the following information and select *OK*:

Source Interface/Zone	Local-LAN
Source Address	Local_users
Destination Interface/Zone	ATT-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	IPSEC
VPN Tunnel	
Allow inbound	Select
Allow outbound	Clear
Inbound NAT	Select
Outbound NAT	Clear

4 Move the policy in the policy list above non-encrypt policies. If there is more than one encrypt policy in the list, place the more specific ones above the more general ones with similar source and destination addresses.

To add the encrypt policy - CLI

```
config firewall policy
  edit 6
    set srcintf Local-LAN
    set srcaddr Local_users
    set dstintf ATT-ISP
    set dstaddr ATT-net
    set schedule always
    set service ANY
    set action ipsec
    set vpntunnel Dialup_tunnel
    set status enable
end
```

Configuring the VPN client

The Local users network configuration allows a single inbound connection from a VPN client on the ATT-ISP network. This part of the network configuration example is optional.

When the VPN user connects to the Local users network and the VPN tunnel is established, the network recognizes the user as being part of the Local users network.

This example shows how to configure FortiClient v4.0 on a computer running Microsoft Windows.

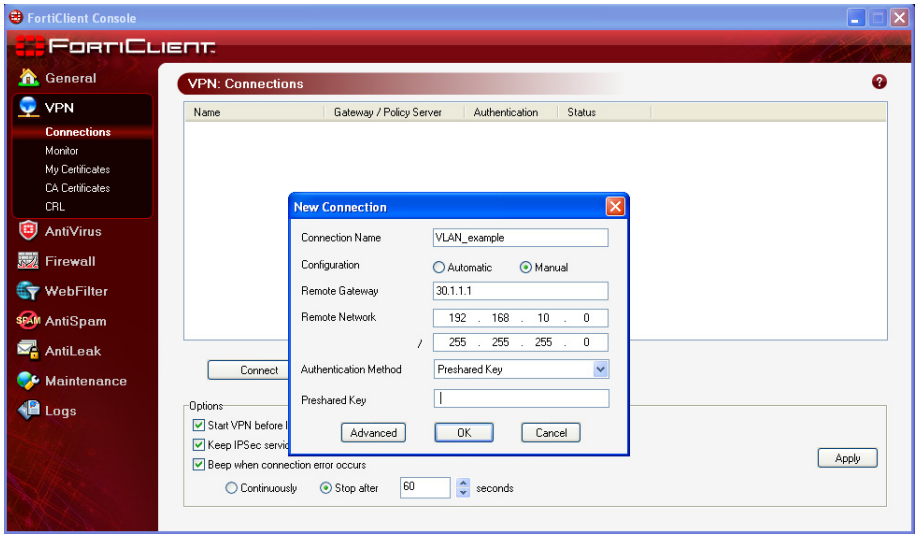
To configure FortiClient as a VPN client

1 Start the FortiClient application.
2 Go to *VPN* > *Connections* and select *Advanced* > *Add*.
3 Enter a name for the connection in the *Connection Name* field.
4 Select *Manual*.
5 For the *Remote Gateway* IP address, enter `30.1.1.1`.
6 For the *Remote Network* address, enter `192.168.10.0/255.255.255.0`.
7 For the *Authentication Method,* select *Preshared Key*.
8 For the *Preshared Key*, enter the pre-shared key.

Note: The pre-shared key must match the FortiGate authentication key.

9 Select *OK*.

Figure 14: New VPN Connection



To test the new VPN connection in FortiClient, highlight the new VPN connection and select *Connect*. A new window will pop up with connection-related messages displayed as each VPN connection phase is attempted and completed. When you have successfully connected, you will be able to access local network resources.

Using VDOMs in NAT/Route mode

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that each function as independent units. Each VDOM has separate routing and firewall policies. A single FortiGate unit with VDOMs enabled is flexible enough to serve multiple departments of an organization, separate organizations, or be the basis for a service provider's managed security service.

Note: The examples in this chapter are intended to be followed in order as procedures build on previous procedures. If you do not complete the previous procedures, the procedure you are working on may not work properly. If this happens, consult previous procedures or FortiGate documentation.

This chapter contains the following sections:

Benefits of VDOMs

VDOMs provide the following benefits:

Easier administration

VDOMs provide separate security domains that allow separate zones, user authentication, firewall policies, routing, and VPN configurations. VDOMs separate security domains and simplify administration of complex configurations—you do not have to manage as many settings at one time. For more information, see "VDOM settings" on page 22.

By default, each FortiGate unit has a VDOM named root. This VDOM includes all of the unit's physical interfaces, modem, VLAN subinterfaces, zones, firewall policies, routing settings, and VPN settings.

Also, you can optionally assign an administrator account restricted to one VDOM. If the VDOM is created to serve an organization, this feature enables the organization to manage its own configuration. For more information, see "Creating VDOM administrators" on page 66.

Management systems such as SNMP, logging, alert email, FDN-based updates, and NTP-based time setting use addresses and routing in the management VDOM to communicate with the network. They can connect only to network resources that communicate with the management VDOM. Using a separate VDOM for management traffic enables easier management of the FortiGate unit global settings, and VDOM administrators can also manage their VDOMs more easily. For more information, see "Changing the management VDOM" on page 69.

Continued security

When a packet enters a VDOM, it is confined to that VDOM and is subject to any firewall policies for connections between VLAN subinterfaces or zones in that VDOM. To travel between VDOMs, a packet must first pass through a firewall on a physical interface. The packet then arrives at another VDOM on that same FortiGate unit, but on a different interface, where it must pass through another firewall before entering. Inter-VDOMs change this limitation because they are internal interfaces; however inter-VDOM packets still require the same security measures as when passing through physical interfaces. For more information see “Configuring firewall policies for a VDOM” on page 83.

VDOMs provide an additional level of security because regular administrator accounts are specific to one VDOM—an administrator restricted to one VDOM cannot change information on another VDOM. Any configuration changes and potential errors will apply only to that VDOM and limit any potential down time

Savings in physical space and power

To increase the number of physical FortiGate units, you need more rack space, cables, and power to install the new units. You also need to change your network configuration to accommodate the new physical units. In the future, if you need fewer physical units you are left with expensive hardware that is idle.

Increasing VDOMs involves no additional hardware, no additional cabling, and very few changes to existing networking configurations. VDOMs save physical space and power. You are limited only by the size of the VDOM license you buy and the physical resources on the FortiGate unit.

By default, FortiGate units support a maximum of 10 VDOMs in any combination of NAT/Route and Transparent modes. For FortiGate models numbered 3000 and higher, you can purchase a license key to increase the maximum number of VDOMs to 25, 50, 100, 250, or 500. For more information on VDOM licences, see “Increasing the number of VDOMs” on page 65.

Getting started with VDOMs

Before using VDOMs, you need to configure your FortiGate unit to operate with VDOMs.

It is assumed that for all procedures after “Enabling VDOM configuration” on page 61 VDOMs are enabled.

You will be:

- Enabling VDOM configuration
- Viewing the VDOM list
- Creating, disabling, and deleting VDOMs
- Increasing the number of VDOMs
- Creating VDOM administrators
- Accessing and configuring VDOMs

Enabling VDOM configuration

When VDOMs are enabled, the web-based manager and the CLI are changed as follows:

- Global and per-VDOM configurations are separated. This is indicated in the *FortiGate Administration Guide* by Global and VDOM icons.
- Only admin accounts using the super_admin profiles can view or configure global options.
- Admin accounts using the super_admin profiles can configure all VDOM configurations.
- All other administrator accounts can configure only the VDOM to which they are assigned.

Using the default admin administration account, you can enable or disable VDOM operation on the FortiGate unit.

Global and per-VDOM settings

Settings configured outside of a VDOM are called global settings. These settings affect the entire FortiGate unit and include areas such as interfaces, HA, maintenance, some antivirus, and some logging. In general, any unit settings that should only be changed by the top level administrator are global settings.

Settings configured within a VDOM are called VDOM settings. These settings affect only that specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, some logging, and reporting.

For more information, see "Global and VDOM settings" on page 21.

To enable VDOM configuration - web-based manager

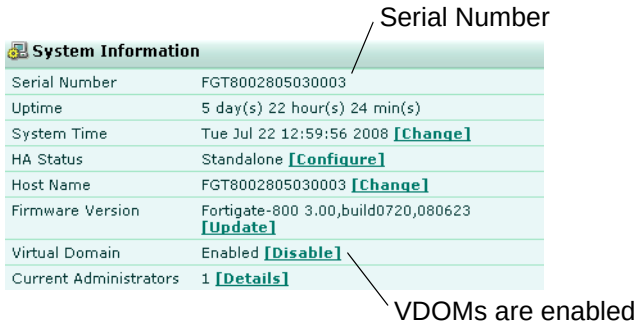
1 Log in with a super_admin account.

2 Go to *System* > *Status*.

3 Under *System Information* > *Virtual Domain*, select *Enable* and confirm your selection.

The FortiGate unit logs off your session. You can now log in again as admin. For more information, see the User authentication chapter of the *FortiGate Administration Guide*.

Figure 15: System Information



To enable VDOM configuration - CLI

```
config system global
  set vdom-admin enable
end
```

Viewing the VDOM list

The VDOM list shows all virtual domains, their status, and which VDOM is the management VDOM. It is accessible if you are logged in on an administrator account with the super_admin profile such as the “admin” administrator account.

In the VDOM list, you can create or delete VDOMs, change the management VDOM, and enable or disable VDOMs.

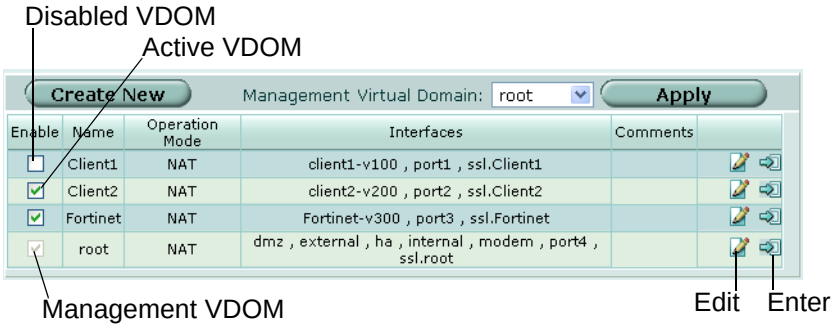
Note: The root domain may not be disabled, even if it is not the management VDOM.

To view the VDOM list

1 If << *Global* appears in the left menu, select it to enter global configuration.

2 Go to *System* > *VDOM*.

Figure 16: List of VDOMs



Create New	Select to add a new VDOM.
Management virtual domain	The management domain. To change, select another VDOM from the list. For more information, see “Changing the management VDOM” on page 69.
Apply	Select *Apply* to save any changes made to this screen.
Enable	Status of this VDOM. Status can be one of: • Disabled - blank - VDOM retains settings, but cannot be entered until it is activated • Active - green check - this VDOM can be used as normal, and can be deleted • Management VDOM - gray check - this VDOM is the management VDOM for this FortiGate unit, and cannot be deleted or disabled
Name	The name of the VDOM
Operation Mode	The operation mode of this VDOM, one of: • NAT - NAT/Route • Transparent
Interfaces	The interfaces associated with this VDOM. Each VDOM also includes an interface that starts with “ssl.” that is created by default.
Comments	Comments entered when the VDOM was created.
Edit	Select to change comments for this VDOM.
Enter	Select to enter this VDOM.

Creating, disabling, and deleting VDOMs

Only a super_admin administrator account such as the default “admin” account can create, disable, or delete VDOMs. By default, the FortiGate unit has one fixed VDOM named “root”, which you cannot delete, disable, or rename.

This section includes:

Creating a VDOM

Once you have enabled VDOMs, you can create additional VDOMs, and name them as you like with the following restrictions:

- only letters, numbers, “-”, and “_” are allowed
- no more than 11 characters are allowed
- no spaces are allowed
- VDOMs cannot have the same names as interfaces, zones, switch interfaces, or other VDOMs.

Note: When creating 250 or more VDOMs, you cannot enable advanced features such as proxies, web filtering, and antivirus due to limited resources. Also when creating large numbers of VDOMs, you may experience reduced performance.

To create a VDOM - web-based manager

1. Log in with a super_admin account.
2. Select *System* > *VDOM*.
3. Select *Create New*.
4. Enter a name for your new VDOM.
5. Enter a short and descriptive comment to identify this VDOM.
6. Select *OK*.
7. Select *OK* again to return to the VDOM list and view the new VDOM.

   Repeat Steps 3 through 7 to add additional VDOMs.

To create a VDOM - CLI

```
config vdom
  edit <new_vdom_name>
end
```

Disabling a VDOM

The status of a VDOM can be Active, Management, or Disabled.

Active status VDOMs can be configured, and are the main status for VDOMs. Management status can be assigned to only one VDOM. For more information, see “Changing the management VDOM” on page 69.

Disabled status VDOMs are considered “offline”. The configuration remains, but you cannot use the VDOM, and only the super_admin administrator can view it. You cannot delete a disabled VDOM without first enabling it—there is no *Delete* icon for disabled status. You can assign interfaces to a disabled VDOM.

Even disabled VDOMs must be deleted to disable all VDOMs on the FortiGate unit. For more information, see “Deleting a VDOM” on page 64.

The following procedures show how to disable a VDOM called “testvdom”.

To disable a VDOM - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Clear the check box in the *Enable* column for “testvdom”.

   To enable a VDOM, select the *Enable* check box.
4. Confirm your selection.

To disable a VDOM - CLI

```
config vdom
  edit testvdom
    config system settings
      set status disable
    end
end
```

Deleting a VDOM

Deleting a VDOM removes it from the FortiGate unit configuration.

Before you can delete a VDOM, all references to it must be removed. This includes any objects listed in “VDOM settings” on page 22. If there are any references to the VDOM remaining, you will see an error message and not be able to delete the VDOM.

The VDOM must also be enabled. A disabled VDOM cannot be deleted.

Tip: Before deleting a VDOM, a good practice is to reset any interface referencing that VDOM to its default configuration, with “root” selected as the Virtual Domain.

You cannot delete the root VDOM or the management VDOM. For more information see “Changing the management VDOM” on page 69.

The following procedures show how to delete the “testvdom” VDOM.

To delete a VDOM - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Select the *Delete* icon for “testvdom”.

   If there is no *Delete* icon, there are still references to the VDOM that must first be removed. The *Delete* icon is visible for this VDOM when all the references are removed.
4. Confirm the deletion.

To delete a VDOM - CLI

```
config vdom
  delete testvdom
end
```

Increasing the number of VDOMs

All FortiGate units, except the 30B, support 10 VDOMs by default.

High-end FortiGate models support the purchase of a VDOM license key from customer support to increase their maximum allowed VDOMs to 25, 50, 100, 250, or 500. Configuring 250 or more VDOMs will result in reduced system performance.

Table 8: VDOMs support by FortiGate model

FortiGate model	Support VDOMs	Default VDOM maximum	Maximum VDOM license
30B	no	0	0
Low and mid-range models	yes	10	10
High-end models	yes	10	500

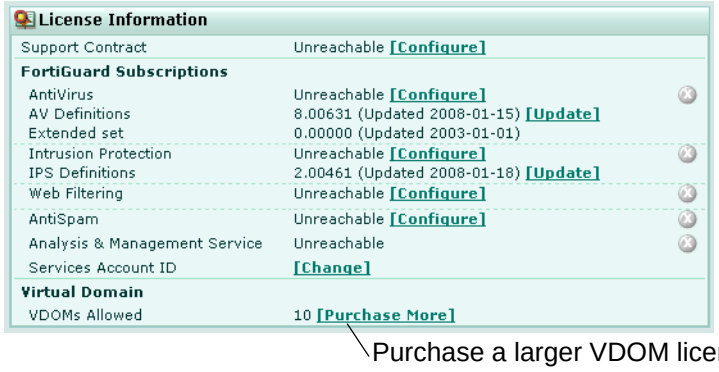
You can purchase a VDOM license key for FortiGate models numbered 3000 and higher from customer support. This will increase the maximum allowed VDOMs to 25, 50, 100, 250, or 500 on your FortiGate unit.

Note: Your FortiGate unit has limited resources that are divided among all configured VDOMs. These resources include system memory and CPU. You cannot run Unified Threat Management (UTM) features when running 250 or more VDOMs. UTM features include proxies, web filtering, and antivirus—your FortiGate unit can provide only basic firewall functionality.

To obtain a VDOM license key

1. Log in with a super_admin account.
2. Go to *System* > *Status*.
3. Record your FortiGate unit serial number as shown in "System Information" on page 61.
4. Under *License Information* > *Virtual Domains*, select *Purchase More*.

Figure 17: VDOM License Information



5. You will be taken to the Fortinet customer support website where you can log in and purchase a license key for 25, 50, 100, 250, or 500 VDOMs.
6. When you receive your license key, go to *System* > *Maintenance* > *License*.

Note: If you do not have a *System* > *Maintenance* > *License* tab, your FortiGate model does not support more than 10 VDOMs.

7 In the *Input License Key* field, enter the 32-character license key you received from Fortinet customer support.

8 Select *Apply*.

To verify the new VDOM license, in global configuration go to *System* > *Status*. Under *License Information*, *Virtual Domains* shows the maximum number of VDOMs allowed.

Note: VDOMs created on a registered FortiGate unit are recognized as real devices by any connected FortiAnalyzer unit. The FortiAnalyzer unit includes VDOMs in its total number of registered devices. For example, if three FortiGate units are registered on the FortiAnalyzer unit and they contain a total of four VDOMs, the total number of registered FortiGate units on the FortiAnalyzer unit is seven. For more information, see the *FortiAnalyzer Administration Guide*.

Creating VDOM administrators

Only super_admin administrator accounts can create other administrator accounts and assign them to a VDOM.

The only difference in admin accounts when VDOMs are enabled is selecting which VDOM the admin account belongs to. Otherwise, by default the administration accounts are the same as when VDOMs are disabled and closely resemble the super_admin account in their privileges.

Note: The newly-created administrator can access the FortiGate unit only through network interfaces that belong to their assigned VDOM or through the console interface. The network interface must be configured to allow management access, such as HTTPS and SSH. Without these in place, the new administrator will not be able to access the FortiGate unit and will have to contact the super_admin administrator for access.

To create administrators for VDOMs - web-based manager

1 Log in with a super_admin account.

2 Go to *System* > *Admin* > *Administrators*.

3 Select *Create New*.

4 Configure the settings of the administrator account. For more information, see the System Admin chapter of the *FortiGate Administration Guide*.

5 When setting the profile for this new account, select

- super_admin to manage accounts in any VDOM on your FortiGate unit or
- another profile for an administrator account that will only manage users on the selected VDOM.

6 From the Virtual Domain list, select the VDOM this administrator will control.

or

If this is a super_admin account, this option will be automatically set to global.

7 Select *OK*.

To create administrators for VDOMs - CLI

```
config global
  config system admin
  edit <new_admin_name>
    set vdom <vdom_for_this_account>
    set password <pwd>
    set accprofile <an_admin_profile>
    ...
end
```

For more information on configuring VDOM interfaces, see "Adding interfaces and VLAN subinterfaces to a VDOM" on page 69. For general information about interfaces, see the *FortiGate Administration Guide*.

Accessing and configuring VDOMs

Only super_admin administrator accounts can access all global settings on the FortiGate and all of the VDOMs as well. Other administrator accounts can access and configure only their own VDOM and must connect to an interface in that VDOM.

Management services communicate using addresses and routing in the management VDOM, which is the root VDOM by default. For more information, see "Changing the management VDOM" on page 69.

Note: Management traffic requires an interface. If there is no interface assigned to the VDOM containing the management traffic, services including updates will not function. For more information, see "Changing the management VDOM" on page 69.

To access a VDOM with a super_admin account - web-based manager

1. Log in with a super_admin account.
2. Select *System* > *VDOM*.

   From here you can select a specific VDOM to configure. For more information, see "List of VDOMs" on page 62.
3. Select *Enter* for the active VDOM or management VDOM you want to change.

   The system network page for that VDOM opens.

   The bottom of the left menu displays the currently selected VDOM name, unless only the root domain exists.
4. When you have finished configuring the VDOM, you can
   - select << *Global* to return to global configuration for the FortiGate unit
   - log out.

To access a VDOM with a super_admin account - CLI

With the super_admin, logging into the CLI involves also logging into the specific VDOM.If you need a reminder, use “edit?” to see a list of existing VDOMs before you editing a VDOM.

```
Login: admin
Password: <admin_password>
config vdom
  edit ?
  edit <chosen_vdom>
    ..
    <enter vdom related commands>
    ..
  end
exit
```

To access a VDOM with a non super_admin account - web-based manager

1. Connect to the FortiGate unit using an interface that belongs to the VDOM to be configured.
2. Log in using an administrator account that has access to the VDOM.

   The main web-based manager page opens. From here you can access VDOM-specific settings.

To access a VDOM with a non-super_admin account - CLI

When a non-super_admin logs into the FortiGate, there is not logging into the VDOM as this account only has access to one VDOM.

```
Login: regular_admin
Password: <password>
..
<enter vdom related commands>
..
exit
```

Configuring VDOMs

Once you have enabled VDOMs and created one or more VDOMs, you need to configure them. Configuring VDOMs on your FortiGate unit includes tasks such as the ones listed here; while you may not require all for your network topology, it is recommended that you perform them in the order given:

- Changing the management VDOM
- Adding interfaces and VLAN subinterfaces to a VDOM
- Configuring VDOM resources
- Configuring firewall policies for a VDOM

Changing the management VDOM

The management VDOM is the VDOM where all the management traffic for the FortiGate unit originates. Management traffic includes:

- DNS lookups
- logs sent to FortiAnalyzer, syslog or webtrends
- FortiGuard service
- alert email
- network time protocol (NTP) traffic
- SNMP traps
- quarantines of suspicious files and email.

By default the management VDOM is the root domain. When other VDOMs are configured on your FortiGate unit, management traffic can be moved to one of these other VDOMs.

Note: The management domain requires at least one interface be connected to the Internet to enable connections to remote services such as FortiGuard services and NTP.

Note: You cannot change the management VDOM if any administrators are using RADIUS authentication.

The following procedure will change the management VDOM to a VDOM named “mgmt_vdom”. It is assumed that “mgmt_vdom” has already been created.

To change the management VDOM - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *System* > *VDOM.*
3. In the *Management Virtual Domain* menu, select *mgmt_vdom*.
4. Select *Apply.*

To change the management VDOM - CLI

```
config global
  config system global
    set management-vdom mgmt_vdom
end
```

Management traffic will now originate from mgmt_vdom.

Adding interfaces and VLAN subinterfaces to a VDOM

A VDOM must contain at least two interfaces to be useful. These can be physical interfaces or VLAN interfaces. By default, all physical interfaces are in the root VDOM. When you create a new VLAN, it is in the root VDOM by default.

When there are VDOMs on the FortiGate unit in both NAT and Transparent operation modes, some interface fields will be displayed as “-” on *System* > *Network* > *Interface*. Only someone with a super_admin account can view all the VDOMs.

Note: When moving an interface to a different VDOM, firewall IP pools and virtual IPs for this interface are deleted. You should manually delete any routes that refer to this interface. Once the interface has been moved to the new VDOM, you can add these services to the interface again.

This section includes the following topics:

Adding a VLAN to a VDOM

The following example shows one way that multiple companies can maintain their security when they are using one FortiGate unit with VLANs that share interfaces on the unit.

This procedure will add a VLAN interface called “client1-v100” with a VLAN ID of 100 to a VDOM called “client1” using the physical interface called “external”. The physical interface does not need to belong to the VDOM that the VLAN belongs to. It is assumed that the VDOM client1 has already been created.

To add a VLAN subinterface to a VDOM - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.

2 Go to *System* > *Network* > *Interface*.

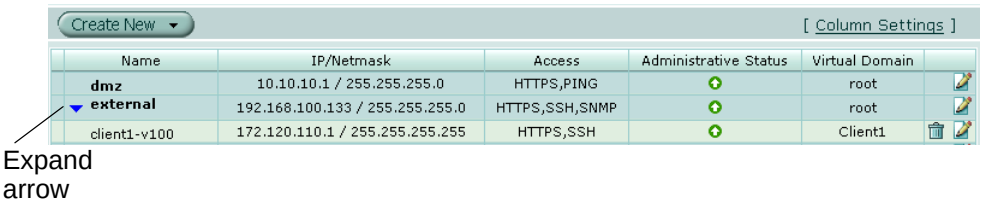
3 Select *Create New*.

4 Enter the following information and select *OK*:

Name	client1-v100
Interface	external
VLAN ID	100
Virtual Domain	Client1
Addressing mode	Manual
IP/Netmask	172.20.120.110/255.255.255.0
Administrative Access	HTTPS, SSH

You will see an expand arrow added to the internal interface. When the arrow is expanded, the interface shows the client1-v100 VLAN subinterface.

Figure 18: New client1-v100 VLAN



To add a VLAN subinterface to a VDOM - CLI

```
config global
config system interface
  edit client1-v100
    set type vlan
    set vlanid 100
    set vdom Client1
    set interface external
    set ip 172.20.120.110 255.255.255.0
    set allowaccess https ssh
  next
  end
end
```

Moving an interface to a VDOM

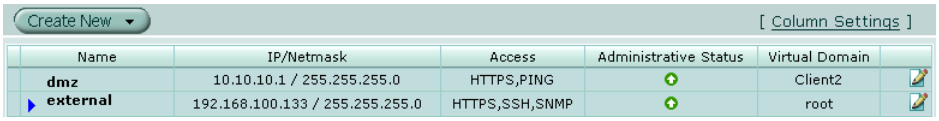
Interfaces belong to the root VDOM by default. Moving an interface is the same from any VDOM.

The following procedure will move the dmz interface to the Client2 VDOM. This is a common action when configuring a VDOM. It is assumed that the Client2 VDOM has already been created. It is also assumed that the FortiGate-800 model is being used. If you are using a different model, your physical interfaces may not be named “internal”, “external” or “dmz”.

To move an existing interface to a different VDOM - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *Network* > *Interface*.
3. Select *Edit* for the dmz interface.
4. Enter `Client2` as the new VDOM name.
5. Select *OK*.

Figure 19: dmz in Client2 VDOM



To move an existing interface to a different VDOM - CLI

```
config global
  config system interface
  edit dmz
    set vdom Client2
  next
end
```

Adding a zone to a VDOM

Grouping interfaces and VLAN subinterfaces into zones simplifies policy creation. You can configure policies for connections to and from a zone, but not between interfaces in a zone.

Zones are VDOM-specific. A zone cannot be moved to a different VDOM. Any interfaces in a zone cannot be used in another zone. To move a zone to a new VDOM requires deleting the current zone and re-creating a zone in the new VDOM. For more information, see the Network chapter of the *FortiGate Administration Guide*.

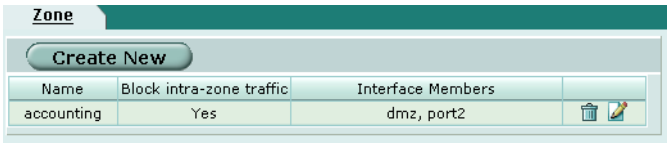
The following procedure will create a zone called `accounting` in the `client2` VDOM. It will not allow intra-zone traffic, and both `dmz` and `port2` interfaces belong to this zone. This is a method of grouping and isolating traffic over particular interfaces—it is useful for added security and control within a larger network.

To add a zone to a VDOM - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Select the client2 VDOM, and select *Enter*.
4. Go to *System* > *Network* > *Zone*.
5. Select *Create New*.
6. Enter the following information and select *OK*:

Zone Name	accounting
Block intra-zone traffic	Select
Interface Members	dmz, port2

Figure 20: New zone in Client2



To add a zone to a VDOM - CLI

```
config vdom
edit client2
  config system zone
    edit accounting
      set interface dmz port2
      set intrazone deny
    next
  end
end
```

Configuring VDOM resources

FortiGate units have upper limits for resources such as firewall policies, protection profiles, and VPN tunnels. These limits vary by model. In general, the more VDOMs the FortiGate unit supports, the greater the impact on resource limits. In previous releases of FortiOS, maximum values for resources belonging to VDOMs applied equally to each VDOM. Maximums for system-wide (global) resources applied globally and the resources were equally accessible to each VDOM.

If you are a super administrator, you can control resource allocation to each VDOM. This limits the impact of each VDOM on other VDOMs due to resource competition. Also, you can set global resource limits to control the impact of various features on system performance.

Note: The resource limits vary for different FortiGate models. The resource limits increase when two or more FortiGates units are in HA mode due to the increased resources that are available to the HA cluster.

VDOM resource limits

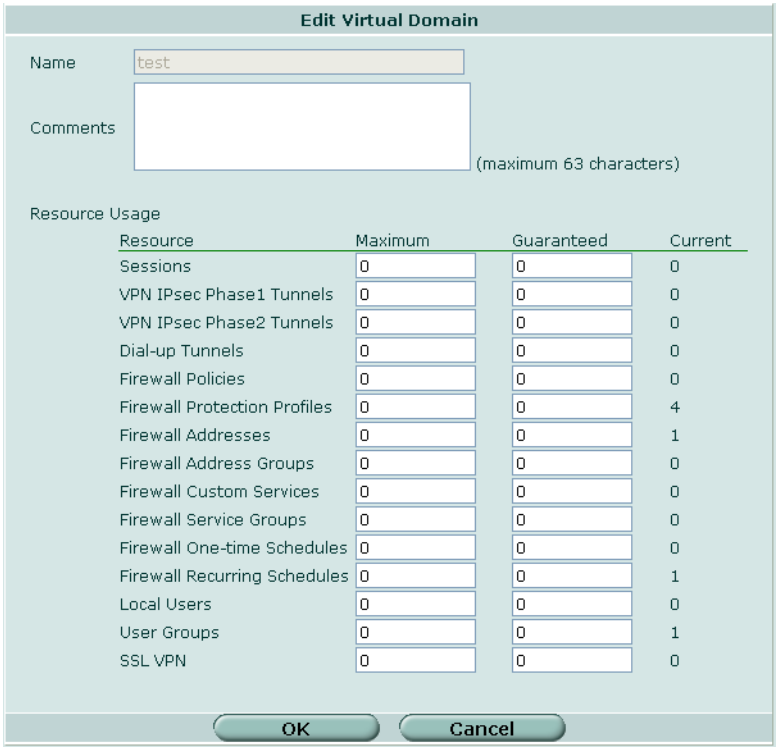
You can configure VDOM resource limits when you create a new VDOM or edit an existing one. These resource limits are restricted by the FortiGate global limits in that the total of each resource across all VDOMs cannot exceed the global limit.

You can optionally set a guaranteed minimum level of resources that will be available to the VDOM. This will ensure that other VDOMs do not use all of an available resource.

To configure VDOM resource limits - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Select *Create New*, enter a name and then select *OK*, or select the *Edit* icon of an existing VDOM.
4. Modify the values described in the table below as required.
5. Select *OK*.

Figure 21: Configuring VDOM resource limits



Resource	Description of the resource.
Maximum	Enter the maximum amount of the resource allowed for this VDOM. This amount might not be available due to usage of this resource type by other VDOMs.
Guaranteed	Enter the minimum amount of the resource available to this VDOM regardless of usage by other VDOMs.
Current	The amount of the resource that this VDOM currently uses.

If you enter a value that is not valid, the web-based manager displays the range of valid values.

To configure VDOM resource limits - CLI

When configuring VDOM resource limits using the CLI, you must use the `vdom-property` command to set the maximum and guaranteed limits of system resources for the specified virtual domain (VDOM). The optional guaranteed limit ensures a minimum number of a resource is always available for this VDOM. For example, a minimum of 200 sessions could be necessary for the root VDOM.

Configured `vdom-property` maximums, when totaled for all VDOMs, cannot exceed the maximum values set in `resource-limits` for that variable, which are for the entire FortiGate unit. For example, if `resource-limits` sets a maximum of 10 000 sessions, then the maximum sessions for VDOMs when totalled must be 10 000 sessions or less.

Restricting system resources on a per-VDOM level allows you to increase the number of VDOMs while minimizing the impact on FortiGate performance. You can also establish tiered service levels for different VDOMs.

This command is available only when VDOMs are enabled.

Note: The resource limits vary for different FortiGate models. The resources are also increased when FortiGate units are in HA mode, due to the increased shared resources that are available.

Use the following syntax and table to configure VDOM resource limits.

```
config global
config system vdom-property
  edit <vdom_name>
    set custom-service <srvc_max> [srvc_min]
    set dialup-tunnel <tunn_max> [tunn_min]
    set firewall-policy <pol_max> [pol_min]
    set firewall-profile <prof_max> [prof_min]
    set firewall-address <addr_max> [addr_min]
    set firewall-addrgrp <group_max> [group_mmin]
    set ipsec-phase1 <tunn_max> [tunn_min]
    set ipsec-phase2 <tunn_max> [tunn_min]
    set onetime-schedule <sched_max> [sched_min]
    set recurring-schedule <sched_max> [sched_min]
    set service-group <group_max> [group_mmin]
    set session <session_max> [session_min]
    set user <user_max> [user_min]
    set user-group <group_max> [group_mmin]
  end
end
```

Variables	Description	Default
`edit <vdom_name>`	Select the VDOM to set the limits for.	
`custom-service <srvc_max> [srvc_min]`	Enter the maximum number and guaranteed number of firewall custom services.	0
`dialup-tunnel <tunn_max> [tunn_min]`	Enter the maximum number and guaranteed number of dialup-tunnels.	0
`firewall-policy <pol_max> [pol_min]`	Enter the maximum number and guaranteed number of firewall policies.	0
`firewall-profile <prof_max> [prof_min]`	Enter the maximum number and guaranteed number of firewall profiles.	0
`firewall-address <addr_max> [addr_min]`	Enter the maximum number and guaranteed number of firewall addresses.	0
`firewall-addrgrp <group_max> [group_mmin]`	Enter the maximum number and guaranteed number of firewall address groups.	0
`ipsec-phase1 <tunn_max> [tunn_min]`	Enter the maximum number and guaranteed number of IPSec Phase 1 tunnels.	0
`ipsec-phase2 <tunn_max> [tunn_min]`	Enter the maximum number and guaranteed number of IPSec Phase 2 tunnels.	0
`onetime-schedule <sched_max> [sched_min]`	Enter the maximum number and guaranteed number of onetime schedules.	0
`recurring-schedule <sched_max> [sched_min]`	Enter the maximum number and guaranteed number of recurring schedules.	0

Variables	Description	Default
`service-group <group_max> [group_mmin]`	Enter the maximum number and guaranteed number of firewall service groups.	0
`session <session_max> [session_min]`	Enter the maximum number and guaranteed number of sessions.	0
`user <user_max> [user_min]`	Enter the maximum number and guaranteed number of users.	0
`user-group <group_max> [group_mmin]`	Enter the maximum number and guaranteed number of user groups.	0

The following example shows how to set a maximum of 1000 sessions on the root VDOM with a guaranteed minimum level of 100 sessions. (VDOMs are enabled.)

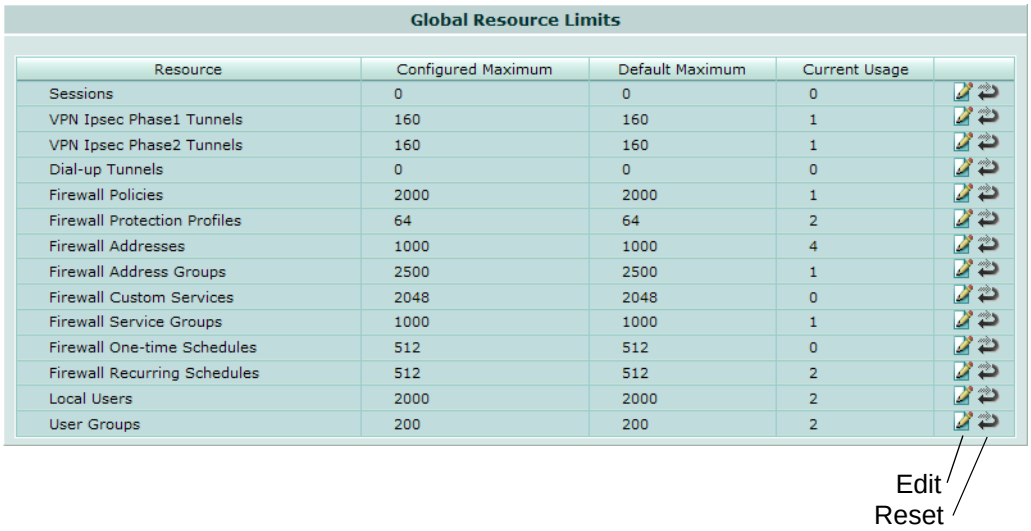
```
config global
config system vdom-property
  edit root
    set sesssion 1000 100
  end
end
```

Global resource limits

To ensure system performance, you can set global resource limits that are less than the maximums set by your unit's hardware. Your configured maximum value for any resource must be greater than the amount of the resource already in use and greater than the sum of all VDOM guaranteed resource values.

To view or set global resource limits, go to *System* > *VDOM* > *Global Resources.* Select the *Edit* icon to change any settings.

Figure 22: Configuring global resource limits



Resource	Description of the resource.
Configured Maximum	The maximum amount of the resource allowed. This amount matches the default maximum until you change it.
Default Maximum	The default maximum value for this resource. This value depends on the unit hardware limitations.
Current Usage	The amount of the resource currently in use.
Edit icon	Change the configured maximum for this resource. The *Edit Global Resource Limits* dialog box lists the valid range of values for the configured maximum. For some resources, you can set the maximum to zero to set no limit.
Reset icon	Reset the configured maximum to the default maximum value.

Configuring VDOM routing

Routing is VDOM-specific. Each VDOM should have a default static route configured as a minimum. Within a VDOM, routing is the same as routing without VDOMs enabled.

When configuring dynamic routing on a VDOM, other VDOMs on the FortiGate unit can be neighbors. The following topics give a brief introduction to the routing protocols, and show specific examples of how to configure dynamic routing for VDOMs. Figures are included to show the FortiGate unit configuration after the successful completion of the routing example.

For more information, see the routing chapters in the *FortiGate Administration Guide*.

This section includes the following topics:

- Adding a default static route for a VDOM
- Configuring RIP for a VDOM
- Configuring OSPF for a VDOM
- Configuring BGP for a VDOM

Adding a default static route for a VDOM

The routing you define applies only to network traffic entering non-ssl interfaces belonging to this VDOM. Set the administrative distance high enough, typically 20, so that automatically configured routes will be preferred to the default.

In the following procedure, it is assumed that a VDOM called “Client2” exists. The procedure will create a default static route for this VDOM. The route has a destination IP of 0.0.0.0, on the dmz interface. It has a gateway of 10.10.10.1, and an administrative distance of 20.

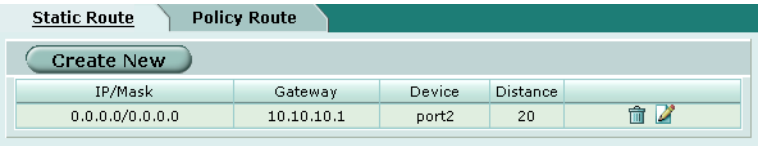
The values used in this procedure are very standard, and this procedure should be part of configuring all VDOMs.

To add a default static route for a VDOM - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.
2 Go to *System* > *VDOM*.
3 Select the *Client2* VDOM and select *Enter*.
4 Go to *Router* > *Static*.
5 Select *Create New*.
6 Enter the following information and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port2
Gateway	10.10.10.1
Distance	20

Figure 23: Default static route on Client2 VDOM



To add a default static route for a VDOM - CLI

```
config vdom
edit Client2
  config router static
  edit 4
    set device port2
    set dst 0.0.0.0 0.0.0.0
    set gateway 10.10.10.1
    set distance 20
  end
end
```

Configuring RIP for a VDOM

The RIP dynamic routing protocol uses hop count to determine the best route, with a hop count of 1 being directly attached to the interface and a hop count of 16 being unreachable. For example if two VDOMs on the same FortiGate unit are RIP neighbors, they have a hop count of 1.

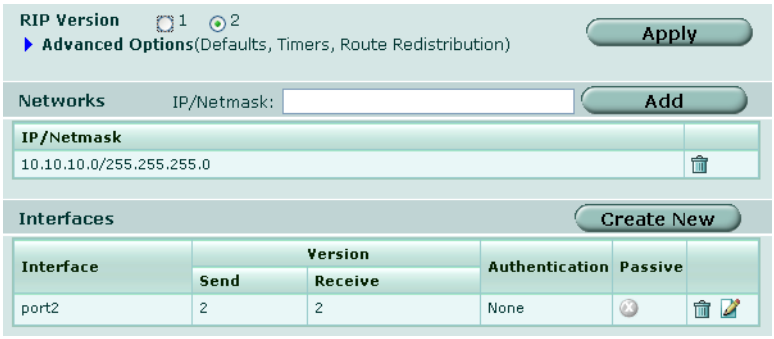
In the following procedure, it is assumed that a VDOM called “Client2” exists. The procedure configures RIP version 2 for the Client2 VDOM and there is a connected network running RIP at 10.10.10.0/255.255.255.0. In fact the connected network includes one of the other VDOMs on this FortiGate unit as well as a local router. The dmz interface is configured to send and receive RIP version 2 with no authentication. The advanced options will remain as default values—this VDOM will not redistribute any routes learned through other protocols.

To configure RIP for a VDOM - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.
2 Go to *System* > *VDOM*.
3 Select the *Client2* VDOM and select *Enter*.
4 Select *Router* > *Dynamic* > *RIP*.
5 Select *RIP Version 2*, and select *Apply*.
6 Enter an *IP/Netmask* of `10.10.10.0/255.255.255.0` for *Networks*.
7 Select *Add*.
8 Select *Create New* for *Interfaces*.
9 Enter the following information and select *OK*:

Interface	dmz
Send Version	2
Receive Version	2
Authentication	None
Passive Interface	(not selected)

Figure 24: RIP on Client2 VDOM



To configure RIP for a VDOM - CLI

In the CLI there are more options available to configure RIP. The extra command used here is the poisoned split-horizon. Enabling this command prevents network looping problems. For more information, see the dynamic routing chapter of the *FortiGate Administration Guide*.

```
config vdom
edit Client2
  config router rip
    set version 2
    config interface
    edit dmz
      set auth-mode none
      set receive-version 2
      set send-version 2
      set split-horizon poisoned
    end
  end
end
```

Configuring OSPF for a VDOM

OSPF communicates the status of its network links to adjacent neighbor routers instead of the complete routing table. When compared to RIP, OSPF is more suitable for large networks, it is not limited by hop count, and is more complex to configure. For smaller OSPF configurations its easiest to just use the backbone area, instead of multiple areas.

In the following procedures, it is assumed that a VDOM called “Client2” exists. The following three procedures configure the Client2 VDOM as a regular internal OSPF router. The procedure configures a router ID of 192.168.10.133—the highest IP address on the VDOM. The backbone area is the only configured area, with an IP of 0.0.0.0 and a regular type area with no authentication. The network connected to the backbone area is configured as 192.168.10.0/255.255.255.0. The OSPF enabled interface is called “OSPF_port2” and uses the port2 interface with an IP address of 192.168.10.133, no authentication, and the default OSPF timer values.

To configure the OSPF router ID - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Select the *Client2* VDOM and select *Enter*.
4. Select *Router* > *Dynamic* > *OSPF*.
5. Enter the *Router ID* as `192.168.10.133`, and select *Apply*.

To configure the OSPF router ID - CLI

```
config vdom
edit Client2
  config router ospf
    set routerid 192.168.10.133
  end
end
```

To configure the backbone area - web-based manager

1. Select *Create New* for *Areas*.
2. Enter the following information and select *OK*:

Area	0.0.0.0 (backbone or Area 0)
Type	Regular
Authentication	None

To configure the backbone area - CLI

```
config vdom
edit Client2
  config router ospf
    config area
    edit 0.0.0.0
      set authentication none
      set type regular
    end
  end
end
```

To configure the network and interface - web-based manager

1 Select *Create New* for *Networks*.

2 Enter the following information and select *OK*:

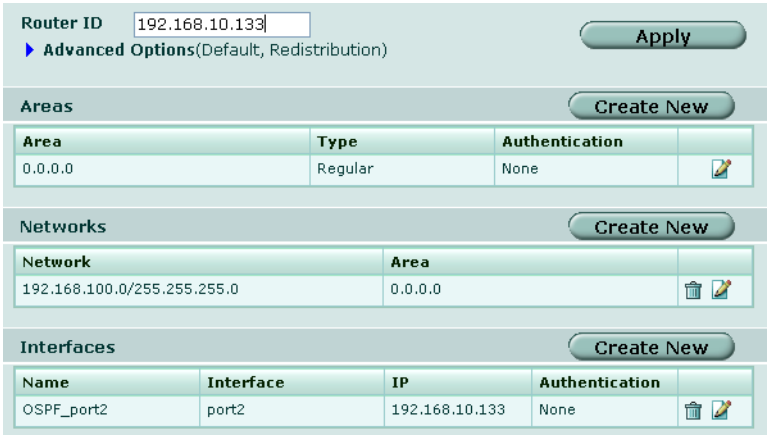
IP/Netmask	192.168.100.0/255.255.255.0
Area	0.0.0.0

3 Select *Create New* for *Interfaces*.

4 Enter the following information and select *OK*:.

Name	OSPF_port2
Interface	port2
IP	192.168.10.133
Authentication	None
Hello Interval	10 seconds (default)
Dead Interval	40 seconds (default)

Figure 25: OSPF on Client2 VDOM



To configure the network and interface - CLI

```
config vdom
edit Client2
  config routing ospf
    config network
    edit 1
      set area 0.0.0.0
      set prefix 192.168.100.0 255.255.255.0
    next
    end
    config ospf-interface
    edit OSPF-port2
      set interface port2
      set ip 192.168.10.133
      set authentication none
      set hello-interval 10
      set dead-interval 40
      set status enable
    end
  end
end
```

Configuring BGP for a VDOM

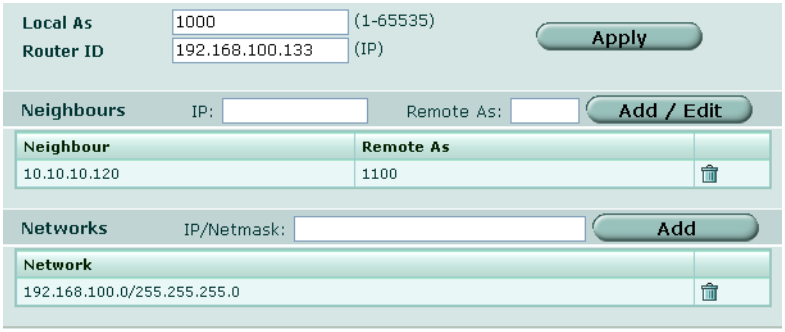
BGP is an Internet gateway protocol (IGP) used to connect autonomous systems (ASes) and is used by Internet service providers (ISPs). BGP stores the full path, or path vector, to a destination and its attributes which aid in proper routing.

In the following procedure, it is assumed that a VDOM called “Client2” exists.The Client2 VDOM is a regular BGP neighbor router. The procedure configures a BGP local AS of 1000, and router ID of 192.168.100.133 for the Client2 VDOM. A neighbor, a peer router, is defined as 10.10.10.120 on AS 1100, a remote AS. A BGP configured network is defined as 192.168.100.0/255.255.255.0.

To configure BGP for a VDOM - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Select the *Client2* VDOM and select *Enter*.
4. Select *Router* > *Dynamic* > *BGP*.
5. Enter the *Local As* as `1000` and *Router ID* as `192.168.10.133`, and select *Apply*.
6. Under *Neighbors*, enter an IP of `10.10.10.120` and a *Remote As* of `1100` and select *Add/Edit*.
7. Under *Networks*, enter an IP of `192.168.100.0/255.255.255.0`, and select *Add*.

Figure 26: BGP on Client2 VDOM



To configure BGP for a VDOM - web-based manager

```
config vdom
edit Client2
  config router bgp
      set as 1000
      set router-id 192.168.10.133
      config neighbor
      edit 10.10.10.120
      set remote-as 1100
    next
    end
    config network
    edit 1
      set prefix 192.168.100.0 255.255.255.0
    end
  end
end
```

Configuring firewall policies for a VDOM

Firewall policies are VDOM-specific. This means that all firewall settings for a VDOM, such as firewall addresses and policies, are configured within the VDOM. For more information about firewall settings, see the Firewall chapter of the *FortiGate Administration Guide*.

Note: You can customize the Firewall Policy display by including some or all columns, and customize the column order onscreen. Due to this feature, firewall policy screenshots may not appear the same as on your screen.

The following procedures will set up one firewall address, and configure a minimal outgoing firewall policy on the client2 VDOM.

The topics in this section include:

- Adding a firewall address to a VDOM
- Configuring a firewall policy for a VDOM

Adding a firewall address to a VDOM

Firewall addresses are an easy-to-read method of grouping addresses together for use in firewall policies.

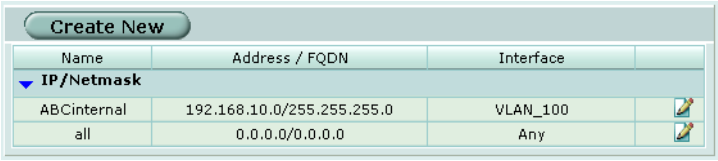
In the following procedure, it is assumed that a VDOM called “Client2” exists. The procedure will configure a firewall address. ABC company’s internal network is the 192.168.100.0/255.255.255.0 subnet that will be called “ABCinternal”.

To add a firewall address to a VDOM - web-based manager

1. Log in as the super_admin administrator.
2. Go to *System* > *VDOM*.
3. Select the *Client2* VDOM and select *Enter*.
4. Go to *Firewall* > *Address*.
5. Select *Create New*.
6. Enter the following information and select *OK*:

Address Name	ABCinternal
Subnet / IP Range	192.168.10.0/255.255.255.0
Interface	VLAN_100

Figure 27: ABCdomain and all address groups defined



To add a firewall address to a VDOM - CLI

```
config vdom
edit Client2
  conifg firewall address
  edit ABCinternal
    set associated-interface VLAN_100
    set subnet 192.168.10.0 255.255.255.0
  next
  end
end
```

Configuring a firewall policy for a VDOM

Your firewall policies can involve only the interfaces, zones, and firewall addresses that are part of the current VDOM, and they are only visible when you are viewing the current VDOM. The firewall policies of this VDOM filter the network traffic on the interfaces and VLAN subinterfaces in this VDOM.

A firewall service group can be configured to group multiple services into one service group. When a descriptive name is used, service groups make it easier for an administrator to quickly determine what services are allowed by a firewall policy.

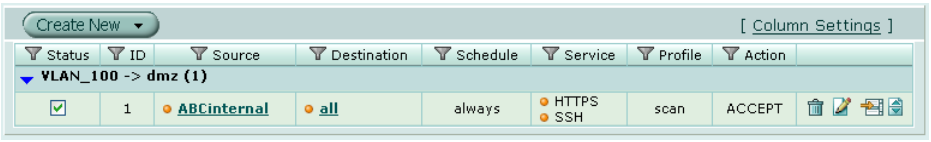
In the following procedure, it is assumed that a VDOM called “Client2” exists.The procedure will configure an outgoing firewall policy. The firewall policy will allow all HTTPS and SSH traffic for the “SalesLocal” address group on VLAN_200 going to all addresses on dmz. This traffic will be scanned and logged.

To configure a firewall policy for a VDOM - web-based manager

1. Go to *System* > *VDOM*.
2. Select the *Client2* VDOM and select *Enter*.
3. Go to *Firewall* > *Policy*.
4. Select *Create New*.
5. Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200
Source Address	SalesLocal
Destination Interface/Zone	dmz
Destination Address	any
Schedule	always
Service	Multiple - HTTPS, SSH
Action	ACCEPT
Protection Profile	scan (Select check box and enable scan)
Log Allowed Traffic	enable

Figure 28: VLAN_100-to-dmz policy allowing HTTPS and SSH



To configure a firewall policy for a VDOM - CLI

```
config vdom
edit Client2
  config firewall policy
  edit 12
    set srcintf VLAN_200
    set srcaddr SlaesLocal
    set dstintf dmz
    set dstaddr any
    set schedule always
    set service HTTPS SSH
    set action accept
    set status enable
    set profile-status enable
    set profile scan
    set logtraffic enable
  next
  end
end
```

Example VDOM configuration

Company ABC and company DEF each have their own internal networks and their own ISPs. They share a FortiGate-800 unit that is configured with two separate VDOMs, with each running in NAT/Route mode enabling separate configuration of network protection profiles. Each ISP is connected to a different interface on the FortiGate unit.

This network example was chosen to illustrate one of the most typical VDOM configurations.

This example has the following sections:

Network topology and assumptions

Both companies have their own ISPs and their own internal interface, external interface, and VDOM on the FortiGate unit.

For easier configuration, all IP addresses on the FortiGate unit end in ".2" such as 30.1.1.2 on the ABC external interface.

The ABC Inc. internal network is on the 172.100.1.0/255.255.255.0 subnet. The DEF Inc. internal network is on the 192.168.1.0/255.255.255.0 subnet.

There are no switches or routers required for this configuration.

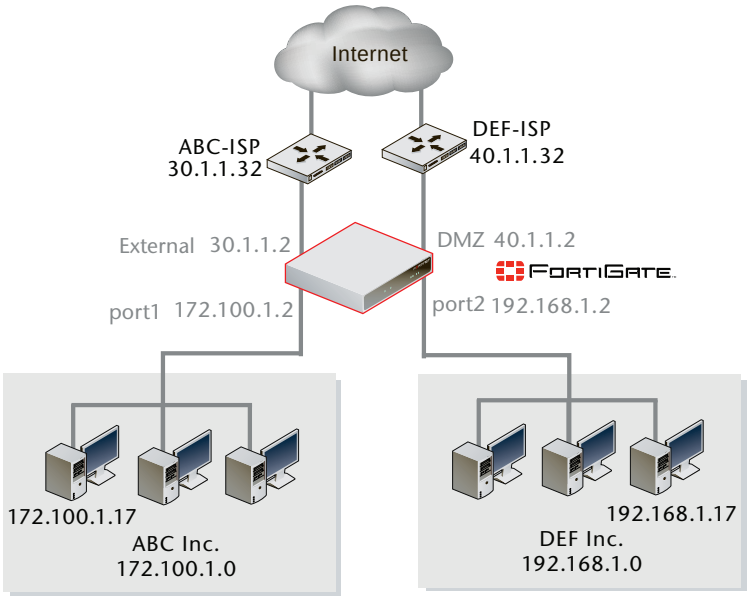
There are no VLANs in this network topology.

The FortiGate-800 is used; some labels may vary if your model is different.

The administrator is a super_admin account. If you are a using a non-super_admin account, refer to "Global and VDOM settings" on page 21 to see which parts a non-super_admin account can also configure.

When configuring firewall policies in the CLI always choose a policy number that is higher than any existing policy numbers, select `services` before `profile-status`, and `profile-status` before `profile`. If these commands are not entered in that order, they will not be available to enter.

Figure 29: Example VDOM configuration



General configuration steps

For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1 Creating the VDOMs
2 Configuring the FortiGate interfaces
3 Configuring the ABCdomain VDOM, and Configuring the DEFdomain VDOM:
4 Testing the configuration

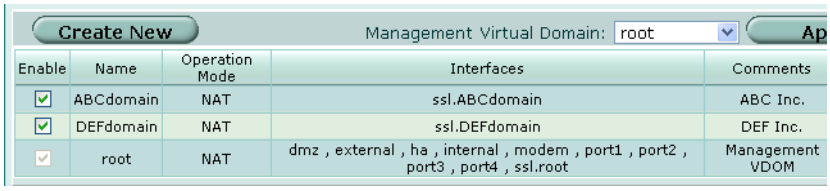
Creating the VDOMs

In this example, two new VDOMs are created: “ABCdomain” for company ABC, and “DEFdomain” for company DEF. These VDOMs will keep the traffic for these two companies separate while enabling each company to access its own ISP.

To create two VDOMs - web-based manager

1 Log in with a super_admin account.
2 If <<*Global* appears in the left menu, select it to enter global configuration.
3 Go to *System* > *VDOM*, and select *Create New*.
4 Enter `ABCdomain` and select *OK*.
5 Select *OK* again to return to the VDOM list.
6 Select *Create New*.
7 Enter `DEFdomain` and select *OK*.

Figure 30: ABCdomain and DEFdomain VDOMs



To create two VDOMs - CLI

```
config vdom
  edit ABCdomain
  next
  edit DEFdomain
  end
```

Configuring the FortiGate interfaces

This section configures the interfaces that connect to the companies' internal networks, and to the companies' ISPs.

All interfaces on the FortiGate unit will be configured with an IP address ending in ".2" such as 30.1.1.2. This will simplify network administration both for the companies, and for the FortiGate unit global administrator.

This section includes the following topics:

- Configuring the ABCdomain interfaces
- Configuring the DEFdomain interfaces

Note: If you cannot change the VDOM of an network interface it is because something is referring to that interface that needs to be deleted. Once all the references are deleted the interface will be available to switch to a different VDOM. For example a common reference to the external interface is the default static route entry.

Configuring the ABCdomain interfaces

The ABCdomain VDOM includes two FortiGate unit interfaces: port1 and external.

The port1 interface connects the ABC Inc. internal network to the FortiGate unit, and shares the internal network subnet of 192.168.1.0/255.255.255.0.

The external interface connects the FortiGate unit to ABC-ISP and the Internet. It shares the ABC-ISP subnet of 30.1.1.0/255.255.255.0.

To configure the ABCdomain interfaces - web-based manager

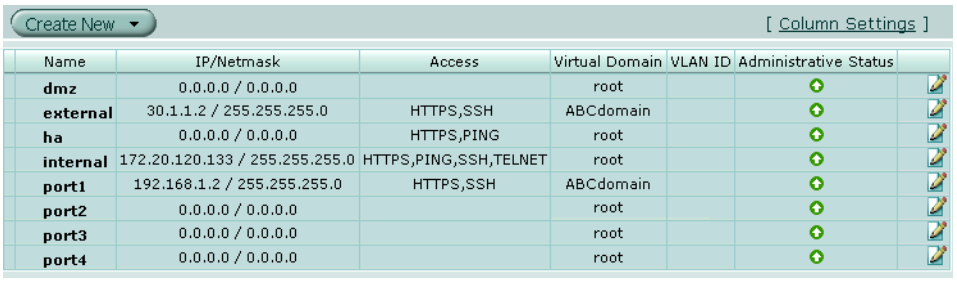
1 If <<*Global* appears in the left menu, select it to enter global configuration.
2 Go to *System* > *Network* > *Interface*.
3 Select *Edit* on the external interface.
4 Enter the following information and select *OK*:

Virtual Domain	ABCdomain
Addressing mode	Manual
IP/Netmask	30.1.1.2/255.255.255.0

5 Select *Edit* on the port1 interface.
6 Enter the following information and select *OK*:

Virtual Domain	ABCdomain
Addressing mode	Manual
IP/Netmask	192.168.1.2/255.255.255.0

Figure 31: Configured ABCdomain interfaces



To configure the ABCdomain interfaces - CLI

```
config global
  config system interface
    edit external
      set vdom ABCdomain
      set mode static
      set ip 30.1.1.2 255.255.255.0
    next
    edit port1
      set vdom ABCdomain
      set mode static
      set ip 192.168.1.2 255.255.255.0
    end
    end
  end
```

Configuring the DEFdomain interfaces

The DEFdomain VDOM includes two FortiGate unit interfaces: port2 and dmz.

The port2 interface connects the DEF Inc. internal network to the FortiGate unit, and shares the internal network subnet of 172.100.1.0/255.255.255.0.

The dmz interface connects the FortiGate unit to DEF-ISP and the Internet. It shares the DEF-ISP subnet of 40.1.1.0/255.255.255.0.

To configure the DEFdomain interfaces - web-based manager

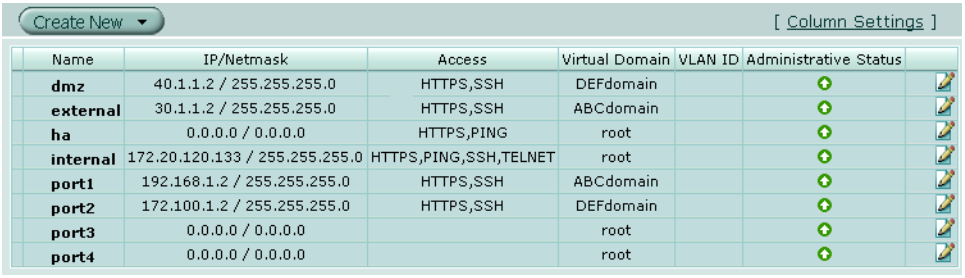
1 If <<*Global* appears in the left menu, select it to enter global configuration.
2 Go to *System* > *Network* > *Interface*.
3 Select *Edit* on the dmz interface.
4 Enter the following information and select *OK*:

Virtual domain	DEFdomain
Addressing mode	Manual
IP/Netmask	40.1.1.2/255.255.255.0

5 Select *Edit* on the port2 interface.
6 Enter the following information and select *OK*:

Virtual domain	DEFdomain
Addressing mode	Manual
IP/Netmask	172.100.1.2/255.255.255.0

Figure 32: Configured DEFdomain interfaces



To configure the DEFdomain interfaces - CLI

```
config global
  config system interface
    edit dmz
      set vdom DEFdomain
      set mode static
      set ip 40.1.1.2 255.255.255.0
    next
    edit port2
      set vdom DEFdomain
      set mode static
      set ip 192.168.1.2 255.255.255.0
    end

  end
```

Configuring the ABCdomain VDOM

With the VDOMs created and the ISPs connected, the next step is to configure the ABCdomain VDOM.

Configuring the ABCdomain includes the following:

- Adding ABCdomain firewall addresses
- Adding the ABCdomain firewall policy
- Adding the ABCdomain default route

Adding ABCdomain firewall addresses

You need to define the addresses used by the ABC company internal network for use in firewall policies. This internal network is on the 172.100.1.0/255.255.255.0 subnet.

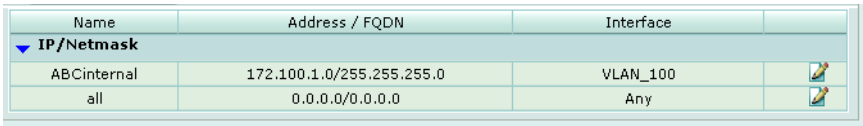
The FortiGate unit provides one default address, “all”, that you can use when a firewall policy applies to all addresses as the source or destination of a packet.

To add the ABCdomain firewall addresses - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.
2 Go to *System* > *VDOM*.
3 Select *ABCdomain*, and select *Enter*.
4 Go to *Firewall* > *Address*.
5 Select *Create New*.
6 Enter the following information and select *OK*:

Address Name	ABCinternal
Type	Subnet / IP Range
Subnet / IP Range	172.100.1.0/255.255.255.0
Interface	port1

Figure 33: ABCdomain VDOM firewall addresses



To add the ABCdomain VDOM firewall addresses - CLI

```
config vdom
  edit ABCdomain
    config firewall address
      edit ABCinternal
        set type ipmask
        set subnet 172.100.1.0 255.255.255.0
    end
  end
```

Adding the ABCdomain firewall policy

You need to add the ABCdomain firewall policy to allow traffic from the internal network to reach the external network, and from the external network to internal as well. You need two policies for this domain.

To add the ABCdomain firewall policy - web-based manager

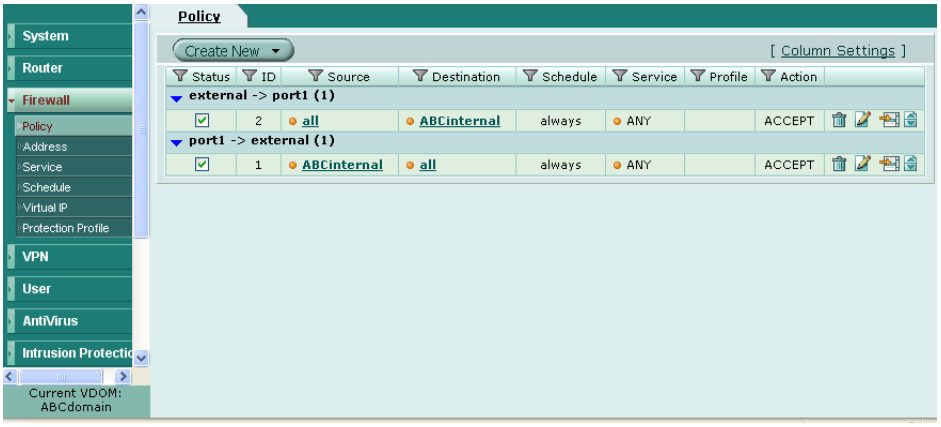
1. Go to *System* > *VDOM*.
2. Select *ABCdomain* and select *Enter*.
3. Go to *Firewall* > *Policy*.
4. Select *Create New*.
5. Enter the following information and select *OK*:

Source Interface/Zone	port1
Source Address	ABCinternal
Destination Interface/Zone	External
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

6. Select *Create New*.
7. Enter the following information and select *OK*:

Source Interface/Zone	External
Source Address	all
Destination Interface/Zone	port1
Destination Address	ABCinternal
Schedule	Always
Service	ANY
Action	ACCEPT

Figure 34: ABCdomain VDOM firewall policy



To add the ABCdomain firewall policy - CLI

```
config vdom
  edit ABCdomain
  config firewall policy
  edit 1
    set srcintf port1
    set srcaddr ABCinternal
    set dstintf external
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set status enable
  next
  edit 2
    set srcintf external
    set srcaddr all
    set dstintf port1
    set dstaddr ABCinternal
    set schedule always
    set service ANY
    set action accept
    set status enable
  end
end
```

Adding the ABCdomain default route

You also need to define a default route to direct packets to the ABC-ISP. Every VDOM needs a default static route to handle traffic addressed to external networks such as the Internet.

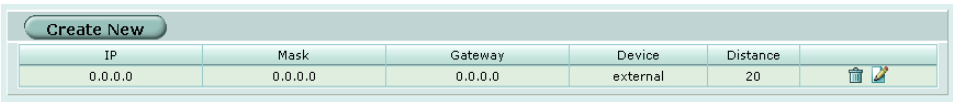
The administrative distance should be set slightly higher than other routes. Lower admin distances will get checked first, and this default route will only be used as a last resort.

To add a default route to the ABCdomain - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *VDOM* > *ABCdomain* and select *Enter*.
3. Goo to *Router* > *Static*.
4. Select *Create New*.
5. Enter the following information and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	external
Gateway	30.1.1.32
Distance	20

Figure 35: ABCdomain VDOM routing table



To add a default route to the ABCdomain - CLI

```
config vdom
  edit ABCdomain
  config router static
  edit 1
    set device external
    set gateway 30.1.1.32
  end
```

Configuring the DEFdomain VDOM

In this example, the DEFdomain VDOM is used for company DEF. Firewall and routing settings are specific to a single VDOM.

DEFdomain includes the FortiGate port2 interface to connect to the DEF internal network, and the FortiGate external interface to connect to the DEF ISP. Firewall policies are needed to allow traffic from port2 to external and from external to port2 interfaces.

This section includes the following topics:

Adding the DEFdomain firewall address

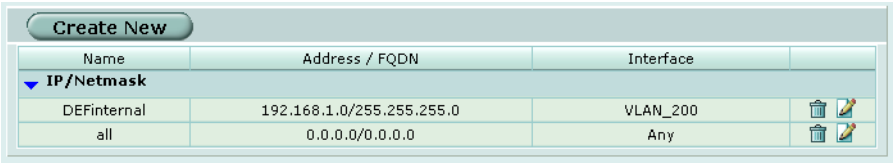
You need to define addresses for use in firewall policies. In this example, the DEFdomain VDOM needs an address for the port2 interface and the “all” address.

To add the DEFdomain firewall address - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Select *DEFdomain*, and select *Enter*.
4. Go to *Firewall* > *Address*.
5. Select *Create New*.
6. Enter the following information and select *OK*:

Address Name	DEFinternal
Type	Subnet / IP Range
Subnet / IP Range	192.168.1.0/255.255.255.0
Interface	port2

Figure 36: DEFdomain firewall addresses



To add the DEFdomain firewall address - CLI

```
config vdom
  edit DEFdomain
    config firewall address
      edit DEFinternal
        set type ipmask
        set subnet 192.168.1.0 255.255.255.0
  end
end
```

Adding the DEFdomain firewall policy

You also need a firewall policy for the DEF domain. In this example, the firewall policy allows all traffic.

To add the DEFdomain firewall policy - web-based manager

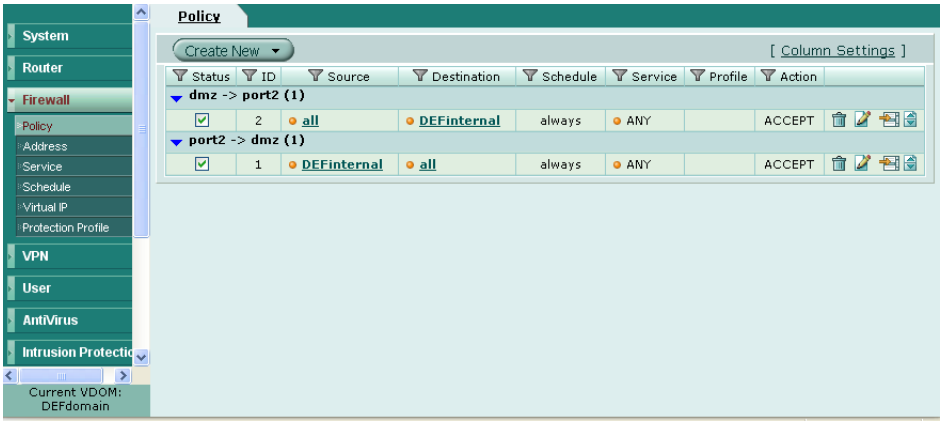
1. Log in with a super_admin account.
2. Go to *System* > *VDOM*.
3. Select *DEFdomain*, and select *Enter*.
4. Go to *Firewall* > *Policy*.
5. Select *Create New*.
6. Enter the following information and select *OK*:

Source Interface/Zone	port2
Source Address	DEFinternal
Destination Interface/Zone	dmz
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

7. Select *Create New*.
8. Enter the following information and select *OK*:

Source Interface/Zone	dmz
Source Address	all
Destination Interface/Zone	port2
Destination Address	DEFinternal
Schedule	Always
Service	ANY
Action	ACCEPT

Figure 37: DEFdomain firewall policy



To add the DEFdomain firewall policy - CLI

```
config firewall policy
  edit 1
    set srcintf port2
    set dstintf dmz
    set srcaddr DEFinternal
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set status enable
  edit 1
    set srcintf dmz
    set dstintf port2
    set srcaddr all
    set dstaddr DEFinternal
    set schedule always
    set service ANY
    set action accept
    set status enable
  end
```

Adding a default route to the DEFdomain VDOM

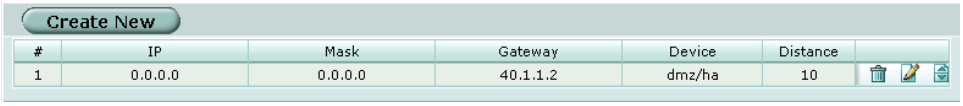
You need to define a default route to direct packets to the DEF ISP.

To add a default route to the DEFdomain VDOM - web-based manager

1. Log in as the super_admin administrator.
2. Go to *System* > *VDOM*.
3. Select *DEFdomain* and select *Enter*.
4. Go to *Router* > *Static*.
5. Select *Create New*.
6. Enter the following information and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	dmz/ha
Gateway	40.1.1.32
Distance	20

Figure 38: DEFdomain routing table



To add a default route to the DEFdomain VDOM - CLI

```
config router static
  edit 1
    set dst 0.0.0.0/0
    set device external
    set gateway 40.1.1.32
  end
```

Testing the configuration

Once you have completed configuration for both company VDOMs, you can use diagnostic commands, such as `tracert` in Windows, to test traffic routed through the FortiGate unit. Alternately, you can use the `traceroute` command on a Linux system with similar output.

Possible errors during the traceroute test are:

- "`***Request timed out`" - the trace was not able to make the next connection towards the destination fast enough
- "`Destination host unreachable`" - after a number of timed-out responses the trace will give up

Possible reasons for these errors are bad connections or configuration errors.

This section includes:

- Testing traffic from the ABC network to the ABC ISP
- Testing traffic from the DEF network to the DEF ISP

Testing traffic from the ABC network to the ABC ISP

In this example, a route is traced from the ABC internal network to the ABC ISP. The test was run on a Windows PC with an IP address of 172.100.1.17.

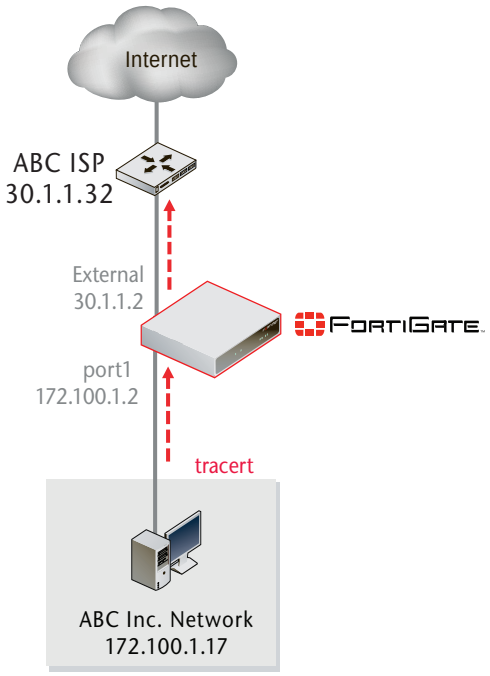
The output here indicates three hops between the source and destination, the IP address of each hop, and that the trace was successful.

From VLAN 100, access a command prompt and enter this command:

```
C:\>tracert 30.1.1.32
Tracing route to 30.1.1.32 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  172.100.1.2
  2   <10 ms   <10 ms   <10 ms  30.1.1.2
  3   <10 ms   <10 ms   <10 ms  30.1.1.32

Trace complete.
```

Figure 39: Example traceroute from ABC internal network to ABC ISP



Testing traffic from the DEF network to the DEF ISP

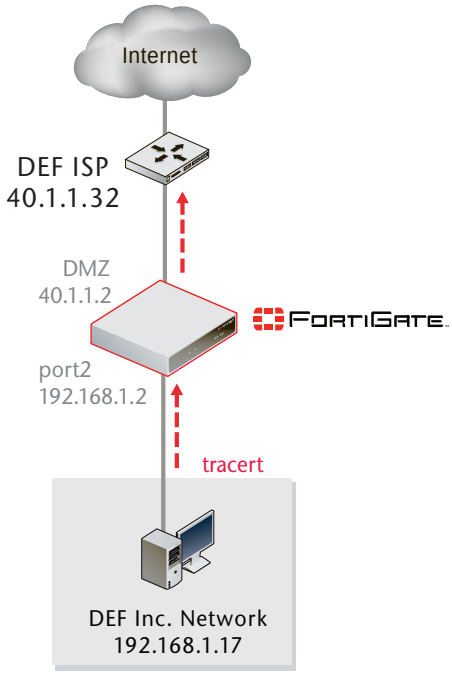
In this test, a route is traced from the DEF internal network to DEF ISP. The computer starting the traceroute command has an IP address of 192.168.1.17.

The output here indicates three hops between the source and destination, the IP address of each hop, and that the trace was successful.

From a computer on the DEF internal network, access an MS Windows command prompt and enter the following command.

```
C:\>tracert 40.1.1.32
Tracing route to 40.1.1.32 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  1192.168.1.2
  2   <10 ms   <10 ms   <10 ms  40.1.1.2
  3   <10 ms   <10 ms   <10 ms  40.1.1.32
Trace complete.
```

Figure 40: Example traceroute from DEF internal network to the ISP for DEF



Example VDOM configuration (advanced)

This example has two organizations, each with two different internal networks, and each with its own VDOM.

One organization is a school with both students and teachers using the network. The network has been broken down into one for the students and one for the teachers. This will allow for more security for the students, but still allow the teachers more access. Also, the teachers can access the student network to check assignments and help students, but students have no access to the teacher network. The school has a single ISP to access the Internet. This is all part of the School VDOM. Each network has its own VLAN as well.

The other organization is a business with a sales department, and a research and development (R&D) department. Both have different networking needs, especially when accessing the Internet and email—many sales contacts would look like spam to R&D. This organization has two ISP connections to the Internet for redundancy. This is all part of the Business VDOM, and each network has its own VLAN.

In this example, both VLANs and VDOMs are used to separate each organization and each network within each organization as well. This enables firewall policies better configured for the users on that network, and both the VDOMs and VLANs keep configurations from getting all mixed together. Each organization can have its own administrator which allows them to make changes more quickly to their configuration as needed.

This section includes the following topics:

Network topology and assumptions

The network topology for this VDOM example is complex and has many parts to configure. Figure 41 illustrates the network topology for this example. The remainder of this chapter describes how to configure the FortiGate-800 unit and Cisco Catalyst 2950 switches for this topology.

The School VDOM is configured as follows.

- The School internal networks are on the IP 192.168.10.0 and 192.168.20.0 subnets.
- The student network is VLAN 10 and is on the FortiGate internal interface.
- The instructor network is VLAN 20 and is also on the FortiGate internal interface.
- The School ISP, ATT-ISP, is on VLAN 30 and is on the FortiGate external interface.
- Firewall policies allow both the instructor and student networks to access the Internet through ATT-ISP, and allow the instructor network to access the student network. Students cannot access the instructor network.
- Students have a stricter protection profile than instructors.

The Business domain is configured as follows:

- The Business internal networks are on the IP 10.10.10.0 and 10.10.20.0 subnets.
- The Sales network is on VLAN 80 and is on the FortiGate internal interface.
- The R&D network is on VLAN 90 and is on the FortiGate internal interface.
- VLAN 40 and VLAN 50 are on the FortiGate external interface, and are configured for redundant access to the Internet via XO-ISP and XS-ISP.
- Firewall policies allow access to the Internet through the XO-ISP and XS-ISP networks from both Sales and R&D networks.
- Firewall policies allow access from the Sales network to the R&D network and from the R&D network to the Sales network.

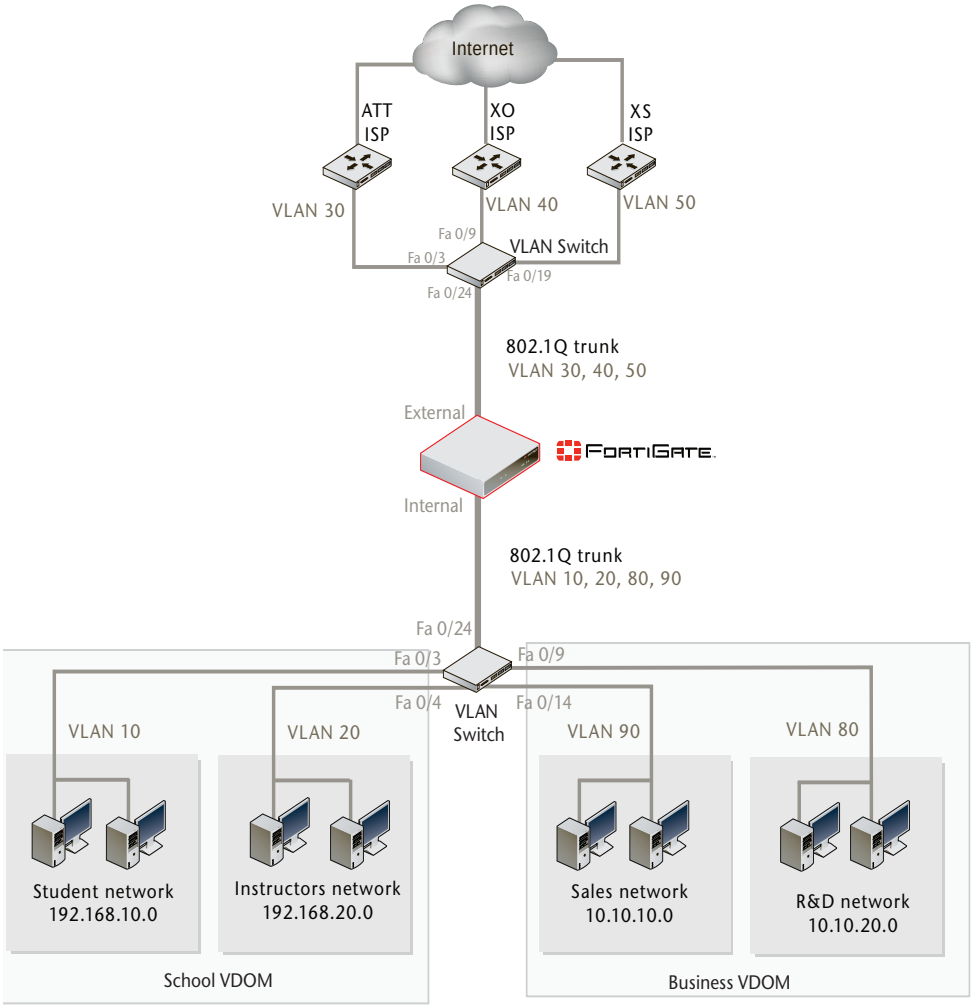
The student network and the R&D network share the same network address ranges. This does not cause a problem because the two address ranges reside in different VDOMs and different VLANs.

As in the earlier example, the FortiGate-800 is used; some labels may vary if your model is different.

The administrator is a super_admin account. If you are a using a non-super_admin account, refer to "Global and VDOM settings" on page 21 to see which parts a non-super_admin account can also configure.

When configuring firewall policies in the CLI always choose a policy number that is higher than any existing policy numbers, select `services` before `profile-status`, and `profile-status` before `profile`. If these commands are not entered in that order, they will not be available to enter.

Figure 41: Example VLAN/VDOM network topology (FortiGate unit in NAT/Route mode)



General configuration steps

This advanced example is broken down into smaller parts for easier configuration. For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Creating the VDOMs
2. Configuring the School VDOM
3. Configuring the Business VDOM
4. Configuring the VLAN switches
5. Testing the configuration

Creating the VDOMs

Two VDOMs are needed— the School VDOM for the teachers and students, and the Business VDOM for the company's Sales and R&D departments.

To create the VDOMs - web-based manager

1. Log in as the super_admin administrator.
2. Go to *System* > *VDOM* and select *Create New*.
3. Enter `School` and select *OK*.
4. Select *OK* again to return to the VDOM list.
5. Select *Create New*.
6. Enter `Business` and select *OK*.

To create the VDOMs - CLI

```
config vdom
  edit School
  next
  edit Business
  next
  end
```

Configuring the School VDOM

In this example, the School VDOM is used to serve a school. You configure two VLAN subinterfaces on the internal interface and one on the external interface. A firewall policy allows connections from the internal VLANs to the VLAN on the external interface.

This section includes the following topics:

- Adding the VLAN subinterfaces
- Adding a default route
- Adding the firewall addresses
- Adding the firewall policies

Adding the VLAN subinterfaces

In the School VDOM, you need two VLAN subinterfaces on the internal physical interface to receive the VLAN 10 and VLAN 20 packets from the students and instructor networks. You need a VLAN subinterface on the external interface to send packets to the ATT-ISP network on VLAN 30.

To add the VLAN subinterfaces - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *Network* > *Interface.*
3. Select *Create New*.
4. Enter the following information for the student network, and select *OK*:

Name	student
Type	VLAN
Interface	internal
VLAN ID	10
Virtual Domain	School
Addressing mode	Manual
IP/Netmask	192.168.10.1/255.255.255.0

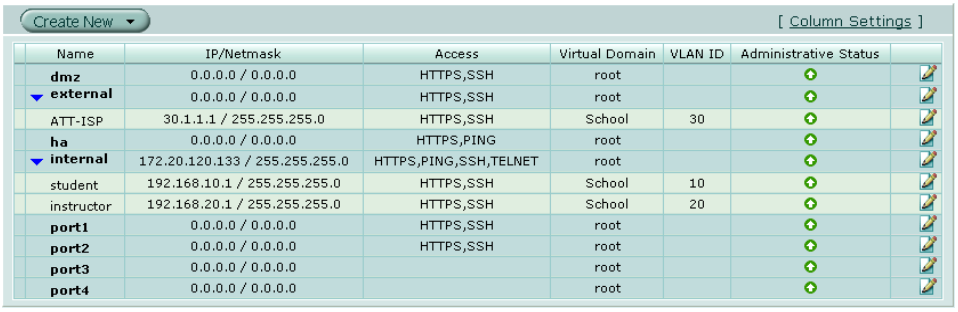
5. Select *Create New*.
6. Enter the following information for the instructor network, and select *OK*:

Name	instructor
Type	VLAN
Interface	internal
VLAN ID	20
Virtual Domain	School
Addressing mode	Manual
IP/Netmask	192.168.20.1/255.255.255.0

7. Select *Create New*.
8. Enter the following information for the ATT ISP network, and select *OK*:

Name	ATT-ISP
Type	VLAN
Interface	external
VLAN ID	30
Virtual Domain	School
Addressing mode	Manual
IP/Netmask	30.1.1.1/255.255.255.0

Figure 42: VLAN subinterfaces for School VDOM



To add the VLAN subinterfaces - CLI

```
config global
  config system interface
  edit student
    set interface internal
    set vlanid 10
    set vdom School
    set mode static
    set ip 192.168.10.1 255.255.255.0
  next
  edit instructor
    set interface internal
    set vlanid 20
    set vdom School
    set mode static
    set ip 192.168.20.1 255.255.255.0
  edit ATT-ISP
    set interface external
    set vlanid 30
    set vdom School
    set mode static
    set ip 30.1.1.1 255.255.255.0
  next
  end
```

Adding a default route

You need to define a default route for packets with destinations that are not on the FortiGate unit networks connected to the School VDOM. The simplest way to do this is to set the ISP gateway address as the route for all packets leaving the VLAN subinterface that is connected to the ISP.

To add a default route - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.
2 Go to *System* > *VDOM*.
3 Select *School* and select *Enter*.
4 Go to *Router* > *Static*.
5 Select *Create New*.
6 Enter the following information to add a default route to ATT-ISP for network traffic leaving the external interface from the School domain and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	ATT-ISP
Gateway	30.1.1.2
Distance	10

To add a default route - CLI

```
config vdom
  edit School
  config router static
  edit 1
    set device ATT-ISP
    set gateway 30.1.1.2
    set distance 10
  next
  end
```

Adding the firewall addresses

You need to define the addresses of the School VDOM subnets for use in firewall policies. In the School VDOM, the FortiGate unit provides one default address, “all”, that you can use when a firewall policy applies to all addresses as a source or destination of a packet. In other VDOMs, you have to create this address.

To add firewall addresses - web-based manager

1 Go to *System* > *VDOM.*
2 Select the School VDOM, and select *Enter*.
3 Go to *Firewall* > *Address*.
4 Select *Create New*.
5 Enter the following information and select *OK*:

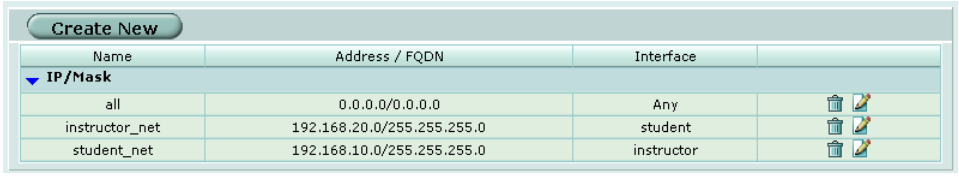
Address Name	student_net
Type	Subnet / IP Range
Subnet / IP Range	192.168.10.0/255.255.255.0
Interface	Any

6 Select *Create New*.

7 Enter the following information and select *OK*:

Address Name	instructor_net
Type	Subnet / IP Range
Subnet / IP Range	192.168.20.0/255.255.255.0
Interface	Any

Figure 43: Firewall addresses for School VDOM



To add firewall addresses - CLI

```
config vdom
  edit School
  config firewall address
  edit student_net
    set subnet 192.168.10.0 255.255.255.0
  next
  edit instructor_net
    set subnet 192.168.20.0 255.255.255.0
  next
  end
```

Adding the firewall policies

Each internal network needs a policy to permit it to access ATT-ISP for connection to the Internet. By choosing different protection profiles in each policy, the two groups of users can be subject to different levels of web filtering, web category filtering and content logging. For simplicity, this example uses the pre-configured “strict” protection profile. You can modify this or create custom protection profiles as needed.

Note: You can customize the Firewall Policy display by including some or all columns, and customize the column order onscreen. Due to this feature, firewall policy screenshots may not appear the same as on your screen.

The following five policies need to be defined.

- student to ATT-ISP
- ATT-ISP to student
- instructor to ATT-ISP
- ATT-ISP to instructor
- instructor and student

To add firewall policies - web-based manager

1. Go to *System* > *VDOM.*
2. Select the School VDOM, and select *Enter*.
3. Go to *Firewall* > *Policy.*
4. Select *Create New*.
5. Enter the following information and select *OK*.

   This policy allows traffic from the student network out to their ISP and the Internet.

Source Interface/Zone	student
Source Address	student_net
Destination Interface/Zone	ATT-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	strict

6. Select *Create New*.
7. Enter the following information and select *OK*.

   This policy allows traffic from the Internet and ISP to the student network.

Source Interface/Zone	ATT-ISP
Source Address	all
Destination Interface/Zone	student
Destination Address	student_net
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	strict

8. Select *Create New*.
9. Enter the following information and select *OK*.

   This policy allows traffic from the instructor network out to the Internet through the ATT ISP.

Source Interface/Zone	instructor
Source Address	instructor_net
Destination Interface/Zone	ATT-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	strict

10. Select *Create New*.

11 Enter the following information and select *OK*.

This policy allows traffic from the Internet and ISP in to the instructor network.

Source Interface/Zone	ATT-ISP
Source Address	all
Destination Interface/Zone	instructor
Destination Address	instructor_net
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	strict

12 Select *Create New*.

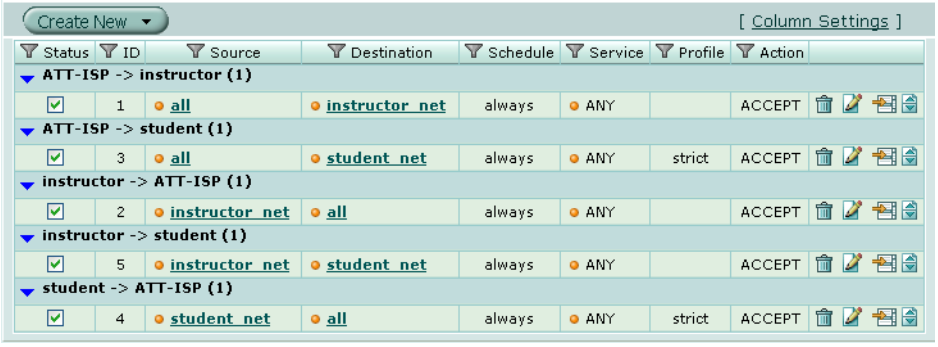
13 Enter the following information and select *OK*.

This policy allows instructors to access the student network.

There is no protection profile here because the communication is entirely on the internal network from teacher to student.

Source Interface/Zone	instructor
Source Destination Address	instructor_net
Destination Interface/Zone	student
Destination Address	student_net
Schedule	Always
Service	ANY
Action	ACCEPT

Figure 44: Firewall policies for School VDOM



To add firewall policies - CLI

```
config vdom
  edit School
  config firewall policy
  edit 1
    set srcintf ATT-ISP
    set dstintf instructor
    set srcaddr all
    set dstaddr instructor_net
    set action accept
```

```
    set schedule always
    set service ANY
    set profile-status enable
    set profile strict
  next
  edit 2
    set srcintf instructor
    set dstintf ATT-ISP
    set srcaddr instructor_net
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set profile-status enable
    set profile strict
  next
  edit 3
    set srcintf ATT-ISP
    set dstintf student
    set srcaddr all
    set dstaddr student_net
    set action accept
    set schedule always
    set service ANY
    set profile-status enable
    set logtraffic enable
    set profile strict
  next
  edit 4
    set srcintf student
    set dstintf ATT-ISP
    set srcaddr student_net
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set profile-status enable
    set logtraffic enable
    set profile strict
  next
  edit 5
    set srcintf instructor
    set dstintf student
    set srcaddr instructor_net
    set dstaddr student_net
    set action accept
    set schedule always
    set service ANY
  next
end
```

Configuring the Business VDOM

The Business VDOM serves a company with Sales and R&D networks.

The VLANs on the Business VDOM organize traffic from the departments, and make sure only computers on that VLAN receive the traffic. They also help with routing through the multiple ISP connections, in effect load balancing.

This section includes the following topics:

Adding the VLAN subinterfaces

In the Business VDOM, you need two VLAN subinterfaces on the internal physical interface to receive VLAN 80 and VLAN 90 packets from the Sales and R&D networks. You need two VLAN subinterfaces on the external interface to send packets to the XO-ISP network on VLAN 40, and to send packets to the XS-ISP network on VLAN 50.

To add the VLAN subinterfaces - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *Network* > *Interface*.
3. Select *Create New*.
4. Enter the following information for the Sales network and select *OK*:

Name	Sales
Type	VLAN
Interface	internal
VLAN ID	80
Virtual Domain	Business
Addressing mode	Manual
IP/Netmask	10.10.10.1/255.255.255.0

5. Select *Create New*.
6. Enter the following information for the R&D network and select *OK*:

Name	RnD
Type	VLAN
Interface	internal
VLAN ID	90
Virtual Domain	Business
Addressing mode	Manual
IP/Netmask	10.10.20.1/255.255.255.0

7. Select *Create New*.

8 Enter the following information for the XO ISP network and select *OK*:

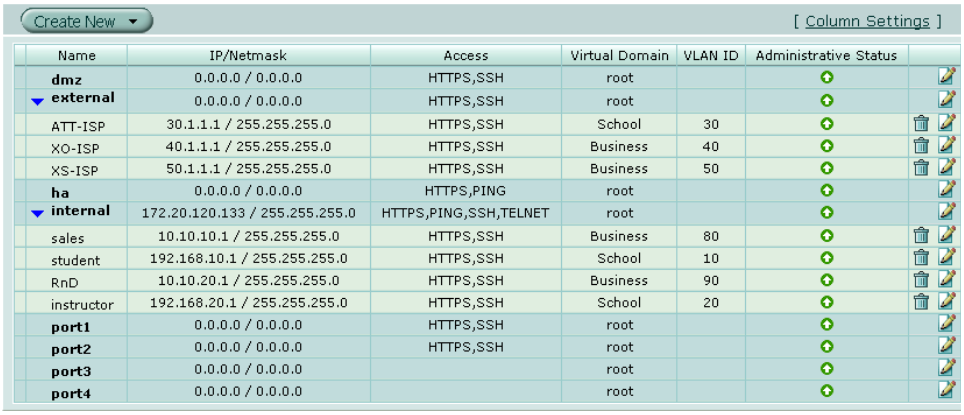
Name	XO-ISP
Type	VLAN
Interface	external
VLAN ID	40
Virtual Domain	Business
Addressing mode	Manual
IP/Netmask	40.1.1.1/255.255.255.0

9 Select *Create New*.

10 Enter the following information for the XS ISP network and select *OK*:

Name	XS-ISP
Interface	external
VLAN ID	50
Virtual Domain	Business
Addressing mode	Manual
IP/Netmask	50.1.1.1/255.255.255.0

Figure 45: VLAN subinterfaces for Business VDOM



To add the VLAN subinterfaces - CLI

```
config system interface
  edit Sales
    set interface internal
    set vlanid 80
    set vdom Business
    set mode static
    set ip 10.10.10.1 255.255.255.0
  next
  edit RnD
    set interface internal
    set vlanid 90
    set vdom Business
    set mode static
    set ip 10.10.20.1 255.255.255.0
  next
  edit XO-ISP
    set interface external
    set vlanid 40
    set vdom Business
    set mode static
    set ip 40.1.1.1 255.255.255.0
  next
  edit XS-ISP
    set interface external
    set vlanid 50
    set vdom Business
    set mode static
    set ip 50.1.1.1 255.255.255.0
  end
```

Adding a default route

You need to define a default static route for packets with destinations that are not on the FortiGate unit's networks. The simplest way to do this is to set the ISP gateway address as the route for all packets leaving the VLAN subinterface connected to the ISP.

As this example includes redundant ISPs, you also define a route to the secondary ISP with a greater administration distance. The FortiGate unit will send packets over this route only if the default route is not available. The behavior that we do want is both a main and a backup connection to the Internet.

You can configure dynamic routing if you want to, but that is beyond the scope of this example. For this example we will configure static routing.

To add a default route - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Go to *System* > *VDOM*.
3. Select the *Business* VDOM and select *Enter*.
4. Go to *Router* > *Static*.
5. Select *Create New*.

6 Enter the following information to add a default route to XO-ISP for network traffic leaving the external interface from the Business domain and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	XO-ISP
Gateway	40.1.1.2
Distance	10

7 Select *Create New*.

8 Enter the following information to add a secondary default route to XS-ISP for network traffic leaving the external interface from the Business domain and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	XS-ISP
Gateway	50.1.1.2
Distance	20

To add a default route - CLI

```
config router static
  edit 1
    set dst 0.0.0.0/0
    set device XO-ISP
    set gateway 40.1.1.2
    set distance 10
  next
  edit 2
    set dst 0.0.0.0/0
    set device XS-ISP
    set gateway 50.1.1.2
    set distance 20
  end
```

Adding the firewall addresses

You need to define the addresses of the Business VDOM subnets for use in firewall policies. In the ABCdomain VDOM, the FortiGate unit provides one default address, “all”, that you can use when a firewall policy applies to all addresses as a source or destination of a packet. In other VDOMs, you have to create this address.

To add the firewall addresses - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.

2 Go to *System* > *VDOM*.

3 Select the *Business* VDOM and select *Enter*.

4 Go to *Firewall* > *Address*.

5 Select *Create New*.

6 Enter the following information and select *OK*:

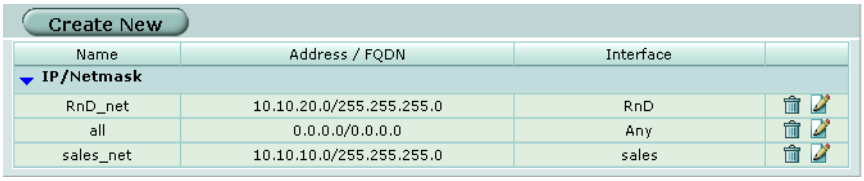
Address Name	RnD_net
Type	Subnet / IP Range
Subnet / IP Range	10.10.20.0/255.255.255.0

7 Select *Create New*.

8 Enter the following information and select *OK*:

Address Name	sales_net
Type	Subnet / IP Range
Subnet / IP Range	10.10.10.0/255.255.255.0

Figure 46: Firewall addresses for Business VDOM



To add the firewall addresses - CLI

```
config firewall address
  edit all
    set subnet 0.0.0.0 0.0.0.0
  next
  edit RnD_net
    set subnet 10.10.20.0 255.255.255.0
  next
  edit sales_net
    set subnet 10.10.10.0 255.255.255.0
  next
  end
```

Adding the firewall policies

The Business VDOM firewall policies have different goals than the School VDOM firewall policies. The Sales and R&D departments need access to the Internet and each other at all times. This is the reason for the two ISPs.

The FortiGate unit will scan all traffic going out or coming in for both the Sales and R&D networks, but will not block websites as it does for the student network in the School VDOM.

There are ten policies to be defined:

- Sales to XO-ISP
- XO-ISP to Sales
- Sales to XS-ISP
- XS-ISP to Sales
- RnD to XO-ISP
- XO-ISP to RnD
- RnD to XS-ISP
- XS-ISP to RnD
- RnD to Sales
- Sales to RnD

To add the firewall policies - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.
2 Go to *System* > *VDOM*.
3 Select the *Business* VDOM and select *Enter*.
1 Go to *Firewall* > *Policy*.
2 Select *Create New*.
3 Enter the following information and select *OK*.

Source Interface/Zone	Sales
Source Address	sales_net
Destination Interface/Zone	XO-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

4 Select *Create New*.
5 Enter the following information and select *OK*.

Source Interface/Zone	XO-ISP
Source Address	all
Destination Interface/Zone	Sales
Destination Address	sales_net
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

6 Select *Create New*.
7 Enter the following information and select *OK*:

Source Interface/Zone	Sales
Source Address	sales_net
Destination Interface/Zone	XS-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

8 Select *Create New*.

9 Enter the following information and select *OK*:

Source Interface/Zone	XS_ISP
Source Address	all
Destination Interface/Zone	Sales
Destination Address	sales_net
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

10 Select *Create New*.

11 Enter the following information and select *OK*:

Source Interface/Zone	RnD
Source Address	RnD_net
Destination Interface/Zone	XO-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

12 Select *Create New*.

13 Enter the following information and select *OK*:

Source Interface/Zone	XO_ISP
Source Address	all
Destination Interface/Zone	RnD
Destination Address	RnD_net
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

14 Select *Create New*.

15 Enter the following information and select *OK*:

Source Interface/Zone	RnD
Source Address	RnD_net
Destination Interface/Zone	XS-ISP
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

16 Select *Create New*.

17 Enter the following information and select *OK*:

Source Interface/Zone	XS_ISP
Source Address	all
Destination Interface/Zone	RnD
Destination Address	RnD_net
Schedule	Always
Service	ANY
Action	ACCEPT
Protection Profile	scan

18 Select *Create New*.

19 Enter the following information and select *OK*:

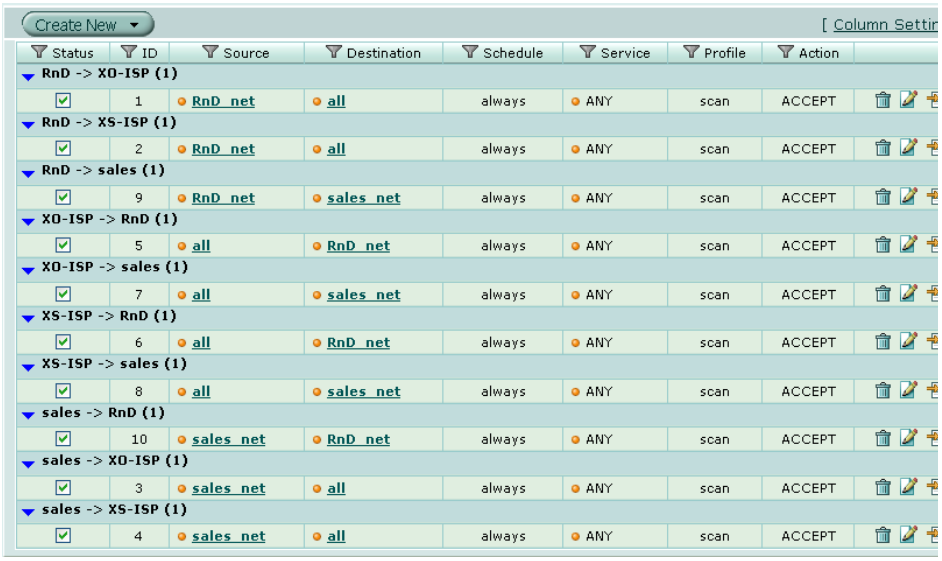
Source Interface/Zone	Sales
Source Address	sales_net
Destination Interface/Zone	RnD
Destination Address	RnD_net
Schedule	Always
Service	ANY
Action	ACCEPT

20 Select *Create New*.

21 Enter the following information and select *OK*:

Source Interface/Zone	RnD
Source Address	RnD_net
Destination Interface/Zone	Sales
Destination Address	sales_net
Schedule	Always
Service	ANY
Action	ACCEPT

Figure 47: Firewall policies for Business VDOM



To add the firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf Sales
    set dstintf XO-ISP
    set srcaddr sales_net
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set profile-status enable
    set profile scan
  next
  edit 2
    set srcintf XO-ISP
    set dstintf Sales
    set srcaddr all
    set dstaddr sales_net
    set action accept
    set schedule always
    set service ANY
    set profile-status enable
    set profile scan
  next
```

```
edit 3
  set srcintf Sales
  set dstintf XS-ISP
  set srcaddr sales_net
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
  set profile-status enable
  set profile scan
next
edit 4
  set srcintf XS-ISP
  set dstintf Sales
  set srcaddr all
  set dstaddr sales_net
  set action accept
  set schedule always
  set service ANY
  set profile-status enable
  set profile scan
next
edit 5
  set srcintf RnD
  set dstintf XO-ISP
  set srcaddr RnD_net
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
  set profile-status enable
  set profile scan
next
edit 6
  set srcintf XO-ISP
  set dstintf RnD
  set srcaddr all
  set dstaddr RnD_net
  set action accept
  set schedule always
  set service ANY
  set profile-status enable
  set profile scan
next
```

```
    edit 7
      set srcintf RnD
      set dstintf XS-ISP
      set srcaddr RnD_net
      set dstaddr all
      set action accept
      set schedule always
      set service ANY
      set profile-status enable
      set profile scan
    next
    edit 8
      set srcintf XS-ISP
      set dstintf RnD
      set srcaddr all
      set dstaddr RnD_net
      set action accept
      set schedule always
      set service ANY
      set profile-status enable
      set profile scan
    next
    edit 9
      set srcintf Sales
      set dstintf RnD
      set srcaddr sales_net
      set dstaddr RnD_net
      set action accept
      set schedule always
      set service ANY
      set profile-status enable
      set profile scan
    next
    edit 10
      set srcintf RnD
      set dstintf Sales
      set srcaddr RnD_net
      set dstaddr sales_net
      set action accept
      set schedule always
      set service ANY
      set profile-status enable
      set profile scan
    next
  end
```

Note: To complete the setup, configure devices on the VLANs with default gateways. The default gateway for VLAN 10 is the FortiGate VLAN 10 subinterface. Configure the rest of the devices, similarly matching the default gateway and FortiGate VLAN subinterface numbers.

Configuring the VLAN switches

In a multiple VDOM configuration, VLAN switches enable multiple networks to share the same physical interface. If there are enough available physical interfaces to support the internal networks, VLANs are not required. However, the configuration in this example is flexible and can be expanded with little additional configuration.

There are two VLAN switches in this example—one switch to combine internal network VLANs to one interface, and another switch to combine external VLANs onto one interface. Cisco 2950 Catalyst switches are used for this configuration. However, other VLAN switches can be used instead.

For more information on configuring your Cisco switch, please consult the Cisco manual.

This section includes the following topics:

Configuring the internal VLAN switch

The internal VLAN switch combines the 10, 20, 80, and 90 VLANs onto the FortiGate internal interface using a VLAN trunk link.

The following set of IOS commands will configure a Cisco 2950 Catalyst switch for this VLAN configuration.

```
!
interface FastEthernet0/3
 switchport access vlan 10
!
interface FastEthernet0/4
 switchport access vlan 20
!
interface FastEthernet0/14
 switchport access vlan 80
!
interface FastEthernet0/16
 switchport access vlan 90
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 10
Port 0/4	VLAN ID 20
Port 0/14	VLAN ID 80
Port 0/16	VLAN ID 90
Port 0/24	802.1Q trunk

Configuring the external VLAN switch

The external VLAN switch combines the 30, 40, and 50 VLANs onto the FortiGate external interface using a VLAN trunk link.

The following set of IOS commands will configure a Cisco 2950 Catalyst switch for this VLAN configuration.

```
!
interface FastEthernet0/3
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 40
!
interface FastEthernet0/19
 switchport access vlan 50
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 30
Port 0/9	VLAN ID 40
Port 0/19	VLAN ID 50
Port 0/24	802.1Q trunk

Testing the configuration

You can use simple diagnostic commands, such as tracert, to test traffic routed through the FortiGate unit and the Cisco switches.

This section includes the following topics:

- Testing traffic from instructor network to student network
- Other tests

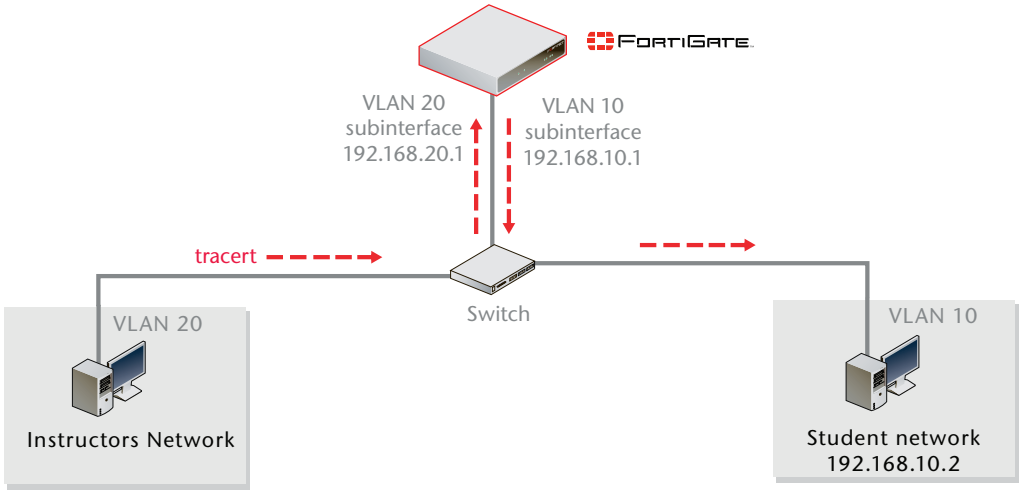
Testing traffic from instructor network to student network

In this example, a route is traced from the instructor network to the student network. The route target is a host on the student network.

From the instructor network, access an MS Windows command prompt and enter this command:

```
C:\>tracert 192.168.10.2
Tracing route to 192.168.10.2 over a maximum of 30 hops:
  1    <10 ms    <10 ms    <10 ms 192.168.20.1
  2    <10 ms    <10 ms    <10 ms 192.168.10.2
Trace complete.
```

Figure 48: Example traceroute from VLAN 20 to VLAN 10



Other tests

Using the preceding method, you can test traffic in the following directions:

- from the R&D network to the Sales network
- from the R&D network to the Internet
- from the Sales network to the R&D network
- from the Sales network to the Internet

Once these routes are confirmed to be working properly, the network will be fully functional.

Inter-VDOM routing

In the past, virtual domains (VDOMs) were separate from each other—there was no internal communication. Any communication between VDOMs involved traffic leaving on a physical interface belonging to one VDOM and re-entering the FortiGate unit on another physical interface belonging to another VDOM to be inspected by firewall policies in both directions.

Inter-VDOM routing changes this. With VDOM links, VDOMs can communicate internally without using additional physical interfaces.

Inter-VDOM routing is the communication between VDOMs. VDOM links are virtual interfaces that connect VDOMs. A VDOM link contains a pair of interfaces with each one connected to a VDOM, and forming either end of the inter-VDOM connection.

This chapter contains the following sections:

Benefits of inter-VDOM routing

Inter-VDOM routing has a number of advantages over independent VDOM routing. These benefits include:

Freed-up physical interfaces

Tying up physical interfaces on the FortiGate unit presents a problem. With a limited number of interfaces available, configuration options for the old style of communication between VDOMs are very limited. VLANs can be an answer to this, but they have some limitations.

For example, the FortiGate-800 has 8 physical ethernet ports. If they are assigned 2 per VDOM (one each for external and internal traffic) there can only be 4 VDOMs at most configured, not the 10 VDOMs the license will allow. Adding even one additional interface per VDOM to be used to communicate between VDOMs leaves only 2 VDOMs for that configuration, since it would required 9 interfaces for 3 VDOMs. Even using one physical interface for both external traffic and inter-VDOM communication would severely lower the available bandwidth for external traffic on that interface.

With the introduction of inter-VDOM routing, traffic can travel between VDOMs internally, freeing up physical interfaces for external traffic. Using the above example we can use the 4 VDOM configuration and all the interfaces will have their full bandwidth.

More speed than physical interfaces

Internal interfaces are faster than physical interfaces. Their speed depends on the CPU and its load. That means that an inter-VDOM link interface will be faster than a outbound physical interface connected to another inbound physical interface.

However, while one virtual interface with normal traffic would be considerably faster than on a physical interface, the more traffic and more internal interfaces you configure, the slower they will become until they are slower than the physical interfaces. CPU load can come from other sources such as AV or content scanning. This produces the same effect—internal interfaces such as inter-VDOM links will be slower.

Continued support for secure firewall policies

VDOMs help to separate traffic based on your needs. This is an important step in satisfying regulations that require proof of secure data handling. This is especially important to health, law, accounting, and other businesses that handle sensitive data every day.

By keeping things separate, traffic has to leave the FortiGate unit and re-enter to change VDOMs. This forces traffic to go through the firewall when leaving and enter through another firewall, keeping traffic secure.

With inter-VDOM routing, the need for the physical interfaces is greatly reduced. However, firewall policies still need to be in place for traffic to pass through any interface, physical or virtual, and thus provide the same level of security both internally and externally. Configuration of firewall policies is the same for inter-VDOM links as for any other interface, and your data will continue to have the high level of security.

Configuration flexibility

A typical VDOM uses at least two interfaces, typically physical interfaces, one for internal and one for external traffic. Depending on the configuration, more interfaces may be required. The one exception to this is possibly one-armed IPS.

As explained earlier, the maximum number of VDOMs configurable on a FortiGate unit is the number of physical interfaces available divided by two. VLANs can increase the number by providing multiple virtual interfaces over a single physical interface, but VLANs have some limitations.

Using physical interfaces for inter-VDOM communication severely limits the number of possible configurations on your FortiGate unit, but inter-VDOM routing allows these connections to be moved inside the FortiGate unit. Using virtual interfaces, VDOM links, frees up the physical interfaces for external traffic. Using VDOM links on a FortiGate unit with 8 interfaces, you can have 4 VDOMs communicating with each other (meshed configuration) and continue to have 2 physical interfaces each for internal and external connections. This configuration would have required 20 physical interfaces without inter-VDOM routing. With inter-VDOM routing it only requires 8 physical interfaces, with the other 12 interfaces being internal VDOM links.

Inter-VDOM routing allows you to select Standalone VDOM configuration, Management VDOM configuration and Meshed VDOM configuration without being limited by the number of physical interfaces on your FortiGate unit.

Getting started with VDOM links

Once VDOMs are configured on your FortiGate unit, configuring inter-VDOM routing and VDOM-links is very much like creating a VLAN interface.

VDOM-links are managed through the web-based manager or CLI. In the web-based manager, VDOM link interfaces are managed in the network interface list.

This section includes the following topics:

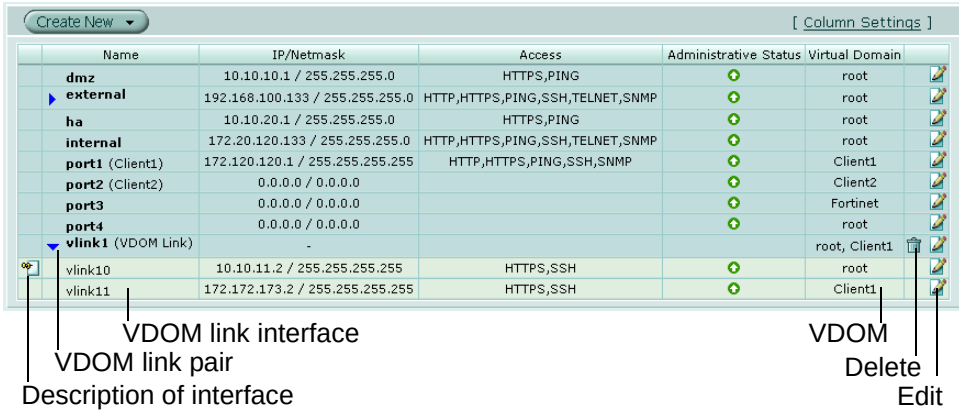
Viewing VDOM links

VDOM links are displayed on the network interface list in the web-based manager.

You can view VDOM links only if you are using a super_admin account and in global configuration.

To view the network interface list go to *System* > *Network.*

Figure 49: Interface list displaying names, IP/netmask, access, administrative status, and VDOMs



Create New	Select the arrow to create a new VDOM link. For more information, see "Creating VDOM links" on page 128.
Column Settings	Select to change which information is displayed about the interfaces, and in which order the columns appear. Use to display VDOM, VLAN, and other information. For more information, see "Adding VLAN subinterfaces" on page 28.
Name	The name of the interface. The name of the VDOM link (`vlink1`) has an expand arrow to display or hide the pair of VDOM link interfaces. For more information, see "Viewing VDOM links" on page 127.
Virtual Domain	The virtual domain this interface belongs to. For more information on VDOMs, see "Using VDOMs in NAT/Route mode" on page 59.
Delete	Select to remove the VDOM link or virtual interface. You cannot delete a physical interface. For more information, see "Deleting VDOM links" on page 129.
Edit	Select to change interface configuration.

Creating VDOM links

VDOM links connect VDOMs together to allow inter-VDOM routing.

To create a VDOM link, you first create the point-to-point interface, and then bind the two interface objects associated with it to virtual domains.

In creating the point-to-point interface, you also create two additional interface objects by default. They are called `vlink10` and `vlink11` - the interface name you chose with a 1 or a 0 to designate the two ends of the link.

Once the interface objects are bound, they are treated like normal FortiGate interfaces and need to be configured just like regular interfaces.

The assumptions for this example are as follows:

- Your FortiGate unit has VDOMs enabled and you have 2 VDOMs called `customer1` and `customer2` already configured. For more information on configuring VDOMs see "Creating, disabling, and deleting VDOMs" on page 63.
- You are using a super_admin account.

Note: Inter-VDOM links cannot include VDOMs in Transparent mode.

To configure an inter-VDOM link - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *System* > *Network*.
3. Select *Create New* > *VDOM link*, enter the following information, and select *OK*.

Name	vlink1 (The name can be up to 11 characters long. Valid characters are letters, numbers, "-", and "_". No spaces are allowed.)
Interface #0	
Virtual Domain	customer1
IP/Netmask	10.11.12.13/255.255.255.0
Administrative Access	HTTPS, SSL
Interface #1	
Virtual Domain	customer2
IP/Netmask	172.120.100.13/255.255.255.0
Administrative Access	HTTPS, SSL

Note: If your inter-VDOM links have names longer than 8 characters, and you upgrade from FortiOS 3.0 MR3, the names will be truncated to 8 characters and will not function. The solution is to change the names of your inter-VDOM links before you upgrade.

To configure an inter-VDOM link - CLI

```
config global
  config system vdom-link
    edit vlink1
  next
end
config system interface
  edit vlink10
    set vdom customer1
  next
  edit vlink11
    set vdom customer2
  next
end
```

Once you have created and bound the interface ends to VDOMs, configure the appropriate firewall policies and other settings that you require. To confirm the inter-VDOM link was created, find the VDOM link pair and use the expand arrow to view the two VDOM link interfaces. You can select edit to change any information.

Deleting VDOM links

When you delete the VDOM link, the two link objects associated with it will also be deleted. You cannot delete the objects by themselves. The example uses a VDOM routing connection called “vlink1”. Removing vlink1 will also remove its two link objects vlink10 and vlink11.

Note: Before deleting the VDOM link, ensure all policies, firewalls, and other configurations that include the VDOM link are deleted, removed, or changed to no longer include the VDOM link.

To remove a VDOM link - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *System* > *Network*.
3. Select *Delete* for the VDOM link *vlink1*.

To remove a VDOM link - CLI

```
config global
  config system vdom-link
    delete vlink1
  end
```

For more information, see the *FortiGate CLI Reference*.

Advanced inter-VDOM issues

While VDOM links behave almost exactly like a physical interface, there are some situations where they have limitations or slightly different behavior. These areas include:

- Advanced inter-VDOM routing
- HA virtual clusters and VDOM links

Advanced inter-VDOM routing

BGP is supported over inter-VDOM links. Unless otherwise indicated, routing works as expected over inter-VDOM links.

HA virtual clusters and VDOM links

FortiGate HA is implemented by configuring two or more FortiGate units to operate as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewall, VPN, IPS, virus scanning, web filtering, and spam filtering.

Virtual clustering extends HA features to provide failover protection and load balancing for a FortiGate unit operating with virtual domains. A virtual cluster consists of a cluster of two FortiGate units operating with virtual domains. Traffic on different virtual domains can be load balanced between the cluster units.

With virtual clusters (vclusters) configured, inter-VDOM links must be entirely within one vcluster. You cannot create links between vclusters, and you cannot move a VDOM that is linked into another virtual cluster. If your FortiGate units are operating in HA mode, with multiple vclusters when you create the vdom-link, the CLI command `config system vdom-link` includes an option to set which vcluster the link will be in. For more information on HA configurations, see the HA section of the *FortiGate Administration Guide* or the *FortiGate HA Guide*.

Inter-VDOM configurations and planning

By using fewer physical interfaces to inter-connect VDOMs, inter-VDOM links provide you with more configuration options.

None of these configurations use VLANs to reduce the number of physical interfaces. It is generally assumed that an internal or client network will have its own internal interface and an external interface to connect to its ISP and the Internet.

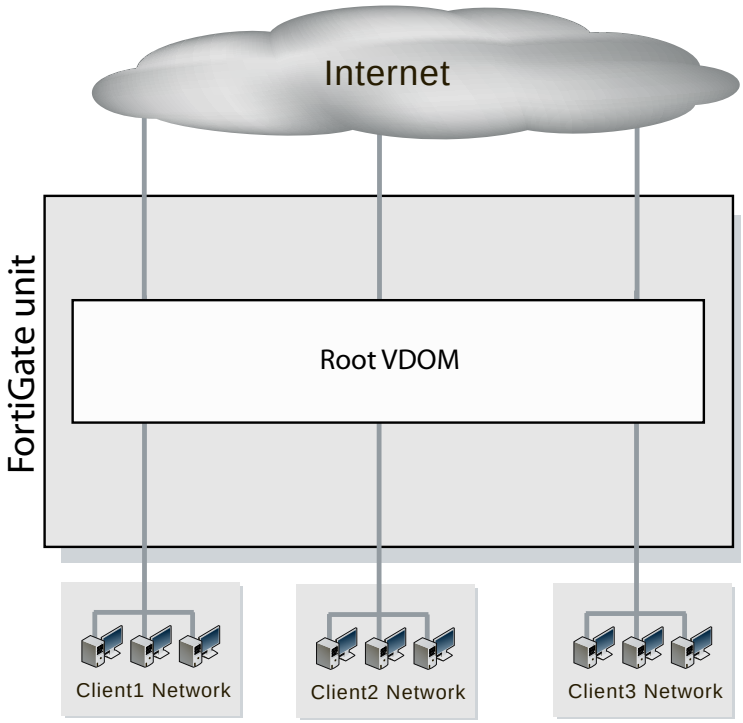
These inter-VDOM configurations can use any FortiGate model with possible limitations based on the number of physical interfaces. VLANs can be used to work around these limitations.

This section includes the following topics:

Standalone VDOM configuration

The standalone VDOM configuration uses a single VDOM on your FortiGate unit—the root VDOM that all FortiGate units have by default. This is the VDOM configuration you are likely familiar with. It is the default configuration for FortiGate units before you create additional VDOMs.

Figure 50: Standalone VDOM



The configuration shown in Figure 50 has no VDOM inter-connections and requires no special configurations or settings.

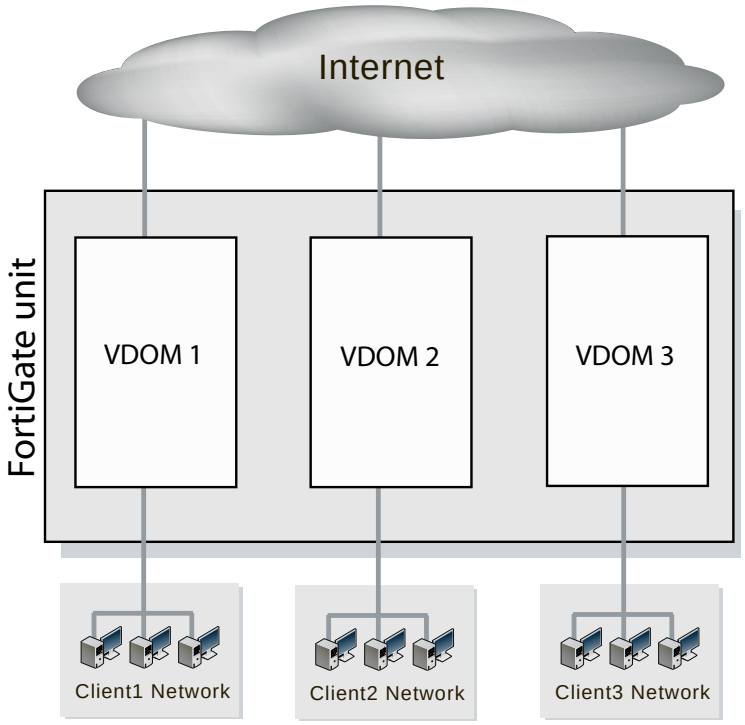
The standalone VDOM configuration can be used for simple network configurations that only have one department or one company administering the connections, firewalls and other VDOM-dependent settings.

However, with this configuration, keeping client networks separate requires many interfaces, considerable firewall design and maintenance, and can quickly become time consuming and complex. Also, configuration errors for one client network can easily affect other client networks, causing unnecessary network downtime.

Independent VDOMs configuration

The independent VDOMs configuration uses multiple VDOMs that are completely separate from each other. This is another common VDOM configuration.

Figure 51: Independent VDOMs



This configuration has no communication between VDOMs and, apart from initially setting up each VDOM, requires no special configurations or settings. Any communication between VDOMs is treated as if communication is between separate physical devices.

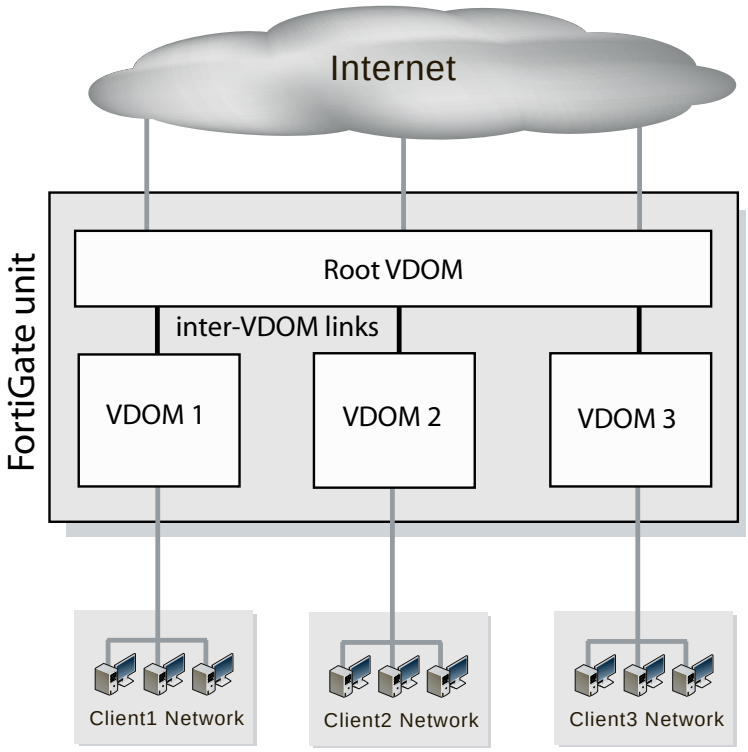
The independent inter-VDOM configuration can be used where more than one department or one company is sharing the FortiGate unit. Each can administer the connections, firewalls and other VDOM-dependent settings for only its own VDOM. To each company or department, it appears as if it has its own FortiGate unit. This configuration reduces the amount of firewall configuration and maintenance required by dividing the work between them.

However, this configuration lacks a management VDOM for VDOMs 1, 2, and 3. This is illustrated in Figure 50. This management VDOM would enable an extra level of control for the FortiGate unit administrator, while still allowing each company or department to administer its own VDOM.

Management VDOM configuration

In the management VDOM configuration, the root VDOM is the management VDOM. The other VDOMs are connected to the management VDOM with inter-VDOM links. There are no other inter-VDOM connections.

Figure 52: Management VDOM configuration



The inter-VDOM links connect the management VDOM to the other VDOMs. This does not require any physical interfaces, and the bandwidth of inter-VDOM links can be faster than physical interfaces, depending on the CPU workload.

Only the management VDOM is connected to the Internet. The other VDOMs are connected to internal networks. All external traffic is routed through the management VDOM using inter-VDOM links and firewall policies between the management VDOM and each VDOM. This ensures the management VDOM has full control over access to the Internet, including what types of traffic are allowed in both directions. There is no communication directly between the non-root VDOMs. Security is greatly increased with only one point of entry and exit. Only the management VDOM needs to be fully managed to ensure network security in this case. Each client network can manage its own configuration without compromising security or bringing down another client network.

The management VDOM configuration is ideally suited for a service provider business. The service provider administers the management VDOM with the other VDOMs as customers. These customers do not require a dedicated IT person to manage their network. The service provider controls the traffic and can prevent the customers from using banned services and prevent Internet connections from initiating those same

banned services. One example of a banned service might be Instant Messaging (IM) at a company concerned about intellectual property. Another example could be to limit bandwidth used by file-sharing applications without banning that application completely. Firewall policies control the traffic between the customer VDOM and the management VDOM and can be customized for each customer.

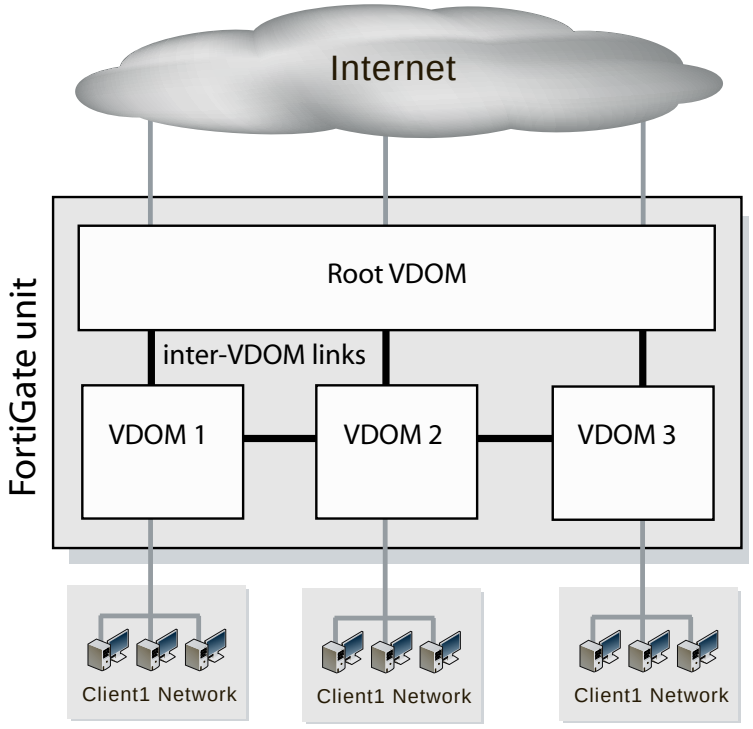
The management VDOM configuration is limited in that the customer VDOMs have no inter-connections. In many situations this limitation is ideal because it maintains proper security. However, some configurations may require customers to communicate with each other, which would be easier if the customer VDOMs were inter-connected.

Meshed VDOM configuration

The meshed VDOMs configuration, including partial and full mesh, has VDOMs inter-connected with other VDOMs. There is no special feature to accomplish this—they are just complex VDOM configurations.

Partial mesh means only some VDOMs are inter-connected. In a full mesh configuration, all VDOMs are inter-connected to all other VDOMs. This can be useful when you want to provide full access between VDOMs but handle traffic differently depending on which VDOM it originates from or is going to.

Figure 53: Meshed VDOMs



With full access between all VDOMs being possible, it is extra important to ensure proper security. You can achieve this level of security by establishing extensive firewall policies and ensuring secure account access for all administrators and users.

Meshed VDOM configurations can become complex very quickly, with full mesh VDOMs being the most complex. Ensure this is the proper solution for your situation before using this configuration. Generally, these configurations are seen as theoretical and are rarely deployed in the field.

Inter-VDOM planning

Inter-VDOM routing enables more FortiGate unit configurations than were previously possible. This additional flexibility has benefits, but also has potential difficulties.

Complexity

With more connections possible in inter-VDOM configurations, complexity quickly becomes an issue. VDOMs are not trivial to manage and, with additional settings and issues to consider, things can easily get out of hand. For example, a minimum of 12 firewall policies are needed for a 3-VDOM fully-meshed (unmanaged) configuration, compared to only 2 for a standalone VDOM configuration. Each additional firewall policy slows down troubleshooting and increases administration time required.

To prevent difficulties, you should carefully plan your move to an inter-VDOM configuration, ensuring you are aware of the differences between your new and old setups as well as how these changes affect the interaction between the VDOMs.

Inter-VDOM and changes to your operating system

Once configured, this new complex configuration means that any changes you make to the system have a greater chance of introducing problems into the system. Extra care should be taken to make sure any changes do not negatively affect your existing FortiGate unit configuration. This is especially true for meshed and fully meshed configurations.

For example, using the old method to change communication between VDOMs, cable connections had to be physically changed. Compared to inter-VDOM where all the changes are internal, there is generally more checking built into the physical process than there is for simple CLI commands. This lowered level of checking may allow unintended changes in VDOM interactions to slip into the configuration undetected.

Example of inter-VDOM routing

This example shows how to configure a FortiGate unit to use inter-VDOM routing.

This section contains the follow topics:

Network topology and assumptions

Two departments of a company, Accounting and Sales, are connected to one FortiGate-800 unit. To do its work, the Sales department receives a lot of email from advertising companies that would appear to be spam if the Accounting department received it. For this reason, each department has its own VDOM to keep firewall policies and other configurations separate. A management VDOM makes sense to ensure company policies are followed for traffic content.

The traffic between Accounting and Sales will be email and HTTPS only. It could use a VDOM link for a meshed configuration, but we will keep from getting too complex. With the configuration, inter-VDOM traffic will have a slightly longer path to follow than normal—from one department VDOM, through the management VDOM, and back to the other department VDOM. Since inter-VDOM links are faster than physical interfaces, this longer path should not be noticed.

Firewall policies will be in place. For added security, firewall policies will allow only valid office services such as email, web browsing, and FTP between either department and the Internet. Any additional services that are required can be added in the future.

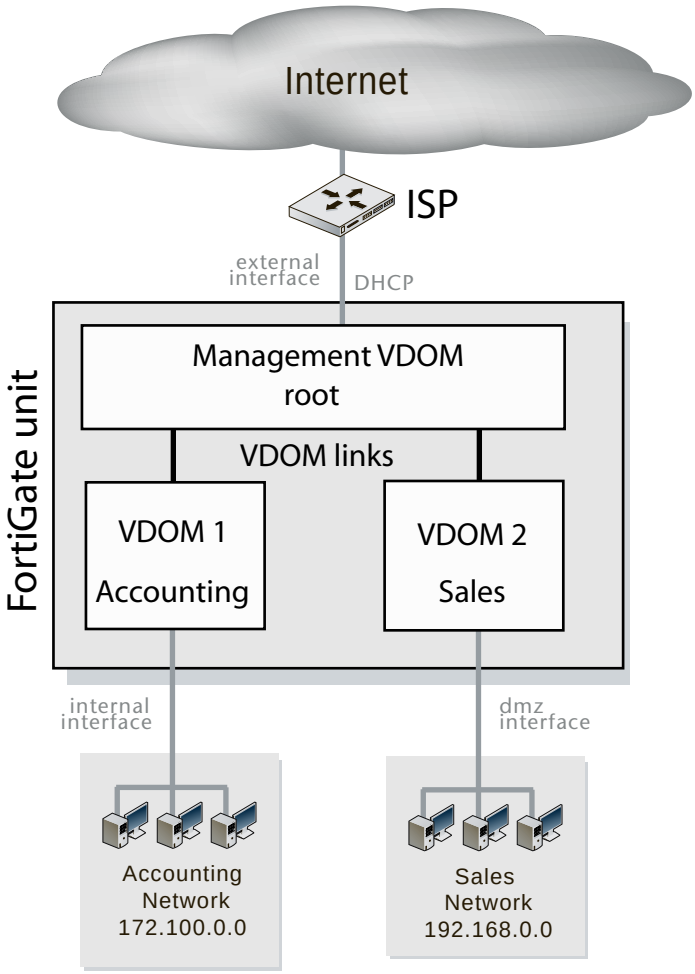
The company uses a single ISP to connect to the Internet. The ISP uses DHCP to provide an IP address to the FortiGate unit. Both departments use the same ISP to reach the Internet.

Other assumptions for this example are as follows:

- Your unit is a FortiGate-800 and has no VDOMs at the start.
- You are using a super_admin account.
- You have the FortiClient application installed.

Note: All configuration is available to a super_admin. A non-super_admin account may also perform certain procedures, but only for the VDOM that the account has access to. For more information, see “Creating VDOM administrators” on page 66.

Figure 54: Management VDOM for two departments



General configuration steps

This example includes the following general steps. For best results, follow the steps in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Creating the VDOMs
2. Configuring the physical interfaces
3. Configuring the VDOM links
4. Configuring the firewall settings
5. Testing the configuration

Creating the VDOMs

This procedure enables VDOMs and creates the Sales and Accounting VDOMs.

To create the VDOMs - web-based manager

1. Log in with a super_admin profile account.
2. Go to *System* > *Status* > *System Information* > *Virtual Domain*, and select *Enable*.
3. Log in again.
4. Go to *System* > *VDOM*.
5. Select *Create New*, name the new VDOM “Accounting”, and select *OK*.
6. Select *Create New*, name the new VDOM “Sales”, and select *OK*.

To create the VDOMs - CLI

```
config system global
  set vdom enable
end

config system vdom
  edit Accounting
  next
  edit Sales
  next
end
```

Configuring the physical interfaces

Next, the physical interfaces must be configured. This example uses three interfaces on the FortiGate-800 unit - internal, dmz, and external. Internal and dmz interfaces each have a department’s network connected. External is for all traffic to or from the Internet and will use DHCP to configure its IP address.

Tip: If your unit has different labels, you can create an alias to help identify internal, external and dmz interfaces.Go to *System* > *Network* and select the *Edit* icon for the physical interface. Add a descriptive name for *Alias* and select *OK* to save your settings.

To configure the physical interfaces - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *System* > *Network*.
3. Select *Edit* for the port1 interface, enter the following information, and select *OK*.

Alias	AccountingLocal
Virtual Domain	Accounting
Addressing mode	Manual
IP/Netmask	172.100.1.1/255.255.0.0
Administrative Access	HTTPS, PING, SSH
Description	This is the accounting department internal interface.

4 Select *Edit* for the port2 interface, enter the following information, and select *OK*.

Alias	SalesLocal
Virtual Domain	Sales
Addressing mode	Manual
IP/Netmask	192.168.1.1/255.255.0.0
Administrative Access	HTTPS, PING, SSH
Description	This is the sales department internal interface.

5 Select *Edit* for the external interface, enter the following information, and select *OK*.

Alias	ManagementExternal
Virtual Domain	root
Addressing Mode	DHCP
Distance	5
Retrieve default gateway from server	Enable
Override internal DNS	Enable
Administrative Access	HTTPS, SSH, SNMP
Description	This is the accounting department internal interface.

Note: When the mode is set to DHCP or PPoE on an interface you can set the distance field. This is the administrative distance for any routes learned through the gateway for this interface. The gateway is added to the static route table with these values. A lower distance indicates a preferred route.

To configure the physical interfaces - CLI

```
config global
config system interface
  edit port1
    set alias AccountingLocal
    set vdom Accounting
    set mode static
    set ip 172.100.1.1 255.255.0.0
    set allowaccess https ping ssh
    set description “The accounting dept internal interface”
  next
  edit port2
    set alias SalesLocal
    set vdom Sales
    set mode static
    set ip 192.168.1.1 255.255.0.0
    set allowaccess https ping ssh
    set description “The sales dept. internal interface”
  next
```

```
  edit external
    set alias ManagementExternal
    set vdom root
    set mode DHCP
    set distance 5
    set gwdetect enable
    set dns-server-override enable
    set allowaccess https ssh snmp
    set description “The systemwide management interface.”
  next
end
end
```

Configuring the VDOM links

To complete the connection between the two VDOMs and the management VDOM, we need to add the two pairs of VDOM link interfaces; one pair is for Accounting - management VDOM and the other is for Sales - management VDOM.

To configure the Accounting and management VDOM link - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *System* > *Network*.
3. Select the expand (down) arrow for *Create New* > *VDOM link*, enter the following information, and select *OK*.

Name	AccountVlnk
Interface #0	
Virtual Domain	Accounting
IP/Netmask	10.0.0.1/255.255.255.0
Administrative Access	HTTPS, PING, SSH
Description	The Accounting VDOM side of the link.
Interface #1	
Virtual Domain	root
IP/Netmask	10.0.0.1/255.255.255.0
Administrative Access	HTTPS, PING, SSH
Description	The Management VDOM side of the link.

To configure the Accounting and management VDOM link - CLI

```
config global
config system vdom-link
  edit AccountVlnk
  next
end
config system interface
  edit AccountVlnk0
    set vdom Accounting
    set ip 10.0.0.1 255.255.255.0
    set allowaccess https ping ssh
    set description “Accounting side of the VDOM link“
  next
```

```
  edit AccountVlnk1
    set vdom root
    set ip 10.0.0.1 255.255.255.0
    set allowaccess https ping ssh
    set description “Management side of the VDOM link“
  next
  end
end
```

To configure the Sales and management VDOM link - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *System* > *Network*.
3. Select the expand (down) arrow for *Create New* > *VDOM link*, enter the following information, and select *OK*.

Name	SalesVlnk
Interface #0	
Virtual Domain	Sales
IP/Netmask	10.0.1.1/255.255.255.0
Administrative Access	HTTPS, PING, SSH
Description	The Sales VDOM side of the link.
Interface #1	
Virtual Domain	root
IP/Netmask	10.0.1.1/255.255.255.0
Administrative Access	HTTPS, PING, SSH
Description	The Management VDOM side of the link.

To configure the Sales and management VDOM link - CLI

```
config global
config system vdom-link
  edit SalesVlnk
  next
end
config system interface
  edit SalesVlnk0
    set vdom Accounting
    set ip 10.0.1.1 255.255.255.0
    set allowaccess https ping ssh
    set description “Sales side of the VDOM link“
  next
  edit SalesVlnk1
    set vdom root
    set ip 10.0.1.1 255.255.255.0
    set allowaccess https ping ssh
    set description “Management side of the VDOM link“
  next
  end
end
```

Configuring the firewall settings

With the VDOMs, physical interfaces, and VDOM links configured the firewall must now be configured to allow the proper traffic. The firewall for each VDOM must be configured from within that VDOM.

The firewall group of services allowed between the internal networks and the Internet are the basic services for web browsing, file transfer, and email - HTTP, HTTPS, SSL, FTP, DNS, NTP, POP3, and SMTP.

The only services allowed between Sales and Accounting are secure web browsing (HTTPS) and email (POP3 and SMTP).

The firewall addresses required are:

- AccountingLocal - all traffic from the internal accounting network
- AccountingVlnk - all traffic from the VDOM link between accounting and management VDOMs
- SalesLocal - all traffic from the internal sales network
- SalesVlnk - all traffic from the VDOM link between sales and management VDOM.

Note: The limited number of services ensures security between departments. The list of services can be expanded in the future if needed.

The following six firewall policies are required.

- AccountingLocal to Internet
- Internet to AccountingLocal
- SalesLocal to Internet
- Internet to SalesLocal
- SalesLocal to AccountingLocal
- AccountingLocal to SalesLocal

This section includes the following topics:

Configuring firewall service groups

Service groups are an easy way to manage multiple services, especially if the same services are used on different networks.

The two service groups used here are intended for normal office traffic to the Internet, and for restricted traffic between departments. In both cases network traffic will be limited to the services listed to prevent any potential security risks or bandwidth-robbing applications.

These service groups can be changed as needed to either include additional valid services that are being used on the network, or to exclude services that are not required. Also, custom services can be created as needed for applications that are not listed. For more information on firewall service groups, see the firewall chapter of the *FortiGate Administration Guide*.

To configure two firewall service groups - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.

2 Select *VDOM* > *Accounting* > *Enter*.

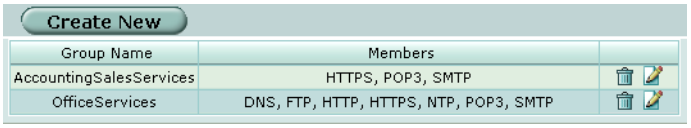
3 Select *Firewall* > *Service* > *Group* > *Create New*, enter the following information, and select *OK*.

Group Name	OfficeServices
Members	HTTP, HTTPS, SSL, FTP, DNS, NTP, POP3, PING, SMTP

4 Select *Create New*, enter the following information, and select *OK*.

Group Name	AccountingSalesServices
Members	HTTPS, POP3, PING, SMTP

Figure 55: AccoutingSalesServices and OfficeServices firewall service groups



To configure two firewall service groups - CLI

```
config vdom
edit Accounting
  config firewall service group
    edit OfficeServices
      set member HTTP HTTPS SSL FTP DNS NTP POP3 PING SMTP
    next
    edit AccountingSalesServices
      set member HTTPS POP3 PING SMTP
    next
  end
end
```

Configuring firewall settings for the Accounting VDOM

This configuration includes two firewall addresses and two firewall policies for the Accounting VDOM - one for the internal network, and one for the VDOM link with the management VDOM.

For added security, all traffic allowed will be scanned. Only valid office traffic will be allowed using the service group OfficeServices. The FortiClient application must be used to ensure additional protection for the sensitive accounting information.

All sales and accounting computers have the FortiClient application installed, so the firewall policies check that FortiClient is installed and that antivirus scanning is enabled.

Note the spelling of “AccountVlnk” which is due to the eleven character limit on VDOM link names.

To configure firewall addresses - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.

2 Select *VDOM* > *Accounting* > *Enter*.

3 Select *Firewall* > *Addresses* > *Create New*, enter the following information, and select *OK*.

Address Name	AccountingLocal
Type	Subnet/ IP Range
Subnet / IP Range	172.100.0.0
Interface	port1

4 Select *Firewall* > *Addresses* > *Create New*, enter the following information, and select *OK*.

Address Name	AccountManagement
Type	Subnet/ IP Range
Subnet / IP Range	10.0.1.0
Interface	AccountVlnk

To configure firewall addresses - CLI

```
config vdom
edit Accounting
  config firewall address
  edit AccountingLocal
    set type iprange
    set subnet 172.100.0.0
    set associated-interface port1
  next
  edit AccountManagement
    set type iprange
    set subnet 10.0.1.0
    set associated-interface AccountVlnk
  next
  end
end
```

To configure the firewall policies from AccountingLocal to the Internet - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *VDOM* > *Accounting* > *Enter*.
3. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	port1
Source Address	AccountingLocal
Destination Interface/Zone	AccountVlnk
Destination Address	AccountManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	enabled
Redirect Non-conforming Clients to Download Portal	enabled

4. Select << *Global*.
5. Select *VDOM* > *root* > *Enter*.
6. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	AccountVlnk
Source Address	AccountManagement
Destination Interface/Zone	external
Destination Address	all
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled

To configure the firewall policies from AccountingLocal to Internet - CLI

```
config vdom
edit Accounting
  config firewall policy
  edit 1
    set srcintf port1
    set srcaddr AccountingLocal
    set dstintf AccountVlnk
    set dstaddr AccountManagement
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
    set endpoint-redir-portal enable
  next
end
end
config vdom
edit root
  config firewall policy
  edit 2
    set srcintf AccountVlnk
    set srcaddr AccountManagement
    set dstintf external
    set dstaddr all
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
  next
  end
end
```

To configure the firewall policies from Internet to AccountingLocal - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *VDOM* > *root* > *Enter*.
3. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	external
Source Address	all
Destination Interface/Zone	AccountVlnk
Destination Address	AccountManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled

4. Select << *Global*.
5. Select *VDOM* > *Accounting* > *Enter*.
6. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	AccountVlnk
Source Address	AccountManagement
Destination Interface/Zone	port1
Destination Address	AccountingLocal
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

To configure the firewall policies from Internet to AccountingLocal - CLI

```
config vdom
edit root
  config firewall policy
  edit 3
    set srcintf external
    set srcaddr all
    set dstintf AccountVlnk
    set dstaddr AccountManagement
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
  next
end
end
config vdom
edit Accounting
  config firewall policy
  edit 4
    set srcintf AccountVlnk
    set srcaddr AccountManagement
    set dstintf port1
    set dstaddr AccountingLocal
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
    set endpoint-redir-portal enable
  next
  end
end
```

Configuring firewall settings for the Sales VDOM

Like the Accounting firewall settings, this configuration includes two firewall addresses and two firewall policies for the sales VDOM: one for the internal network, and one for the VDOM link with the management VDOM.

When entering the CLI commands, the number of the firewall policies must be high enough to be a new policy. Depending on the number of firewall policies on your FortiGate unit, this may require starting at a higher number than the 6 required for the default configuration. This number is added automatically when you configure firewall policies using the web manager interface.

The FortiClient application must be used on Sales network computers to ensure additional protection for the sensitive information and for protection against spam.

To configure firewall addresses - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.

2 Select *VDOM* > *Sales* > *Enter*.

3 Select *Firewall* > *Addresses* > *Create New,* enter the following information, and select *OK*.

Address Name	SalesLocal
Type	Subnet / IP Range
Subnet / IP Range	172.100.0.0
Interface	port2

4 Select *Firewall* > *Addresses* > *Create New*, enter the following information, and select OK.

Address Name	SalesManagement
Type	Subnet / IP Range
Subnet / IP Range	10.0.1.0
Interface	SalesVlnk

To configure the firewall addresses - CLI

```
config vdom
  edit Sales
    config fireall address
    edit SalesLocal
      set type iprange
      set subnet 172.100.0.0
      set associated-interface port2
    next
    edit SalesManagement
      set type iprange
      set subnet 10.0.1.0
      set associated-interface SalesVlnk
    next
  end
```

To configure the firewall policies from SalesLocal to the Internet - web-based manager

1 If <<*Global* appears in the left menu, select it to enter global configuration.

2 Select *VDOM* > *Sales* > *Enter*.

3 Select *Firewall* > *Policy* > *Create New*, enter the following information, and select OK.

Source Interface/Zone	port2
Source Address	SalesLocal
Destination Interface/Zone	SalesVlnk
Destination Address	SalesManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

4 Select << *Global*.

5 Select *VDOM* > *root* > *Enter*.

6 Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	SalesVlnk
Source Address	SalesManagement
Destination Interface/Zone	external
Destination Address	all
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled

To configure the firewall policies from SalesLocal to the Internet - CLI

```
config vdom
  edit root
  config firewall policy
  edit 6
    set srcintf port2
    set srcaddr SalesLocal
    set dstintf SalesVlnk
    set dstaddr SalesManagement
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
    set endpoint-redir-portal enable
  next
  end
  end

  config vdom
  edit Sales
  config firewall policy
  edit 7
    set srcintf SalesVlnk
    set srcaddr SalesManagement
    set dstintf external
    set dstaddr all
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
  next
  end
end
```

To configure the firewall policies from the Internet to SalesLocal - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *VDOM* > *root* > *Enter*.
3. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	external
Source Address	all
Destination Interface/Zone	SalesVlnk
Destination Address	SalesManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled

4. Select << *Global*.
5. Select *VDOM* > *Sales* > *Enter*.
6. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	SalesVlnk
Source Address	SalesManagement
Destination Interface/Zone	port2
Destination Address	SalesLocal
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

To configure the firewall policies from the Internet to SalesLocal - CLI

```
config vdom
  edit root
  config firewall policy
  edit 8
    set srcintf external
    set srcaddr all
    set dstintf SalesVlnk
    set dstaddr SalesManagement
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
    set endpoint-redir-portal enable
  next
  end
  end

  config vdom
  edit Sales
  config firewall policy
  edit 9
    set srcintf SalesVlnk
    set srcaddr SalesManagement
    set dstintf port2
    set dstaddr SalesLocal
    set schedule always
    set service OfficeServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
    set endpoint-redir-portal enable
  next
  end
end
```

Configuring firewall settings between the Accounting and Sales VDOMs

Firewall policies are required for any communication between each internal network and the Internet. Policies are also required for the two internal networks to communicate with each other through the management VDOM.

The more limited AccountingSalesServices group of services will be used between Sales and Accounting to ensure the traffic is necessary business traffic only. These policies will result in a partially meshed VDOM configuration. The FortiClient application must be used to ensure additional protection for the sensitive accounting information.

Two firewall policies are required to allow traffic in both directions between Sales and Accounting.

To configure the firewall policy between Sales and Accounting on the management VDOM - web-based manager

1. If <<*Global* appears in the left menu, select it to enter global configuration.
2. Select *VDOM* > *root* > *Enter*.
3. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	SalesVlnk
Source Address	SalesManagement
Destination Interface/Zone	AccountVlnk
Destination Address	AccountingManagement
Schedule	always
Service	AccountingSalesServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

4. Select *Firewall* > *Policy* > *Create New*, enter the following information, and select *OK*.

Source Interface/Zone	AccountVlnk
Source Address	AccountingManagement
Destination Interface/Zone	SalesVlnk
Destination Address	SalesManagement
Schedule	always
Service	AccountingSalesServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled
Enable Endpoint Control Check	disabled
Redirect Non-conforming Clients to Download Portal	enabled

To configure the firewall policy between Sales and Accounting on the management VDOM - CLI

```
config vdom
edit root
  config system firewall policy
  edit 9
    set srcintf SalesVlnk
    set srcaddr SalesManagement
    set dstintf AccountVlnk
    set dstaddr AccountManagement
    set schedule always
    set service AccountingSalesServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
    set endpoint-redir-portal enable
  next
  edit 10
    set srcintf AccountVlnk
    set srcaddr AccountManagement
    set dstintf SalesVlnk
    set dstaddr SalesManagement
    set schedule always
    set service AccountingSalesServices
    set action accept
    set profile-status enable
    set profile scan
    set logtraffic enable
    set endpoint-check enable
    set endpoint-redir-portal enable
  next
  end
end
```

Testing the configuration

Once the inter-VDOM routing has been configured, tests must be conducted to confirm proper operation. If there are any problems, use the troubleshooting tips to resolve them.

This section includes the following topics:

Testing connectivity

Testing connectivity ensures that physical networking connections as well as FortiGate unit interface configurations, including firewall policies, are properly configured.

The easiest way to test connectivity is to use the `ping` and `traceroute` commands to confirm the connectivity of different routes on the network. Include testing:

- from AccountingLocal to Internet
- from Internet to AccountingLocal
- from SalesLocal to Internet
- from Internet to SalesLocal
- from AccountingLocal to SalesLocal.

When using the commands on a Windows computer, go to a command line prompt and enter either `ping <IP address>` or `tracert <IP address>`.

When using the commands on a FortiGate unit, go to the CLI and enter either `exec ping <IP address>` or `exec traceroute <IP address>`.

Troubleshooting Tips

When there are problems with connectivity, the following troubleshooting tips will help resolve the issues.

- If a multiple hop test, such as traceroute, is not successful then reduce it to a single hop to simplify the test. Test each link of the path to see which hop is down. If all hops are up, check the FortiGate unit policies to ensure they allow basic traffic to flow as expected.
- If ping does not work, confirm that the FortiGate unit interfaces have Ping enabled and also ensure Ping is enabled in the firewall policies. Otherwise the Ping traffic will be blocked.
- If one protocol does not work but others do work, check the FortiGate unit firewall policies for that one protocol to ensure it is allowed.
- If there are unexplained connectivity problems, check the local computer to ensure it does not have a software firewall running that may be blocking traffic. MS Windows computers have a firewall running by default that can cause problems.

Using VLANs and VDOMs in Transparent mode

In Transparent mode, the FortiGate unit behaves like a layer-2 bridge but can still provide services such as antivirus scanning, web filtering, spam filtering and intrusion protection to traffic. There are some limitations in Transparent mode in that you cannot use SSL VPN, PPTP/L2TP VPN, DHCP server, or easily perform NAT on traffic. The limits in Transparent mode apply to IEEE 802.1Q VLAN trunks passing through the unit.

VDOMs can each be configured to operate either in Transparent or NAT/Route operation mode, with each VDOM behaving like a separate FortiGate unit operating in the respective mode. VLANs configured on a VDOM in Transparent mode are the same as VLANs configured on the FortiGate unit when VDOMs are disabled.

This chapter includes the following sections:

Before you begin

Before you begin using this chapter, take a moment to note the following:

- The information in this chapter applies to all FortiGate units. All FortiGate models except the FortiGate-30B model support VDOMs, and all FortiGate models support VLANs.
- By default, your FortiGate unit supports a maximum of 10 VDOMs in any combination of NAT/Route and Transparent operating modes. For FortiGate models numbered 3000 and higher, you can purchase a license key to increase the maximum number to 25, 50, 100 or 250 VDOMs.
- This chapter uses a FortiGate-800 for examples and procedures. The interface names on some models will vary. For example, some models do not have interfaces labeled external or internal.
- A super_admin administrator account is assumed for the procedures and examples; however, if you are an administrator restricted to a VDOM, you may be able to perform some procedures. For more information, see “Administration of VDOMs” on page 20.

VLANs and Transparent mode

You can insert the FortiGate unit operating in Transparent mode into the VLAN trunk without making changes to your network. In a typical configuration, the FortiGate unit internal interface accepts VLAN packets on a VLAN trunk from a VLAN switch or router connected to internal network VLANs. The FortiGate unit external interface forwards VLAN-tagged packets through another VLAN trunk to an external VLAN switch or router and on to external networks such as the Internet. You can configure the unit to apply different policies for traffic on each VLAN in the trunk.

To pass VLAN traffic through the FortiGate unit, you add two VLAN subinterfaces with the same VLAN ID, one to the internal interface and the other to the external interface. You then create a firewall policy to permit packets to flow from the internal VLAN interface to the external VLAN interface. If required, you create another firewall policy to permit packets to flow from the external VLAN interface to the internal VLAN interface. Typically in Transparent mode, you do not permit packets to move between different VLANs. Network protection features, such as spam filtering, web filtering and anti-virus scanning, are applied through the protection profile specified in each firewall policy, enabling very detailed control over traffic.

When the FortiGate unit receives a VLAN-tagged packet at a physical interface, it directs the packet to the VLAN subinterface with the matching VLAN ID. The VLAN tag is removed from the packet, and the FortiGate unit then applies firewall policies using the same method it uses for non-VLAN packets. If the packet exits the FortiGate unit through a VLAN subinterface, the VLAN ID for that subinterface is added to the packet and the packet is sent to the corresponding physical interface. For a configuration example, see “Example of VLANs in Transparent mode” on page 161.

VDOMs and VLANs and Transparent mode

When VDOMs are enabled, you associate VLAN subinterfaces with one of the VDOMs. By default, the FortiGate unit’s configuration includes one VDOM, named “root”. VDOMs are not enabled by default, and you can add as many VLAN subinterfaces as you require to the root VDOM. The only limit is the number of interfaces permitted per VDOM.

A VDOM, such as root, can have a maximum of 255 interfaces in Network Address Translation (NAT) mode or Transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. To have more than a total of 255 interfaces configured, you need multiple VDOMs with multiple interfaces on each.

You can add more VDOMs to separate groups of VLAN subinterfaces. When using a FortiGate unit to serve multiple organizations, this configuration simplifies administration because you see only the firewall policies and settings for the VDOM you are configuring. For information on adding and configuring virtual domains, see “Getting started with VDOMs” on page 60.

One essential application of VDOMs is to prevent problems caused when a FortiGate unit is connected to a layer-2 switch that has a global MAC table. FortiGate units normally forward ARP requests to all interfaces, including VLAN subinterfaces. It is then possible for the switch to receive duplicate ARP packets on different VLANs. Some layer-2 switches reset when this happens. As ARP requests are only forwarded to interfaces in the same VDOM, you can solve this problem by creating a VDOM for each VLAN. For a configuration example, see “Example of VLANs and VDOMs in Transparent mode (advanced)” on page 168.

Configuring the FortiGate unit in Transparent mode

There are two essential steps to configure your FortiGate unit to work with VLANs in Transparent mode:

- Adding VLAN subinterfaces
- Creating firewall policies.

You can also configure the protection profiles that manage antivirus scanning, web filtering and spam filtering. Protection profiles are covered in the *FortiGate Administration Guide*.

In Transparent mode, you can access the FortiGate web-based manager by connecting to an interface configured for administrative access and using HTTPS to access the management IP address. On the FortiGate-800, the model used for examples in this guide, administrative access is enabled by default on the internal interface and the default management IP address is 10.10.10.1.

For the procedures in this section, it is assumed that you have not enabled VDOM configuration. If VDOM configuration is enabled, you may need to navigate to the global or VDOM configuration before following each procedure. For more information on VDOM navigation, see "Global and VDOM settings" on page 21.

Adding VLAN subinterfaces

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch. The VLAN ID can be any number between 1 and 4094, with 0 being used only for high priority frames and 4095 being reserved. You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

For this example, we are creating a VLAN called internal_v225 on the internal interface, with a VLAN ID of 225. Administrative access is enabled for HTTPS and SSH. VDOMs are not enabled.

To add VLAN subinterfaces in Transparent mode - web-based manager

1 Go to *System* > *Network* > *Interface*.

2 Select *Create New*.

3 Enter the following information and select *OK*.

Name	internal_v225
Type	VLAN
Interface	internal
VLAN ID	225
Ping Server	not enabled
Administrative Access	Enable HTTPS, and SSH. These are very secure access methods.
Description	VLAN 225 on internal interface

The FortiGate unit adds the new subinterface to the interface that you selected.

Repeat steps 2 and 3 to add additional VLANs. You will need to change the *VLAN ID*, *Name*, and possibly *Interface* when adding additional VLANs.

To add VLAN subinterfaces in Transparent mode - CLI

```
config system interface
  edit internal_v225
    set interface internal
    set vlanid 225
    set allowaccess HTTPS SSH
    set description “VLAN 225 on internal interface”
    set vdom root
next
end
```

Creating firewall policies

Firewall policies permit communication between the FortiGate unit's network interfaces based on source and destination IP addresses. Optionally, you can limit communication to particular times and services.

In Transparent mode, the FortiGate unit performs antivirus and antispam scanning on each VLAN's packets as they pass through the unit. You need firewall policies to permit packets to pass from the VLAN interface where they enter the unit to the VLAN interface where they exit the unit. If there are no firewall policies configured, no packets will be allowed to pass from one interface to another.

To add firewall policies for VLAN subinterfaces - web based manager

1. Go to *Firewall* > *Address*.
2. Select *Create New* to add firewall addresses that match the source and destination IP addresses of VLAN packets.
3. Go to *Firewall* > *Policy*.
4. Select *Create New*.
5. From the Source Interface/Zone list, select the VLAN interface where packets enter the unit.
6. From the Destination Interface/Zone list, select the VLAN interface where packets exit the unit.
7. Select the Source and Destination Address names that you added in step 2.
8. Select *Protection Profile*, and select the profile from the list.
9. Configure other settings as required.
10. Select *OK*.

To add firewall policies for VLAN subinterfaces - CLI

```
config firewall address
edit incoming_VLAN_address
  set associated-interface <incoming_VLAN_interface>
  set type ipmask
  set subnet <IPv4_address_mask)
next
edit outgoing_VLAN_address
  set associated-interface <outgoing_VLAN_interface>
  set type ipmask
  set subnet <IPv4_address_mask>
next
end
```

```
config firewall policy
edit <unused_policy_number>
   set srcintf <VLAN_number>
   set srcaddr incoming_VLAN_address
   set destintf <VLAN_number>
   set destaddr outgoing_VLAN_address
   set service <protocol_to_allow_on VLAN>
   set action ACCEPT
   set profile-status enable
   set profile <selected_profile>
next
end
end
```

Example of VLANs in Transparent mode

In this example, the FortiGate unit is operating in Transparent mode and is configured with two VLANs—one with an ID of 100 and the other with ID 200. The internal and external physical interfaces each have two VLAN subinterfaces, one for VLAN_100 and one for VLAN_200.

This section includes the following topics:

Network topology and assumptions

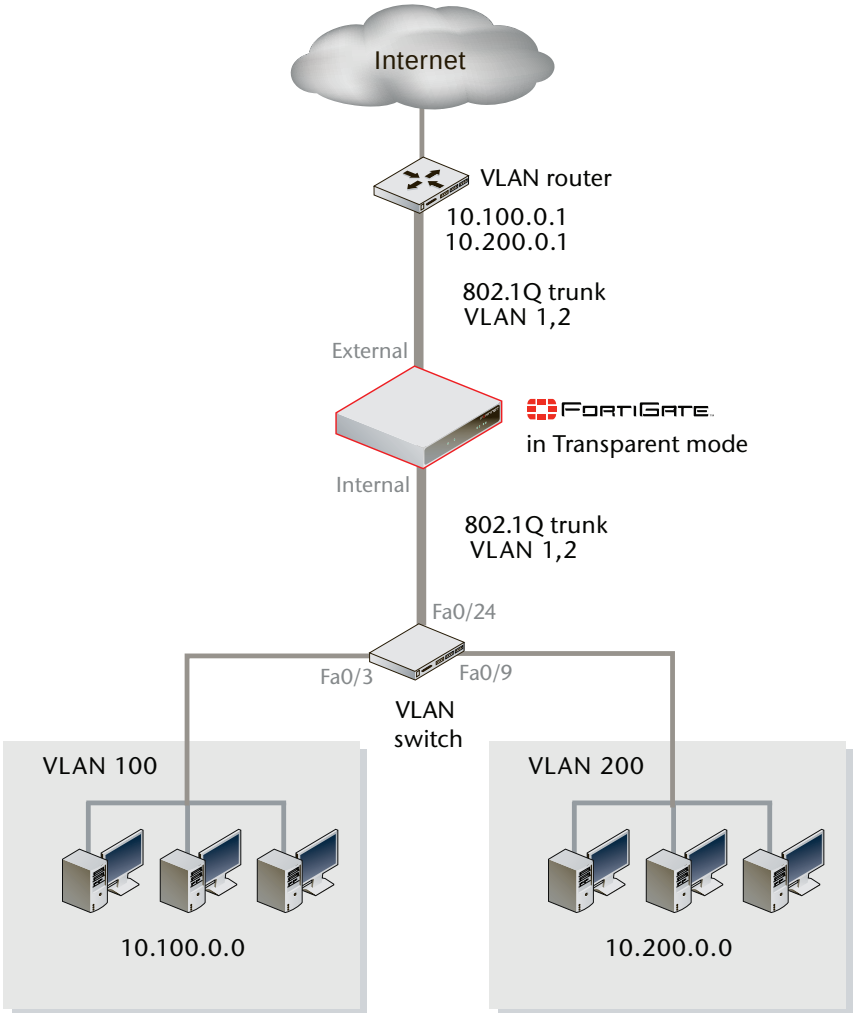
The network topology for this example is straightforward, with two internal networks entering the FortiGate unit on one physical interface, and leaving on another physical interface.

The IP range for the internal VLAN_100 network is 10.100.0.0/255.255.0.0, and for the internal VLAN_200 network is 10.200.0.0/255.255.0.0.

The internal networks are connected to a Cisco 2950 VLAN switch, which combines traffic from the two VLANs onto one physical interface—the FortiGate unit internal interface. The VLAN traffic leaves the FortiGate unit on the external network interface, goes on to the VLAN switch, and on to the Internet. When the FortiGate units receives a tagged packet, it directs it from the incoming VLAN subinterface to the outgoing VLAN subinterface for that VLAN.

This section describes how to configure a FortiGate-800 unit, Cisco switch, and Cisco router in the network topology shown in Figure 56.

Figure 56: VLAN Transparent network topology



General configuration steps

The following steps summarize the configuration for this example. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1 Configuring the FortiGate unit includes
   - Adding VLAN subinterfaces
   - Adding the firewall policies
2 Configuring the Cisco switch and router
3 Testing the configuration

Configuring the FortiGate unit

The FortiGate unit must be configured with the VLAN subinterfaces and the proper firewall policies to enable traffic to flow through the FortiGate unit.

This section includes the following topics:

- Adding VLAN subinterfaces
- Adding the firewall policies

Adding VLAN subinterfaces

For each VLAN, you need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager

1 Go to *System* > *Network* > *Interface*.

2 Select *Create New*.

3 Enter the following information and select *OK*:

Name	VLAN_100_int
Interface	internal
VLAN ID	100

4 Select *Create New*.

5 Enter the following information and select *OK*:

Name	VLAN_100_ext
Interface	external
VLAN ID	100

6 Select *Create New*.

7 Enter the following information and select *OK*:

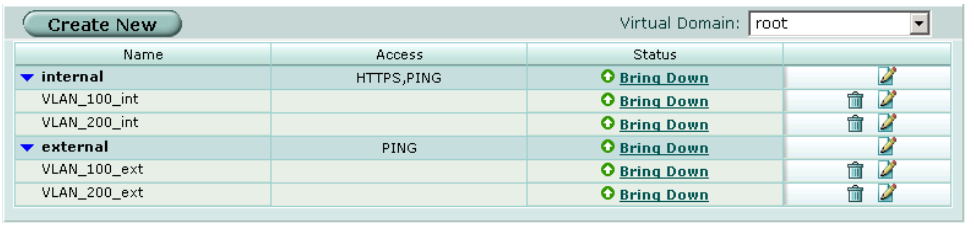
Name	VLAN_200_int
Interface	internal
VLAN ID	200

8 Select *Create New*.

9 Enter the following information and select *OK*:

Name	VLAN_200_ext
Interface	external
VLAN ID	200

Figure 57: VLAN_100 and VLAN_200 internal and external subinterfaces



To add VLAN subinterfaces - CLI

```
config system interface
  edit VLAN_100_int
    set status down
    set type vlan
    set interface internal
    set vlanid 100
  next
  edit VLAN_100_ext
    set status down
    set type vlan
    set interface external
    set vlanid 100
  next
  edit VLAN_200_int
    set status down
    set type vlan
    set interface internal
    set vlanid 200
  next
  edit VLAN_200_ext
    set status down
    set type vlan
    set interface external
    set vlanid 200
  end
```

Adding the firewall policies

Firewall policies allow packets to travel between the VLAN_100_int interface and the VLAN_100_ext interface. Two policies are required—one for each direction of traffic. The same is required between the VLAN_200_int interface and the VLAN_200_ext interface, for a total of four required firewall policies.

To add the firewall policies - web-based manager

1. Go to *Firewall* > *Policy.*
2. Select *Create New*.
3. Enter the following information and select *OK*:

Source Interface/Zone	VLAN_100_int
Source Address	all
Destination Interface/Zone	VLAN_100_ext
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

4. Select *Create New*.

5 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_100_ext
Source Address	all
Destination Interface/Zone	VLAN_100_int
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

6 Go to *Firewall > Policy*.

7 Select *Create New*.

8 Enter the following information and select *OK*:

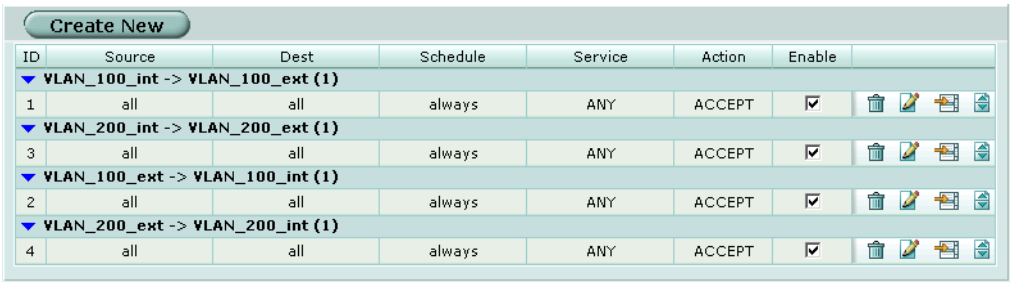
Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

9 Select Create New.

10 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200_ext
Source Address	all
Destination Interface/Zone	VLAN_200_int
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

Figure 58: Firewall policies for VLAN_100_and VLAN_200 internal and external interfaces



To add the firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_100_int
    set srcaddr all
    set dstintf VLAN_100_ext
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
  next
  edit 2
    set srcintf VLAN_100_ext
    set srcaddr all
    set dstintf VLAN_100_int
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
  next
  edit 3
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
  next
  edit 4
    set srcintf VLAN_200_ext
    set srcaddr all
    set dstintf VLAN_200_int
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
  end
```

Configuring the Cisco switch and router

This example includes configuration for the Cisco Catalyst 2900 ethernet switch, and for the Cisco Multiservice 2620 ethernet router. If you have access to a different VLAN enabled switch or VLAN router you can use them instead, however their configuration is not included in this document.

This section includes the following topics:

Configuring the Cisco switch

On the VLAN switch, you need to define VLAN_100 and VLAN_200 in the VLAN database and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

Add this file to the Cisco switch:

```
interface FastEthernet0/3
 switchport access vlan 100
!
interface FastEthernet0/9
 switchport access vlan 200
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 100
Port 0/9	VLAN ID 200
Port 0/24	802.1Q trunk

Configuring the Cisco router

You need to add a configuration file to the Cisco Multiservice 2620 ethernet router. The file defines the VLAN subinterfaces and the 802.1Q trunk interface on the router. The 802.1Q trunk is the physical interface on the router.

The IP address for each VLAN on the router is the gateway for that VLAN. For example, all devices on the internal VLAN_100 network will have 10.100.0.1 as their gateway.

Add this file to the Cisco router:

```
!
interface FastEthernet0/0
!
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 10.100.0.1 255.255.255.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 200
 ip address 10.200.0.1 255.255.255.0
!
```

The router has the following configuration:

Port 0/0.1	VLAN ID 100
Port 0/0.2	VLAN ID 200
Port 0/0	802.1Q trunk

Testing the configuration

Use diagnostic network commands such as traceroute (`tracert`) and ping to test traffic routed through the network.

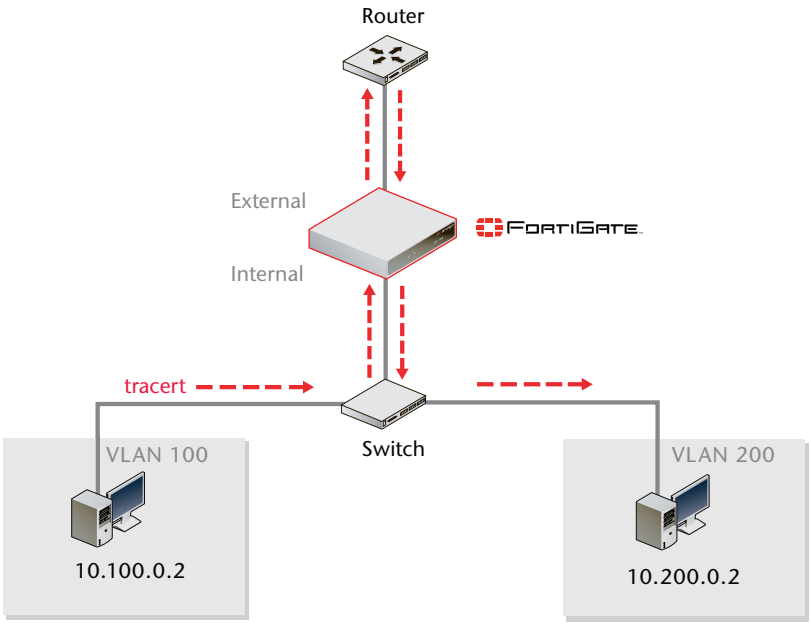
Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between the two internal networks. The route target is a host on VLAN_200. The Windows traceroute command `tracert` is used.

From VLAN_100, access a Windows command prompt and enter this command:

```
C:\>tracert 10.1.2.2
Tracing route to 10.1.2.2 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.1.1.1
  2   <10 ms   <10 ms   <10 ms  10.1.2.2
Trace complete.
```

Figure 59: Example traceroute from VLAN_100 to VLAN_200



Example of VLANs and VDOMs in Transparent mode (advanced)

In this example, the FortiGate unit provides network protection to three organizations (ABC Inc., DEF Inc., and XYZ Inc.) that have quite different policies for incoming and outgoing traffic. This requires different firewall policies and protection profiles for each company. Although you do not need to use VDOMs for this configuration, by doing so you can manage the profiles and policies more easily by configuring them within one VDOM at a time.

This example includes the following sections:

- Network topology and assumptions
- General configuration steps
- Configuring common items
- Creating virtual domains

- Configuring the ABCdomain
- Configuring the DEFdomain
- Configuring the XYZdomain
- Configuring the VLAN switch and router
- Testing the configuration

Network topology and assumptions

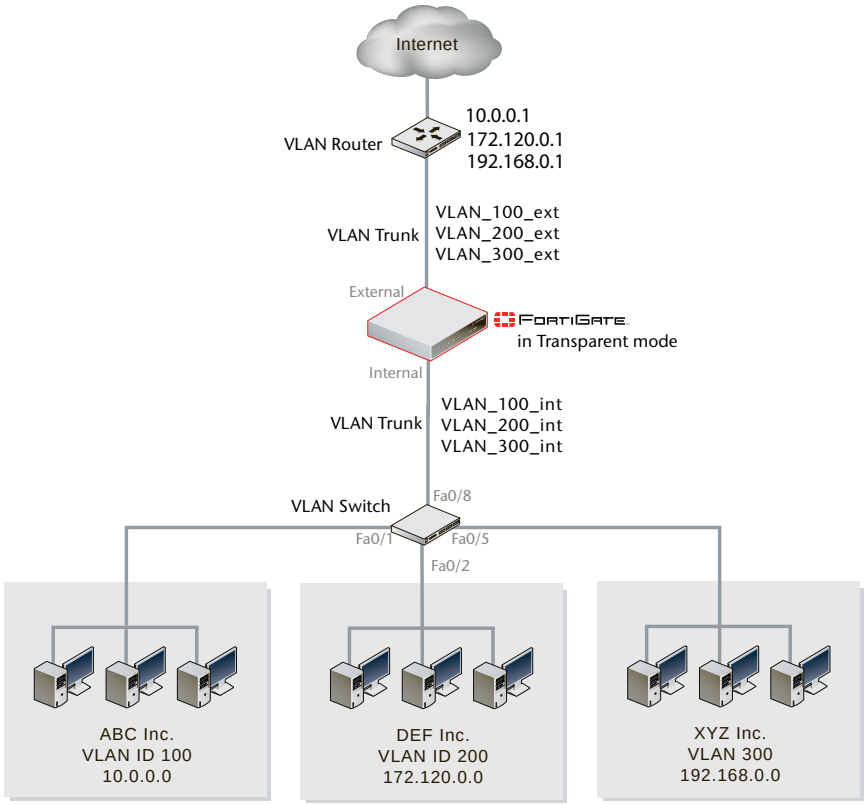
Each organization's internal network has a different range of IP addresses assigned to it:

- 10.0.0.0/255.255.0.0 for ABC Inc.
- 172.120.0.0/255.255.0.0 for DEF Inc.
- 192.168.0.0/255.255.0.0 for XYZ Inc.

For the procedures in this section, it is assumed that you have enabled VDOM configuration on your FortiGate unit. For more information, see "Getting started with VDOMs" on page 60.

The VDOM names are similar to the company names for easy recognition. The root VDOM cannot be renamed and is not used in this example.

Figure 60: VLAN and VDOM Transparent example network topology



General configuration steps

The following steps summarize the configuration for this example. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configuring common items
2. Creating virtual domains
3. Configuring the ABCdomain
4. Configuring the DEFdomain
5. Configuring the XYZdomain
6. Configuring the VLAN switch and router
7. Testing the configuration

Configuring common items

Some components of the protection profiles that you create will be common to all VDOMs. You have to configure them separately for each VDOM, but the steps for each are the same.

This section includes the following topics:

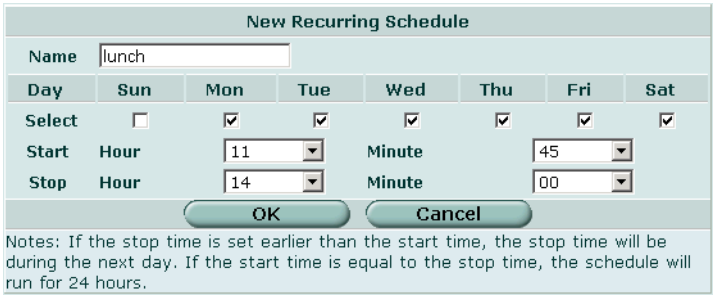
- Creating schedules
- Creating protection profiles

Creating schedules

All organizations have the same lunch schedule, to make things easier for this example. Lunch will be on Monday to Friday from 11:45am to 2:00pm (14:00).

To create a recurring schedule for lunchtime - web-based manager

1. Go to *Firewall* > *Schedule* > *Recurring*.
2. Select *Create New*.
3. Enter Lunch as the name for the schedule.
4. Select *Mon*, *Tues*, *Wed*, *Thu*, and *Fri*.
5. Set the *Start* time as 11:45 and set the *Stop* time as 14:00.



6. Select *OK*.

To create a recurring schedule for lunchtime - CLI

```
config firewall schedule recurring
  edit Lunch
    set day monday tuesday wednesday thursday friday
    set start 11:45
    set end 14:00
  end
```

Creating protection profiles

The FortiGate-800 provides pre-configured protection profiles: strict, scan, web and unfiltered. This example also requires custom protection profiles to take advantage of the FortiGate content blocking features. Protection profiles are not global, so you can create as many as you need to cover the requirements of different organizations.

This example requires protection profiles in the VDOMs that use them as follows. The BusinessOnly profile is used during business hours to limit online activities to business-related only, and to block questionable or potentially liable or damaging activities. The Lunch profile relaxes some of the non-productive activity restrictions while still maintaining blocks on liable or potentially damaging activities.

For these profiles, we assume that all protocols will be on their standard ports, such as port 80 for http traffic. If the ports are changed, such as using port 8080 for http traffic, you will have to create custom services for protocols with non-standard ports, and assign them different names.

Profile name	Description	Used by	Time of Day
BusinessOnly	Antivirus, spam filtering, banned word list, IPS. Web category filtering designed to prevent non-business activity.	ABC Inc., DEF Inc.	All times except lunch
Relaxed (Lunch)	Antivirus, spam filtering, banned word list, IPS are the same as for BusinessOnly. Relaxed controls on web category filtering to allow some general-interest web browsing during lunch hour.	ABC Inc., DEF Inc.	11:45 to 14:00 Monday to Friday

To create the BusinessOnly protection profile - web-based manager

Repeat the following procedure for both ABC Inc. and DEF Inc. VDOMs.

1. Go to *Firewall* > *Protection Profile*.
2. Select Create New.
3. Enter `BusinessOnly` as the *Profile Name*.
4. Select *Anti-Virus* and enable *Virus Scan* for all protocols listed.
5. Select *IPS*, enable *IPS Sensor,* and select *protect_client* from the IPS sensor list.
6. Select *Web Filtering.*
7. For *Enable FortiGuard Web Filtering,* select HTTP.

8 Configure categories as follows:

Potentially Liable (group)	Block
Controversial (group)	Block
Potentially Non-productive (group)	Block
Potentially Bandwidth Consuming (group)	Block
Potentially Security Violating (group)	Block
General Interest (group)	Block
Business Oriented	Allow, Log
Others	Block
Unrated	Allow, Log

9 Select *Spam Filtering*, and for all protocols (IMAP, POP3, SMPTP, IMAPS, POP3S, and SMTPS), select

- IP address check
- Spam submission
- IP address BWL check
- Return e-mail DNS check
- Banned word check

10 For *Spam Action*, select *Discard* for SMTP and SMTPS, and *Tagged* for all others.

11 Select *OK*.

To create the BusinessOnly protection profile - CLI

```
config firewall profile
  edit BusinessOnly
    config log
      set log-web-ftgd-err enable
    end
    set httpsoversizelimit 0
    set ftp scan splice
    set http scan fortiguard-wf
    unset https
    set imap scan fragmail spamfssubmit
    set imaps fragmail spamfssubmit
    set pop3 scan fragmail spamfssubmit
    set pop3s fragmail spamfssubmit
    set smtp scan fragmail spamfssubmit splice
    set smtps fragmail spamfssubmit
    set pop3-spamtagtype subject
    set imap-spamtagtype subject
    set pop3s-spamtagtype subject
    set imaps-spamtagtype subject
    unset nntp
    set ips-sensor-status enable
    set ips-sensor "protect_client"
    unset im
    set ftgd-wf-options strict-blocking
    set ftgd-wf-https-options strict-blocking
    set ftgd-wf-allow g07 g21 g22 c01 c02 c03 c04 c05 c06
    set ftgd-wf-deny g01 g02 g03 g04 g05 g06 g08
    set ftgd-wf-log g07 g21
  next
end
```

To create the Relaxed protection profile - web-based manager

1. Go to *Firewall* > *Protection Profile*.
2. Select *Create New*.
3. Enter `Relaxed` as the *Profile Name*.
4. Select *Anti-Virus* and select the following options.

Virus Scan	Enable for all protocols
Pass Fragmented Emails	Enable for all email protocols

5. Select *IPS*, enable *IPS Sensor,* and select *protect_client* from the IPS sensor list.
6. Select *Web Filtering.*
7. For *Enable FortiGuard Web Filtering,* select HTTP.

8 Configure categories as follows:

Potentially Liable (group)	Block
Controversial (group)	Block
Potentially Non-productive (group)	Allow, Log
Potentially Bandwidth Consuming (group)	Allow, Log
Potentially Security Violating (group)	Block
General Interest (group)	Allow, Log
Business Oriented	Allow
Others	Allow
Unrated	Allow, Block

9 Select *Spam Filtering* and enable the following options for all protocols.

IP Address BWL check	Check the IP address against Black Lists and White lists
Banned word check	Check content for known banned words
E-mail address BWL check	Check the email address against Black Lists and White Lists
Return e-mail DNS check	Check DNS entry for the return address of the e-mail to ensure it exists

10 For *Spam Action*, select *Discard* for SMTP and SMTPS, and ensure *Tagged* is set for all other protocols.

11 Select *OK*.

To create the Relaxed protection profile - CLI

```
config firewall profile
  edit Relaxed
    set httpsoversizelimit 0
    config log
      set log-web-ftgd-err enable
    end
    set ftp scan splice
    set http scan fortiguard-wf
    unset https
    set imap scan fragmail spamfssubmit
    set imaps scan fragmail spamfssubmit
    set pop3 scan fragmail spamfssubmit
    set pop3s scan fragmail spamfssubmit
    set smtp scan fragmail spamfssubmit splice
    set smtps scan fragmail spamfssubmit
    set pop3-spamtagtype subject
    set imap-spamtagtype subject
    set pop3s-spamtagtype subject
    set imaps-spamtagtype subject
    set nntp scan
    set ips-sensor-status enable
    set ips-sensor protect_client
    set im scan
    set ftgd-wf-options strict-blocking
    set ftgd-wf-https-options strict-blocking
    set ftgd-wf-allow g03 g04 g07 g08 g21 g22 c01 c02 c03 c04 c05
       c06
    set ftgd-wf-deny g01 g02 g05 g06
    set ftgd-wf-log g03 g04 g06 g21
  next
end
```

Creating virtual domains

The FortiGate-800 supports 10 virtual domains. Root is the default VDOM. It cannot be deleted or renamed. The root VDOM is not used in this example. New VDOMs are created for ABC Inc., DEF Inc. and XYZ Inc.

To create the virtual domains - web-based manager

1. With VDOMs enabled, select *System* > *VDOM*.
2. Select *Create New*.
3. Enter `ABCdomain` for Name, and select *OK*.
4. Select *Create New*.
5. Enter `DEFdomain` for Name, and select *OK*.
6. Select *Create New*.
7. Enter `XYZdomain` for Name, and select *OK*.

To create the virtual domains - CLI

```
config system vdom
  edit ABCdomain
  next
  edit DEFdomain
  next
  edit XYZdomain
  end
```

Configuring the ABCdomain

This section describes how to add VLAN subinterfaces and configure firewall policies for the ABCdomain VDOM.

This section includes the following topics:

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager

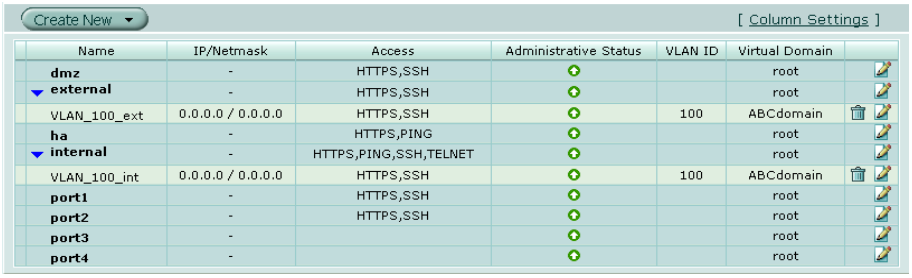
1. Go to *System* > *Network* > *Interface*.
2. Select *Create New*.
3. Enter the following information and select *OK*:

Name	VLAN_100_int
Interface	internal
VLAN ID	100
Virtual Domain	ABCdomain

4. Select *Create New*.
5. Enter the following information and select *OK*:

Name	VLAN_100_ext
Interface	external
VLAN ID	100
Virtual Domain	ABCdomain

Figure 61: VLAN_100 internal and external subinterfaces for ABCdomain



To add the VLAN subinterfaces - CLI

```
config system interface
  edit VLAN_100_int
    set interface internal
    set vlanid 100
    set vdom ABCdomain
  next
  edit VLAN_100_ext
    set interface external
    set vlanid 100
    set vdom ABCdomain
  end
```

Selecting the ABCdomain VDOM

Before you follow the rest of the procedure for configuring VLAN_100, you must ensure that the current domain is ABCdomain.

To select the ABCdomain VDOM - web-based manager

1. Go to *System* > *VDOM*.
2. Select *Enter* for the ABCdomain VDOM.

To select the ABCdomain VDOM - CLI

```
config vdom
  edit ABCdomain
```

Creating service groups

ABC Inc. does not want its employees to use online chat or gaming software. To simplify the creation of firewall policies for this purpose, you create a service group that contains all of the services you want to restrict because a firewall policy can manage only one service or one group. Without creating this group, you would need six separate firewall policies for each one.

To create a games and chat service group - web-based manager

1. Go to *Firewall* > *Service* > *Group*.
2. Select *Create New*.
3. Enter `games-chat` in the *Group Name* field.
4. For each of AOL, IRC, NetMeeting, QUAKE, SIP-MSNmessenger and TALK, select the service in the *Available Services* list and select the right arrow to add it to the *Members* list.
5. Select *OK*.

To create a games and chat service group - CLI

```
config firewall service group
  edit games-chat
    set member IRC NetMeeting QUAKE SIP-MSNmessenger AOL TALK
  end
```

Configuring ABCdomain firewall addresses

The “all” address is present by default in the root domain. In other domains, you must create it.

To configure ABCdomain firewall addresses - web-based manager

1. Go to *Firewall* > *Address*.
2. Select *Create New*.
3. Enter `new` in the *Address Name* field.
4. Type 0.0.0.0/0.0.0.0 in the *Subnet / IP Range* field.
5. Select *OK*.

To configure ABCdomain firewall addresses - CLI

```
config firewall address
  edit all
    set type ipmask
    set subnet 0.0.0.0 0.0.0.0
  end
```

Configuring ABCdomain firewall policies

Firewall policies allow packets to travel from the VLAN_100 interface to the external interface subject to the restrictions of the protection profile.

To configure ABCdomain firewall policies - web-based manager

1. Go to *Firewall* > *Policy*.
2. Select *Create New*.

3 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_100_int
Source Address	all
Destination Interface/Zone	VLAN_100_ext
Destination Address	all
Schedule	BusinessDay
Service	games-chat
Action	DENY

This policy prevents the use of network games or chat programs during business hours.

4 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_100_int
Source Address	all
Destination Interface/Zone	VLAN_100_ext
Destination Address	all
Schedule	Lunch
Service	HTTP
Action	ACCEPT
Protection Profile	Relaxed

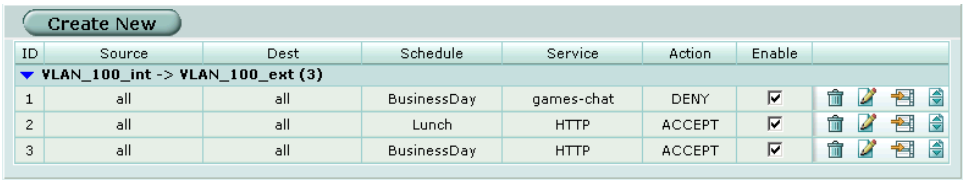
This policy relaxes the web category filtering during lunch hour.

5 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_100_int
Source Address	all
Destination Interface/Zone	VLAN_100_ext
Destination Address	all
Schedule	BusinessDay
Service	HTTP
Action	ACCEPT
Protection Profile	BusinessOnly

This policy provides rather strict web category filtering during business hours.

Figure 62: ABCdomain firewall policies



To configure ABCdomain firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_100_int
    set dstintf VLAN_100_ext
    set srcaddr all
    set dstaddr all
    set schedule BusinessDay
    set service games-chat
  next
  edit 2
    set srcintf VLAN_100_int
    set dstintf VLAN_100_ext
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule Lunch
    set service HTTP
    set profile_status enable
    set profile Relaxed
  next
  edit 3
    set srcintf VLAN_100_int
    set dstintf VLAN_100_ext
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule BusinessDay
    set service HTTP
    set profile_status enable
    set profile BusinessOnly
  end
```

Configuring the DEFdomain

This section describes how to add VLAN subinterfaces and configure firewall policies for the DEFdomain VDOM.

This section includes the following topics:

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager

1 Go to *System* > *Network* > *Interface*.

2 Select *Create New*.

3 Enter the following information and select *OK*:

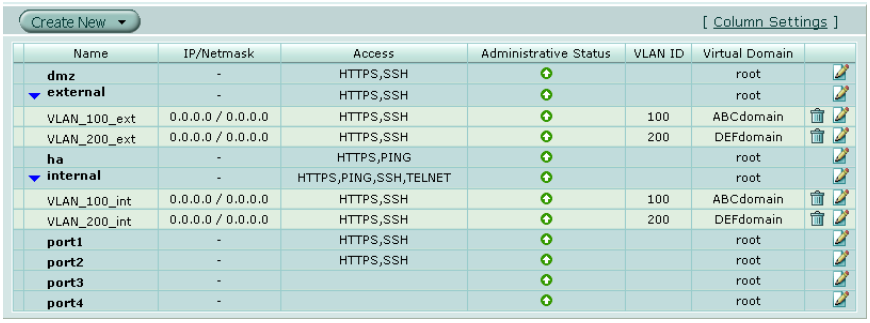
Name	VLAN_200_int
Interface	internal
VLAN ID	200
Virtual Domain	DEFdomain

4 Select *Create New*.

5 Enter the following information and select *OK*:

Name	VLAN_200_ext
Interface	external
VLAN ID	200
Virtual Domain	DEFdomain

Figure 63: VLAN_200 internal and external interfaces for DEFdomain



To add the VLAN subinterfaces - CLI

```
config system interface
  edit VLAN_200_int
    set interface internal
    set vlanid 200
    set vdom DEFdomain
  next
  edit VLAN_200_ext
    set interface external
    set vlanid 200
    set vdom DEFdomain
  end
```

Selecting the DEFdomain VDOM

Before you follow the rest of the procedure for configuring VLAN_200, you must ensure that the current VDOM is DEFdomain.

To select the DEFdomain VDOM - web-based manager

1. Go to *System* > *VDOM*.
2. Select *Enter* for the DEFdomain VDOM.

To select the DEFdomain VDOM - CLI

```
config vdom
  edit DEFdomain
```

Creating service groups

DEF Inc. does not want its employees to use online gaming software or any online chat software except NetMeeting, which the company uses for net conferencing. To simplify the creation of a firewall policy for this purpose, you create a service group that contains all of the services you want to restrict. A firewall policy can manage only one service or one group. The administrator decided to simply name this group “Games” although it also restricts chat software.

To create a games service group - web-based manager

1. Go to *Firewall* > *Service* > *Group*.
2. Select *Create New*.
3. Enter `Games` in the *Group Name* field.
4. For each of AOL, IRC, QUAKE, SIP-MSNmessenger and TALK, select the service in the *Available Services* list and select the right arrow to add it to the *Members* list.
5. Select *OK*.

To create a games and chat service group - CLI

```
config firewall service group
  edit Games
    set member IRC QUAKE SIP-MSNmessenger AOL TALK
  end
```

Configuring DEFdomain firewall addresses

The “all” address is present by default in the root domain. In other domains, you must create it.

To configure DEFdomain firewall addresses - web-based manager

1. Go to *Firewall* > *Address.*
2. Select *Create New*.
3. Enter `new` in the *Address Name* field.
4. Type 0.0.0.0/0.0.0.0 in the *Subnet / IP Range* field.
5. Select *OK*.

To configure DEFdomain firewall addresses - CLI

```
config firewall address
  edit all
    set type ipmask
    set subnet 0.0.0.0 0.0.0.0
  end
```

Configuring DEFdomain firewall policies

Firewall policies allow packets to travel from the VLAN_200 interface to the external interface subject to the restrictions of the protection profile.

To configure DEFdomain firewall policies - web-based manager

1. Go to *Firewall* > *Policy*.
2. Select *Create New*.
3. Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	BusinessDay
Service	games-chat
Action	DENY

   This policy prevents the use of network games or chat programs (except NetMeeting) during business hours.

4. Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	Lunch
Service	HTTP
Action	ACCEPT
Protection Profile	Relaxed

   This policy relaxes the web category filtering during lunch hour.

5. Select *Create New*.

6 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	BusinessDay
Service	HTTP
Action	ACCEPT
Protection Profile	BusinessOnly

This policy provides rather strict web category filtering during business hours.

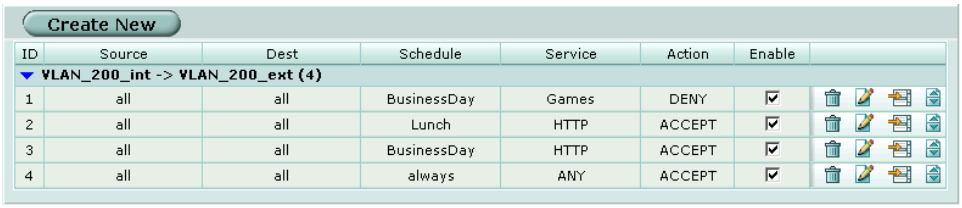
7 Select *Create New*.

8 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_200_int
Source Address	all
Destination Interface/Zone	VLAN_200_ext
Destination Address	all
Schedule	always
Service	ANY
Action	ACCEPT
Protection Profile	Relaxed

Because it is last in the list, this policy applies to the times and services not covered in preceding policies. This means that outside of regular business hours, the Relaxed protection profile applies to email and web browsing, and online chat and games are permitted. DEF Inc. needs this policy because its employees sometimes work overtime. The other companies in this example maintain fixed hours and do not want any after-hours Internet access.

Figure 64: DEFdomain firewall policies



To configure DEFdomain firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set schedule BusinessDay
    set service Games
    set action deny
  next
  edit 2
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule Lunch
    set service HTTP
    set profile_status enable
    set profile Relaxed
  next
  edit 3
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule BusinessDay
    set service HTTP
    set profile_status enable
    set profile BusinessOnly
  next
  edit 4
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set profile_status enable
    set profile Relaxed
end
```

Configuring the XYZdomain

This section describes how to add VLAN subinterfaces and configure firewall policies for the XYZdomain VDOM.

This section includes the following topics:

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add the VLAN subinterfaces - web-based manager

1 Go to *System* > *Network* > *Interface*.

2 Select *Create New*.

3 Enter the following information and select *OK*:

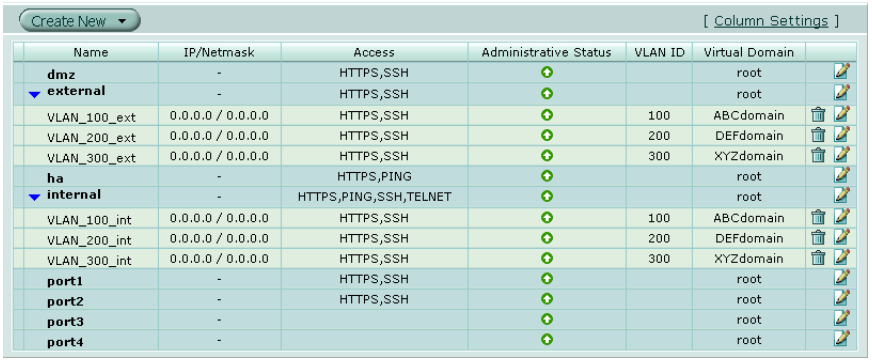
Name	VLAN_300_int
Interface	internal
VLAN ID	300
Virtual Domain	XYZdomain

4 Select *Create New*.

5 Enter the following information and select *OK*:

Name	VLAN_300_ext
Interface	external
VLAN ID	300
Virtual Domain	XYZdomain

Figure 65: VLAN_300 internal and external interfaces for XYZdomain



To add the VLAN subinterfaces - CLI

```
config system interface
  edit VLAN_300_int
    set interface internal
    set type vlan
    set vlanid 300
    set vdom XYZdomain
  next
  edit VLAN_300_ext
    set interface external
    set type vlan
    set vlanid 300
    set vdom XYZdomain
end
```

Selecting the XYZdomain VDOM

Before you follow the rest of the procedure for configuring VLAN_300, you must ensure that the current domain is XYZdomain.

To select the XYZdomain VDOM - web-based manager

1. Go to *System* > *VDOM*.
2. Select *Enter* for the XYZdomain VDOM.

To select the XYZdomain VDOM - CLI

```
config vdom
  edit XYZdomain
```

Creating service groups

XYZ Inc. wants network protection for email and web services. To simplify creation of firewall policies, you can create a email service group for POP3, IMAP and SMTP and a web service group for HTTP, HTTPS and FTP.

To create an email service group - web-based manager

1. Go to *Firewall* > *Service* > *Group*.
2. Select *Create New*.
3. Enter `Email` in the *Group Name* field.
4. For each of POP3, IMAP and SMTP, select the service in the *Available Services* list and select the right arrow to add it to the *Members* list.
5. Select *OK*.

To create an email service group - CLI

```
config firewall service group
  edit Email
    set member POP3 IMAP SMTP
end
```

To create a web service group - web-based manager

1. Go to *Firewall* > *Service* > *Group*.
2. Select *Create New*.
3. Enter `Web` in the *Group Name* field.
4. For each of HTTP, HTTPS and FTP, select the service in the *Available Services* list and select the right arrow to add it to the *Members* list.
5. Select *OK*.

To create a web service group - CLI

```
config firewall service group
  edit Web
    set member HTTP HTTPS FTP
end
```

Configuring XYZdomain firewall addresses

The “all” address is present by default in the root domain. In other domains, you must create it.

To configure XYZdomain firewall addresses - web-based manager

1. Go to *Firewall* > *Address*.
2. Select *Create New*.
3. Enter `new` in the *Address Name* field.
4. Enter `0.0.0.0/0.0.0.0` in the *Subnet / IP Range* field.
5. Select *OK*.

To configure XYZdomain firewall addresses - CLI

```
config firewall address
  edit all
    set type ipmask
    set subnet 0.0.0.0 0.0.0.0
end
```

Configuring XYZdomain firewall policies

Firewall policies allow packets to travel from the VLAN_300 interface to the external interface subject to the restrictions of the protection profile.

To configure XYZdomain firewall policies - web-based manager

1. Go to *Firewall* > *Policy*.
2. Select *Create New*.

3 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_300_int
Source Address	all
Destination Interface/Zone	VLAN_300_ext
Destination Address	all
Schedule	always
Service	Email
Action	ACCEPT
Protection Profile	strict

This policy provides network protection for email using the default strict protection profile. The administrator must also configure the antivirus, web filter and spam filter settings. These procedures are not described in this document.

4 Select *Create New*.

5 Enter the following information and select *OK*:

Source Interface/Zone	VLAN_300_int
Source Address	all
Destination Interface/Zone	VLAN_300_ext
Destination Address	all
Schedule	always
Service	Web
Action	ACCEPT
Protection Profile	web

This policy provides network protection for HTTP, HTTPS and FTP using the default web protection profile. The administrator must also configure the antivirus and web filter settings. These procedures are not described in this document.

Figure 66: XYZdomain firewall policies

To configure XYZdomain firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_300_int
    set srcaddr all
    set dstintf VLAN_300_ext
    set dstaddr all
    set action accept
    set schedule always
    set service Email
    set profile_status enable
    set profile strict
  next
```

```
    edit 2
      set srcintf VLAN_300_int
      set srcaddr all
      set dstintf VLAN_300_ext
      set dstaddr all
      set action accept
      set schedule always
      set service Web
      set profile_status enable
      set profile web
end
```

Configuring the VLAN switch and router

The Cisco switch is the first VLAN device internal passes through, and the Cisco router is the last device before the Internet or ISP.

This section includes the following topics:

- Configuring the Cisco switch
- Configuring the Cisco router

Configuring the Cisco switch

On the Cisco Catalyst 2900 ethernet switch, you need to define the VLANs 100, 200 and 300 in the VLAN database, and then add configuration files to define the VLAN subinterfaces and the 802.1Q trunk interface.

Add this file to Cisco VLAN switch:

```
!
interface FastEthernet0/1
 switchport access vlan 100
!
interface FastEthernet0/2
 switchport access vlan 200
!
interface FastEthernet0/5
 switchport access vlan 300
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

Switch 1 has the following configuration:

Port 0/1	VLAN ID 100
Port 0/2	VLAN ID 200
Port 0/3	VLAN ID 300
Port 0/6	802.1Q trunk

Configuring the Cisco router

The configuration for the Cisco router in this example is the same as in the basic example, except we add VLAN_300. Each of the three companies has its own subnet assigned to it.

The IP addressees assigned to each VLAN on the router are the gateway addresses for the VLANs. For example, devices on VLAN_100 would have their gateway set to 10.10.0.1/255.255.0.0.

```
!
interface FastEthernet0/0
!
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 10.10.0.1 255.255.0.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 200
 ip address 172.120.0.1 255.255.0.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 300
 ip address 192.168.0.1 255.255.0.0
!
```

The router has the following configuration:

Port 0/0.1	VLAN ID 100
Port 0/0.2	VLAN ID 200
Port 0/0.3	VLAN ID 300
Port 0/0	802.1Q trunk

Testing the configuration

Use diagnostic commands, such as tracert, to test traffic routed through the network.

You should test traffic between the internal VLANs as well as from the internal VLANs to the Internet to ensure connectivity.

This section includes the following topics:

- Testing traffic from VLAN_100 to the Internet
- Testing traffic from VLAN_100 to VLAN_200

Testing traffic from VLAN_100 to the Internet

In this example, a route is traced from VLANs to a host on the Internet. The route target is www.example.com.

From a host on VLAN_100, access a command prompt and enter this command:

```
C:\>tracert www.example.com
Tracing route to www.example.com [208.77.188.166]
over a maximum of 30 hops:
 1   <10 ms   <10 ms   <10 ms  10.100.0.1
...
14   172 ms   141 ms   140 ms  208.77.188.166
Trace complete.
```

The number of steps between the first and the last hop, as well as their IP addresses, will vary depending on your location and ISP. However, all successful tracerts to www.example.com will start and end with these lines.

Repeat the tracert for VLAN_200 and VLAN_300.

The tracert for each VLAN will include the gateway for that VLAN as the first step. Otherwise, the tracert should be the same for each VLAN.

Testing traffic from VLAN_100 to VLAN_200

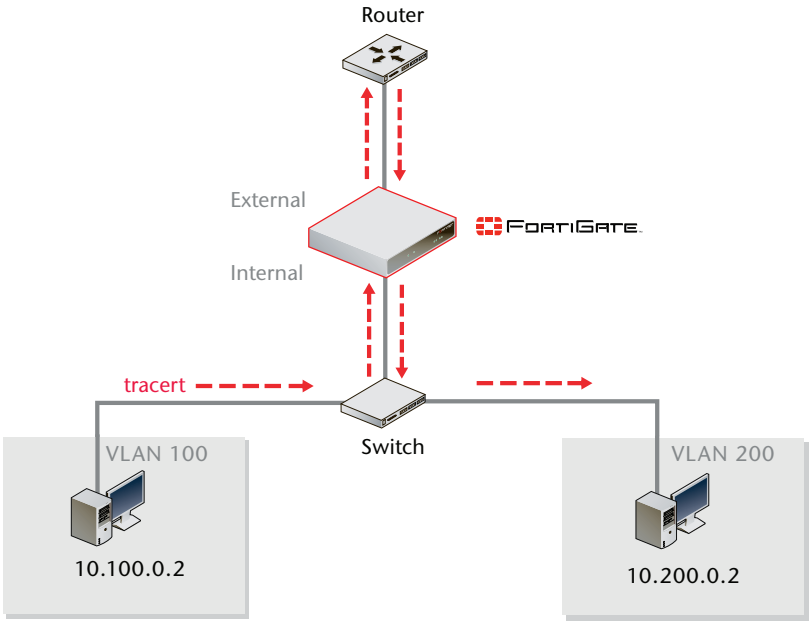
In this example, a route is traced between two internal networks. The route target is a host on VLAN_200. The Windows traceroute command `tracert` is used.

From VLAN_100, access a Windows command prompt and enter this command:

```
C:\>tracert 10.200.0.2
Tracing route to 10.200.0.2 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.100.0.1
  2   <10 ms   <10 ms   <10 ms  10.200.0.2
Trace complete.
```

You can repeat this for VLAN_100 to VLAN_300, and VLAN_200 to VLAN_300. In each case the IP addresses will be the gateway for the starting VLAN, and the end point at the ending VLAN.

Figure 67: Example trace route from VLAN_100 to VLAN_200



Avoiding problems with VLANs

Several problems can occur with your VLANs. This chapter provides solutions to these problems, under the following topics:

Asymmetric routing

You might discover unexpectedly that hosts on some networks are unable to reach certain other networks. This occurs when request and response packets follow different paths. If the FortiGate unit recognizes the response packets, but not the requests, it blocks the packets as invalid. Also, if the FortiGate unit recognizes the same packets repeated on multiple interfaces, it blocks the session as a potential attack.

This is asymmetric routing. By default, the FortiGate unit blocks packets or drops the session when this happens. You can configure the FortiGate unit to permit asymmetric routing by using the following CLI command:

```
config vdom
  edit <vdom_name>
    config system settings
    set asymroute enable
  end
end
```

If VDOMs are enabled, this command is per VDOM—you must set it for each VDOM that has the problem.

If this solves your blocked traffic problem, you know that asymmetric routing is the cause. But allowing asymmetric routing is not the best solution, because it reduces the security of your network.

For a long-term solution, it is better to change your routing configuration or change how your FortiGate unit connects to your network. The *Asymmetric Routing and Other FortiGate Layer-2 Installation Issues* technical note provides detailed examples of asymmetric routing situations and possible solutions.

Caution: If you enable asymmetric routing, antivirus and intrusion prevention systems will not be effective. Your FortiGate unit will be unaware of connections and treat each packet individually. It will become a stateless firewall.

Layer-2 and Arp traffic

By default, FortiGate units do not pass layer-2 traffic. If there are layer-2 protocols such as IPX, PPTP or L2TP in use on your network, you need to configure your FortiGate unit interfaces to pass these protocols without blocking. Another type of layer-2 traffic is ARP traffic. For more information on ARP traffic, see “ARP traffic” on page 194.

You can allow these layer-2 protocols using the CLI command:

```
config vdom
  edit <vdom_name>
    config system interface
    edit <name_str>
    set l2forward enable
  end
end
```

where `<name_str>` is the name of an interface.

If VDOMs are enabled, this command is per VDOM—you must set it for each VDOM that has the problem.

If you enable layer-2 traffic, you may experience a problem if packets are allowed to repeatedly loop through the network. This repeated looping, very similar to a broadcast storm, happens when you have more than one layer-2 path to a destination—traffic may overflow and bring your network to a halt. You can break the loop by enabling Spanning Tree Protocol (STP) on your network's switches and routers. For more information, see "STP forwarding" on page 197.

ARP traffic

Address Resolution Protocol (ARP) packets are vital to communication on a network, and ARP support is enabled on FortiGate unit interfaces by default. Normally you want ARP packets to pass through the FortiGate unit, especially if it is sitting between a client and a server or between a client and a router.

ARP traffic can cause problems, especially in Transparent mode where ARP packets arriving on one interface are sent to all other interfaces including VLAN subinterfaces. Some layer-2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN. This instability can occur if the layer-2 switch does not maintain separate MAC address tables for each VLAN. Unstable switches may reset and cause network traffic to slow down considerably.

Multiple VDOMs solution

By default, physical interfaces are in the root domain. If you do not configure any of your VLANs in the root VDOM, it will not matter how many interfaces are in the root VDOM.

The multiple VDOMs solution is to configure multiple VDOMs on the FortiGate unit, one for each VLAN. In this solution, you configure one inbound and one outbound VLAN interface in each VDOM. ARP packets are not forwarded between VDOMs. This configuration limits the VLANs in a VDOM and correspondingly reduces the administration needed per VDOM.

As a result of this configuration, the switches do not receive multiple ARP packets with duplicate MACs. Instead, the switches receive ARP packets with different VLAN IDs and different MACs. Your switches are stable.

However, you should ***not*** use the multiple VDOMs solution under any of the following conditions:

- you have more VLANs than licensed VDOMs
- you do not have enough physical interfaces
- your configuration needs VLAN grouping.

Instead, use one of two possible solutions, depending on which operation mode you are using:

- In NAT/Route mode, you can use the `vlan forward` CLI command.
- In Transparent mode, you can use the `forward-domain` CLI command. But you still need to be careful in some rare configurations.

Vlanforward solution

If you are using NAT/Route mode, the solution is to use the `vlanforward` CLI command for the interface in question. By default, this command is enabled and will forward VLAN traffic to all VLANs on this interface. When disabled, each VLAN on this physical interface can send traffic only to the same VLAN—there is no ”cross-talk” between VLANs, and ARP packets are forced to take one path along the network which prevents the multiple paths problem.

In the following example, `vlanforward` is disabled on port1. All VLANs configured on port1 will be separate and will not forward any traffic to each other.

```
config system interface
  edit port1
    set vlanforward disable
end
```

Forward-domain solution

If you are using Transparent mode, the solution is to use the `forward-domain` CLI command. This command tags VLAN traffic as belonging to a particular collision group, and only VLANs tagged as part of that collision group receive that traffic—it is like an additional set of VLANs. By default, all interfaces and VLANs are part of forward-domain collision group 0.

The many benefits of this solution include reduced administration, the need for fewer physical interfaces, and the availability of more flexible network solutions.

In the following example, forward-domain collision group 340 includes VLAN 340 traffic on port1 and untagged traffic on port2. Forward-domain collision group 341 includes VLAN 341 traffic on port1 and untagged traffic on port3. All other interfaces are part of forward-domain collision group 0 by default. This configuration separates VLANs 340 and 341 from each other on port1, and prevents the ARP packet problems from before.

Use these CLI commands:

```
config system interface
  edit port1
  next
  edit port2
    set forward_domain 340
  next
  edit port3
    set forward_domain 341
  next
  edit port1-340
    set forward_domain 340
    set interface port1
    set vlanid 340
  next
  edit port1-341
    set forward_domain 341
    set interface port1
    set vlanid 341
end
```

You may experience connection issues with layer-2 traffic, such as ping, if your network configuration has:

- packets going through the FortiGate unit in Transparent mode more than once
- more than one forwarding domain (such as incoming on one forwarding domain and outgoing on another)
- IPS and AV enabled.

In releases prior to FortiOS v3.0 MR5, packets could go through IPS and AV checks each time they passed through the FortiGate unit. In FortiOS v3.0 MR5 this problem was fixed. Now IPS and AV is applied the first time packets go through the FortiGate unit, but not on subsequent passes. Only applying IPS and AV to this first pass fixes the network layer-2-related connection issues.

There is a more detailed discussion of this issue in the *Asymmetric Routing and Other FortiGate Layer-2 Installation Issues* technical note.

NetBIOS

Computers running Microsoft Windows operating systems that are connected through a network rely on a WINS server to resolve host names to IP addresses. The hosts communicate with the WINS server by using the NetBIOS protocol.

To support this type of network, you need to enable the forwarding of NetBIOS requests to a WINS server. The following example will forward NetBIOS requests on the internal interface for the WINS server located at an IP address of 192.168.111.222.

```
config system interface
  edit internal
    set netbios_forward enable
    set wins-ip 192.168.111.222
end
```

These commands apply only in NAT/Route mode. If VDOMs are enabled, these commands are per VDOM—you must set them for each VDOM that has the problem.

STP forwarding

The FortiGate unit does not participate in the Spanning Tree Protocol (STP). STP is an IEEE 802.1 protocol that ensures there are no layer-2 loops on the network. Loops are created when there is more than one route for traffic to take and that traffic is broadcast back to the original switch. This loop floods the network with traffic, reducing available bandwidth to nothing.

If you use your FortiGate unit in a network topology that relies on STP for network loop protection, you need to make changes to your FortiGate configuration. Otherwise, STP recognizes your FortiGate unit as a blocked link and forwards the data to another path. By default, your FortiGate unit blocks STP as well as other non-IP protocol traffic.

Using the CLI, you can enable forwarding of STP and other layer-2 protocols through the interface. In this example, layer-2 forwarding is enabled on the external interface:

```
config system interface
  edit external
    set l2forward enable
    set stpforward enable
end
```

By substituting different commands for `stpforward enable`, you can also allow layer-2 protocols such as IPX, PPTP or L2TP to be used on the network. For more information, see “Layer-2 and Arp traffic” on page 193.

Too many VLAN interfaces

Any virtual domain can have a maximum of 255 interfaces in Transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. NAT/Route mode supports from 255 to 8192 depending on the FortiGate model. This total number of interfaces includes VLANs, other virtual interfaces, and physical interfaces.

Your FortiGate unit may allow you to configure more interfaces than this. However, if you configure more than 255 interfaces, your system will become unstable and, over time, will not work properly. As all interfaces are used, they will overflow the routing table that stores the interface information, and connections will fail. When you try to add more interfaces, an error message will state that the maximum limit has already been reached.

If you see this error message, chances are you already have too many VLANs on your system and your routing has become unstable. To verify, delete a VLAN and try to add it back. If you have too many, you will not be able to add it back on to the system. In this case, you will need to remove enough interfaces (including VLANs) so that the total number of interfaces drops to 255 or less. After doing this, you should also reboot your FortiGate unit to clean up its memory and buffers, or you will continue to experience unstable behavior.

To configure more than 255 interfaces on your FortiGate unit in Transparent mode, you have to configure multiple VDOMs, each with many VLANs. However, if you want to create more than the default 10 VDOMs (or a maximum of 2550 interfaces), you must buy a license for additional VDOMs. Only FortiGate models 3000 and higher support more than 10 VDOMs. For more information, see “Increasing the number of VDOMs” on page 65.

With these extra licenses, you can configure up to 500 VDOMs, with each VDOM containing up to 255 VLANs in Transparent mode. This is a theoretical maximum of over 127 500 interfaces. However, system resources will quickly get used up before reaching that theoretical maximum. To achieve the maximum number of VDOMs, you need to have top-end hardware with the most resources possible.

In NAT/Route mode, if you have a top-end model, the maximum interfaces per VDOM can be as high as 8192. This is enough for all the VLANs that are needed.

Note: Your FortiGate unit has limited resources, such as CPU load and memory, that are divided between all configured VDOMs. When running 250 or more VDOMs, you cannot run Unified Threat Management (UTM) features such as proxies, web filtering, or antivirus—your FortiGate unit can only provide basic firewall functionality.

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

T

U

V

W

www.fortinet.com

www.fortinet.com