

The Fortinet logo is displayed in white, bold, uppercase letters. The letter 'O' is replaced by a red square containing a white grid pattern. A small 'TM' trademark symbol is located at the bottom right of the word.

FORTINETTM

FortiGate VLANs and VDOMs

User Guide

FortiGate VLANs and VDOMs Guide

Version 1.1

1 April 2005

01-28007-0091-20050401

© Copyright 2005 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

FortiGate VLANs and VDOMs Guide

Version 1.1

1 April 2005

01-28007-0091-20050401

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

CAUTION: RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

For technical support, please visit <http://www.fortinet.com>.

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

Table of Contents

Introduction	9
About FortiGate VLANs amd VDOMs	9
About this document	9
FortiGate documentation	10
Related documentation	10
FortiManager documentation	11
FortiClient documentation	11
FortiMail documentation	11
FortiLog documentation	11
Fortinet Knowledge Center	12
Comments on Fortinet technical documentation	12
Customer service and technical support	12
Introduction to VLANs and VDOMs	13
Overview of VLAN technology	14
VLAN layer-2 switching	14
VLAN layer-3 routing	15
Rules for VLAN IDs	16
Overview of Virtual Domains	16
Administration of virtual domains	17
Global and virtual domain properties	17
Creating virtual domains	19
Selecting the current virtual domain	19
For more information	19
Using VLANs in NAT/Route mode	21
Overview	21
Configuring FortiGate units in NAT/Route mode	21
Adding VLAN subinterfaces	22
Creating firewall policies	23
Configuring routing	23
Example configuration NAT/Route mode (simple)	24
General configuration steps	24
Configuring the FortiGate-300 unit	24
Configuring the external interface - web-based manager	24
Configuring the external interface - CLI	25
Adding VLAN subinterfaces - web-based manager	25
Adding VLAN subinterfaces - CLI	26
Adding the firewall addresses - web-based manager	26
Adding the firewall addresses - CLI	27
Adding the firewall policies - web-based manager	27

Adding the firewall policies - CLI	28
Configuring the Cisco switch.....	29
Configuring the VLAN subinterfaces and the trunk interfaces	29
Testing the configuration.....	30
Testing traffic from VLAN 100 to VLAN 200	30
Testing traffic from VLAN 100 to the external network.....	30
Example configuration NAT/Route mode (complex).....	31
General configuration steps	33
Configuring the FortiGate-300 unit.....	33
Adding the VLAN subinterfaces - web-based manager.....	33
Adding the VLAN subinterfaces - CLI.....	34
Adding a default route - web-based manager	35
Adding a default route - CLI.....	36
Adding the firewall addresses - web-based manager.....	36
Adding the firewall addresses - CLI.....	36
Adding the firewall policies - web-based manager	37
Adding the firewall policies - CLI	39
Configuring the FortiGate-300 IPsec VPN tunnel and encrypt policy.....	40
Configuring the VPN gateway - web-based manager	40
Configuring the VPN gateway - CLI.....	41
Configuring the VPN tunnel - web-based manager.....	41
Configuring the VPN tunnel - CLI	42
Defining the VPN user IP address - web-based users	42
Defining the VPN user IP address - CLI	43
Adding the encrypt policy - web-based manager	43
Adding the encrypt policy - CLI.....	43
Configuring the VPN client.....	44
Creating a new VPN connection.....	44
Configuring the internal Cisco switch.....	46
Configuring the VLAN subinterfaces and the trunk interfaces.....	46
Configuring the external Cisco switch.....	47
Configuring the VLAN subinterfaces and the trunk interfaces.....	47
Testing the configuration.....	47
Testing traffic from VLAN 20 to VLAN 10.....	47
Testing traffic from VLAN 10 to the external network.....	48
Using VDOMs in NAT/Route mode.....	49
Overview.....	49
Adding virtual domains.....	49
Administration of virtual domains	49

Configuring virtual domains	50
Adding interfaces and VLAN subinterfaces to a virtual domain	50
Configuring routing for a virtual domain	51
Configuring firewall policies for a virtual domain	51
Configuring VPNs for a virtual domain	52
Example VDOM configuration in NAT/Route mode (simple)	53
General configuration steps	53
Creating virtual domains	54
Creating the vdomain2 virtual domain	54
Configuring the FortiGate-300 external and DMZ interfaces	54
Configuring the external interface - web-based manager	54
Configuring the external interface - CLI	54
Configuring the DMZ interface - web-based manager	54
Configuring the DMZ interface - CLI	55
Configuring the root virtual domain	55
Adding the VLAN 100 subinterface - web-based manager	55
Adding VLAN 100 subinterface - CLI	55
Selecting the root virtual domain - web-based manager	56
Selecting the root virtual domain - CLI	56
Adding root domain firewall addresses - web-based manager	56
Adding the root domain firewall addresses - CLI	56
Adding the root domain firewall policy - web-based manager	56
Adding the firewall policy - CLI	57
Adding a default route - web-based manager	57
Adding a default route - CLI	58
Configuring the vdomain2 virtual domain	58
Adding the VLAN 200 subinterface - web-based manager	58
Adding VLAN 200 subinterface - CLI	59
Selecting the vdomain2 virtual domain - web-based manager	59
Selecting the vdomain2 virtual domain - CLI	59
Adding the vdomain2 firewall address - web-based manager	59
Adding the vdomain2 firewall address - CLI	60
Adding the vdomain2 firewall policy - web-based manager	60
Adding the vdomain2 firewall policy - CLI	61
Adding a default route - web-based manager	61
Adding a default route - CLI	61
Configuring the Cisco switch	62
Configuring the VLAN subinterfaces and the trunk interfaces	62
Testing the configuration	62
Testing traffic from VLAN 100 to the external network	62
Testing traffic from VLAN 200 to the DMZ network	63

Example VDOM configuration in NAT/Route mode (complex)	64
General configuration steps	66
Creating the virtual domains	66
Configuring the root domain	67
Selecting the root virtual domain	67
Adding the VLAN subinterfaces	67
Adding a default route	69
Adding the firewall addresses	70
Adding the firewall policies	71
Configuring the Commercial vdomain	73
Selecting the Commercial virtual domain	73
Adding the VLAN subinterfaces	73
Adding a default route	76
Adding the firewall addresses	77
Adding the firewall policies	78
Configuring the Cisco switch	83
Configuring the VLAN subinterfaces and the trunk interfaces	83
Testing the configuration	84
Testing traffic from instructors network to student network	84
Other tests	85

Using VLANs and VDOMs in Transparent mode 87

Overview	87
VLANs and virtual domains	87
Configuring the FortiGate unit in Transparent mode	88
Adding VLAN subinterfaces	88
Creating firewall policies	89
Example configuration Transparent mode (simple)	90
General configuration steps	91
Configuring the FortiGate-300 unit	91
Adding VLAN subinterfaces	91
Adding the firewall policies	93
Configuring the Cisco switch	95
Configuring the VLAN subinterfaces and the trunk interfaces	95
Configuring the Cisco router	96
Configuring the VLAN subinterfaces and the trunk interfaces	96
Testing the configuration	97
Testing traffic from VLAN 100 to VLAN 200	97
Example configuration Transparent mode (multiple virtual domains)	98
Configuring global items	99
Creating schedules	99
Creating protection profiles	100
Creating virtual domains	102

Configuring the ABCdomain	103
Adding VLAN subinterfaces.....	103
Selecting the ABCdomain VDOM.....	104
Creating service groups.....	104
Configuring ABCdomain firewall addresses	105
Configuring ABCdomain firewall policies.....	105
Configuring the DEFdomain.....	107
Adding VLAN subinterfaces.....	107
Selecting the DEFdomain VDOM.....	108
Creating service groups.....	109
Configuring DEFdomain firewall addresses	109
Configuring DEFdomain firewall policies	110
Configuring the XYZdomain	113
Adding VLAN subinterfaces.....	113
Selecting the XYZdomain VDOM	114
Creating service groups.....	114
Configuring XYZdomain firewall addresses.....	115
Configuring XYZdomain firewall policies	115
Configuring the Cisco switch.....	117
Configuring switch 1	117
Configuring switch 2	118
Testing the configuration.....	118
Testing traffic from VLAN 100 to the Internet	118
Avoiding Problems with VLANs	119
Overview	119
Asymmetric routing	119
Layer 2 traffic	120
ARP traffic.....	120
NetBIOS.....	121
STP forwarding	121



Introduction

This chapter introduces you to FortiGate VLANs and VDOMs and the following topics:

- [About FortiGate VLANs and VDOMs](#)
- [About this document](#)
- [FortiGate documentation](#)
- [Related documentation](#)
- [Customer service and technical support](#)

About FortiGate VLANs and VDOMs

Virtual Local Area Networks (VLANs) and Virtual Domains (VDOMs) multiply the capabilities of your FortiGate unit. VLANs increase the number of network interfaces beyond the physical connections on the unit. VDOMs enable the unit to function as multiple independent units with common administration.

About this document

This document describes how to implement IEEE 802.1Q VLAN technology on FortiGate units operating in both NAT/Route and Transparent mode. It also describes how to use the FortiGate VDOMs to provide separate network protection, routing and VPN configurations for multiple organizations.

This document contains the following chapters:

- [Introduction to VLANs and VDOMs](#)
- [Using VLANs in NAT/Route mode](#)
- [Using VDOMs in NAT/Route mode](#)
- [Using VLANs and VDOMs in Transparent mode](#)
- [Avoiding Problems with VLANs](#)

FortiGate documentation

Information about FortiGate products is available from the following guides:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference Guide*
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference Guide*
Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability Guide*
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS Guide*
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate VPN Guide*
Explains how to configure VPNs using the web-based manager.
- *FortiGate VLANs and VDOMs Guide*
Describes how to configure VLANs and VDOMs in both NAT/Route and Transparent mode. Includes detailed examples.

Related documentation

Additional information about Fortinet products is available from the following related documentation.

FortiManager documentation

- *FortiManager QuickStart Guide*
Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.
- *FortiManager System Administration Guide*
Describes how to use the FortiManager System to manage FortiGate devices.
- *FortiManager System online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the FortiManager Console as you work.

FortiClient documentation

- *FortiClient Host Security User Guide*
Describes how to use FortiClient Host Security software to set up a VPN connection from your computer to remote networks, scan your computer for viruses, and restrict access to your computer and applications by setting up firewall policies.
- *FortiClient Host Security online help*
Provides information and procedures for using and configuring the FortiClient software.

FortiMail documentation

- *FortiMail Administration Guide*
Describes how to install, configure, and manage a FortiMail unit in gateway mode and server mode, including how to configure the unit; create profiles and policies; configure antispam and antivirus filters; create user accounts; and set up logging and reporting.
- *FortiMail online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Web Mail Online Help*
Describes how to use the FortiMail web-based email client, including how to send and receive email; how to add, import, and export addresses; and how to configure message display preferences.

FortiLog documentation

- *FortiLog Administration Guide*
Describes how to install and configure a FortiLog unit to collect FortiGate and FortiMail log files. It also describes how to view FortiGate and FortiMail log files, generate and view log reports, and use the FortiLog unit as a NAS server.
- *FortiLog online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

Fortinet Knowledge Center

The most recent versions of all Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com/>.

Comments on Fortinet technical documentation

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

Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet Technical Support web site at <http://support.fortinet.com>.

You can also register Fortinet products and service contracts from <http://support.fortinet.com> and change your registration information at any time.

Technical support is available through email from any of the following addresses. Choose the email address for your region:

- | | |
|---|---|
| amer_support@fortinet.com | For customers in the United States, Canada, Mexico, Latin America and South America. |
| apac_support@fortinet.com | For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia. |
| eu_support@fortinet.com | For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East. |

For information about our priority support hotline (live support), see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- your name
- your company's name and location
- your email address
- your telephone number
- your support contract number (if applicable)
- the product name and model number
- the product serial number (if applicable)
- the software or firmware version number
- a detailed description of the problem

Introduction to VLANs and VDOMs

Virtual Local Area Networks (VLANs) and Virtual Domains (VDOMs) multiply the capabilities of your FortiGate unit. VLANs increase the number of network interfaces beyond the physical connections on the unit. VDOMs enable the unit to function as multiple independent units with common administration.

Using VLANs, a single FortiGate unit can provide security services and control connections between multiple security domains. Traffic from each security domain is given a different VLAN ID. The FortiGate unit can also apply authentication, protection profiles, and other firewall policy features for network and VPN traffic that is allowed to pass between security domains.

This document describes how to implement IEEE 802.1Q Virtual LAN (VLAN) technology on FortiGate units operating in both NAT/Route and Transparent mode. Example configurations illustrate how VLANs can be implemented between FortiGate units and other 802.1Q-compliant devices, such as Cisco switches and routers.

Using VDOMs, a single FortiGate unit can serve multiple organizations. It can provide separate firewall policies and, in NAT/Route mode, completely separate routing and VPN configurations for each organization. Using VDOMs can also simplify administration of complex configurations. This document describes FortiGate VDOM functionality and provides example configurations to illustrate the use of VDOMs in both NAT/Route and Transparent mode.

The information in this document applies to all FortiGate units. All FortiGate models support VLANs and VDOMs. Only the maximum number of VLANs and VDOMs varies. Models 50, 60 and 100 support a maximum of 12 network interfaces, which includes physical interfaces and VLAN subinterfaces. Other models support a maximum of 4096 interfaces. Most models support 10 virtual domains. For models 3000 and higher, firmware builds are available to support up to 250 VDOMs.

This document contains the following sections:

- [Overview of VLAN technology](#)
- [Overview of Virtual Domains](#)
- [Using VLANs in NAT/Route mode](#)
- [Using VDOMs in NAT/Route mode](#)
- [Using VLANs and VDOMs in Transparent mode](#)

Each of the Using sections contains detailed example configurations.

Overview of VLAN technology

A VLAN is a group of PCs, servers, and other network devices that communicate as if they were on the same LAN segment—even though they may not be. For example, the workstations and servers for an accounting department could be scattered throughout an office, connected to numerous network segments, but they can still belong to the same VLAN.

A VLAN segregates devices logically instead of physically. Each VLAN is treated as a broadcast domain. Devices in VLAN 1 can connect with other devices in VLAN 1, but cannot connect with devices in other VLANs. The communication among devices on a VLAN is independent of the physical network.

FortiGate units support IEEE 802.1Q Virtual LAN (VLAN) technology.

A VLAN segregates devices by adding 802.1Q VLAN tags to all of the packets sent and received by the devices in the VLAN. VLAN tags are 4-byte frame extensions that contain a VLAN identifier as well as other information.

In a typical VLAN configuration, 802.1Q-compliant VLAN layer-2 switches or layer-3 routers or firewalls add VLAN tags to packets. Packets passing between devices in the same VLAN can be handled by layer-2 switches. Packets passing between devices in different VLANs must be handled by a layer-3 device such as a router, firewall, or layer-3 switch.

VLAN layer-2 switching

A FortiGate unit in Transparent mode acts as a layer-2 device and can be interconnected with other layer-2 devices such as switches.

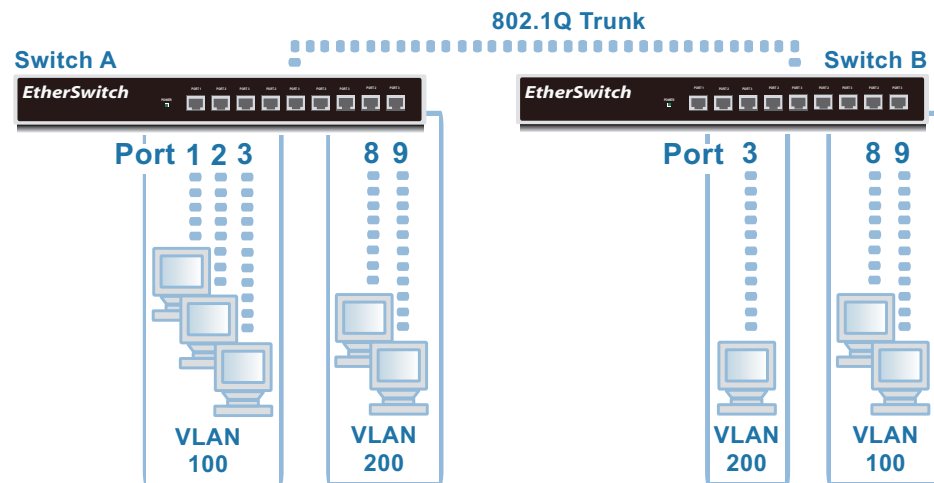
The network administrator configures a layer-2 switch by assigning VLAN IDs to the switch's network interfaces. Each network interface can be in a different VLAN or multiple interfaces can be added to the same VLAN. The administrator can also configure some network interfaces as 802.1Q "trunks." Trunks relay traffic between switches that support the same VLANs.

For example, a switch with 9 network interfaces could have network interfaces 1, 2 and 3 in one VLAN and interfaces 8 and 9 in another. In this configuration, the switch adds VLAN tags with ID set to 100 to frames arriving on network interfaces 1, 2 and 3, and VLAN tags with ID set to 200 to frames arriving on network interfaces 8 and 9. In this example, interfaces 4, 5, 6 and 7 are unused.

After adding the VLAN tag, the switch forwards the frame to other network interfaces with the same VLAN ID (and so in the same VLAN broadcast domain). The broadcast domain can be limited to network interfaces on the switch, or extended across trunks to include network interfaces on other 802.1Q-compliant switches.

For example, when switch A receives a frame at network interface 1, it applies a tag for VLAN 100. Switch A then forwards the frame to local network interfaces that are also in VLAN 1 and across a trunk to switch B. Switch B reads the VLAN tag and forwards the frame through its own local network interfaces that are in VLAN 1. The VLAN switch does not forward the frame outside of VLAN 1.

Figure 1: Example VLAN layer-2 switching



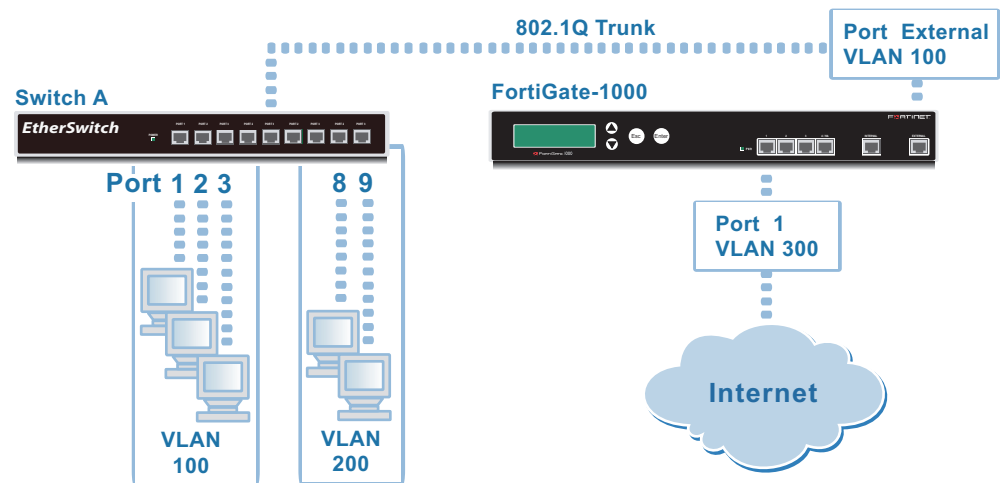
VLAN layer-3 routing

A FortiGate unit in NAT/Route mode is a layer-3 device. As in layer-2, it is 802.1Q-compliant.

In a layer-3 environment, the 802.1Q-compliant device receives the packet and assigns a VLAN ID. The device then forwards the packet 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. Layer-3 devices use the information contained in the packet, including the VLAN tag, protocol, IP address and port number, to make a routing decision. The packet may be forwarded to the same or another VLAN, or sent to a regular, non-tagged network.

In the example shown in [Figure 2](#), for switch A and the FortiGate-1000 unit to communicate over an 802.1Q trunk, the switch forwards a packet tagged with VLAN ID 100 to the FortiGate unit. When the FortiGate unit receives the packet, it removes the VLAN tag and examines the source and destination addresses, protocol, port number and other information. The FortiGate unit uses this information to select a firewall policy. The firewall policy indicates that the packet must be forwarded to its destination through a FortiGate unit VLAN subinterface. Before the packet exits the FortiGate unit, the VLAN subinterfaces add a new VLAN tag with VLAN ID 300 to the packet. The FortiGate unit then forwards the packet to its destination.

Figure 2: Example VLAN layer-3 routing



Rules for VLAN IDs

VLAN subinterfaces added to the same physical interface of a FortiGate unit cannot have the same VLAN ID. However, you can add VLAN subinterfaces with the same VLAN ID to different physical interfaces. Creating VLAN subinterfaces with same VLAN ID does not create any internal connection between them. Their relationship is the same as between any two FortiGate network interfaces.

Overview of Virtual Domains

Virtual Domains provide a way to divide your FortiGate unit and operate it as multiple separate units with common administration. You can configure and manage interfaces, VLAN subinterfaces, zones, firewall policies, routing, and VPN configurations for each virtual domain separately. This separation simplifies configuration because you do not have to manage as many 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. Communication between organizations is possible only if both allow access to an external network such as the internet.

When a packet enters a virtual domain, it is confined to that virtual domain. In a given domain, you can only create firewall policies for connections between VLAN subinterfaces or zones in the virtual domain. The packet never crosses virtual domain borders.

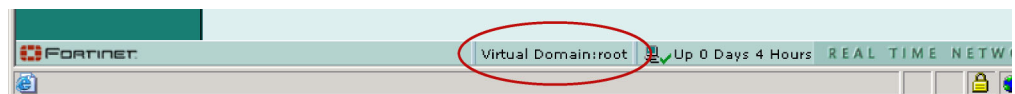
Administration of virtual domains

Virtual domains share a common administrative model. Administrators have access to all of the virtual domains on the FortiGate unit. Access profiles configure administrator access (read-only or read/write) to system configuration, logs and reporting, security policy, user authorization, administrator configuration, FortiProtect Update and system shutdown.

Global and virtual domain properties

When working with virtual domains, it is important to remember which settings belong exclusively to the virtual domain and which apply to the entire FortiGate unit. The web-based manager helps you understand the scope of the settings you are configuring by showing the affected virtual domain in the center of the status line at the bottom of the page. If you are configuring global properties, it shows “All”.

Figure 3: Status line virtual domain indicator



Properties exclusive to virtual domains

The following configuration settings are exclusively part of a virtual domain and are not shared between virtual domains:

- System settings
 - Physical interfaces
 - VLAN subinterfaces
 - Zones
 - Management IP address for Transparent mode
- Routing configuration
 - Router configuration in NAT/Route mode
 - Routing table configuration in Transparent mode
- Firewall settings
 - Policies
 - Addresses
 - Service groups
 - IP pools
 - Virtual IPs
- Virtual Private Network (VPN) configurations for
 - IPSec
 - PPTP
 - L2TP

Properties shared by all virtual domains

Virtual domains share the following global properties with other processes on the FortiGate unit:

- Unit configuration
 - Host Name
 - Firmware Version
 - Antivirus Definitions and engine
 - Attack Definitions and engine
 - Serial Number
 - Operation Mode
- Network configuration
 - DNS settings
- DHCP configuration

DHCP settings are applied per interface no matter which virtual domain the interface has been added to
- System Config
 - Time
 - Options
 - HA
 - SNMP v1/v2c
 - Replacement messages
 - FortiManager configuration
- System Administration
 - Administrators
 - Access profiles
- System Maintenance
 - Update Center
- Firewall
 - Services (predefined and custom) but not service groups
 - Schedules
 - Protection Profiles
- Users and authentication
- IPS
- Antivirus
- Web filter
- Spam filter
- Log and report
- VPN Certificates

Creating virtual domains

By default, the FortiGate unit has one fixed virtual domain named “root”, which you cannot delete or rename. You can create additional virtual domains and name them as you like.

- 1 Go to **System > Virtual Domain**.
- 2 Select Create New.
- 3 Enter the name for your virtual domain select OK.

Selecting the current virtual domain

The current virtual domain is the one to which virtual domain-specific configuration changes such as routing and firewall policies apply.

- 1 Go to **System > Virtual Domain**.
- 2 Select Change beside the listed Current virtual domain.
- 3 Select the virtual domain that you want to configure and select OK.

For more information

Detailed information and procedures involving virtual domains are provided in the [“Using VDOMs in NAT/Route mode”](#) and [“Using VLANs and VDOMs in Transparent mode”](#) chapters.

Using VLANs in NAT/Route mode

Overview

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

In NAT/Route mode, the FortiGate units support VLANs for constructing VLAN trunks between an IEEE 802.1Q-compliant switch (or router) and the FortiGate unit. Normally the FortiGate unit internal interface connects to a VLAN trunk on an internal switch, and the external interface connects to an upstream Internet router untagged. The FortiGate unit can then apply different policies for traffic on each VLAN that connects to the internal interface.

In this configuration, you add VLAN subinterfaces to the FortiGate physical interfaces that have VLAN IDs that match the VLAN IDs of packets in the VLAN trunk. The FortiGate unit directs packets with VLAN IDs to subinterfaces with matching VLAN IDs.

You can define VLAN subinterfaces on all FortiGate interfaces. The FortiGate unit can add VLAN tags to packets leaving a VLAN subinterface or remove VLAN tags from incoming packets and add a different VLAN tags to outgoing packets.

Configuring FortiGate units in NAT/Route mode

There are several essential steps to configure your FortiGate unit to work with VLANs:

- Add VLAN subinterfaces
- Create firewall policies
- Configure routing

You can also configure the protection profiles that govern virus scanning, web filtering, and spam filtering. Protection profiles are covered in the documentation for your FortiGate unit.

In NAT/Route mode, you can access the FortiGate unit's web-based manager by connecting to an interface configured for administrative access and using HTTPS to access the IP address of the interface. On the FortiGate 300 used as an example in this document, administrative access is enabled by default on the Internal interface and the default address of the interface is 192.168.1.99. If you need more information, see the *Quick Start Guide* or *Installation Guide* for your unit.

Adding VLAN subinterfaces

You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

IP addresses of all FortiGate interfaces cannot overlap. That is, the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to VLAN subinterfaces.



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.

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router. The VLAN ID can be any number between 1 and 4096. Each VLAN subinterface must also be configured with its own IP address and netmask.

To add a VLAN subinterface in NAT/Route mode

- 1 Go to **System > Network > Interface**.
- 2 Select Create New to add a VLAN subinterface.
- 3 Enter a Name to identify the VLAN subinterface.
- 4 Select the physical interface that receives the VLAN packets intended for this VLAN subinterface.
- 5 Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.
- 6 Configure the VLAN subinterface settings as you would for any FortiGate interface.
- 7 Select OK to save your changes.

The FortiGate unit adds the new VLAN subinterface to the interface that you selected in step 4.

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.

You need firewall policies to permit packets to pass from the VLAN interface where they enter the unit to the interface where they exit the unit. For each VLAN, you create a firewall policy for each of the following permitted connections:

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

The FortiGate unit subjects the packets on each VLAN to antivirus and antispam scanning as they pass through the unit.

To add firewall policies for VLAN subinterfaces

- 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 Add firewall policies as required.

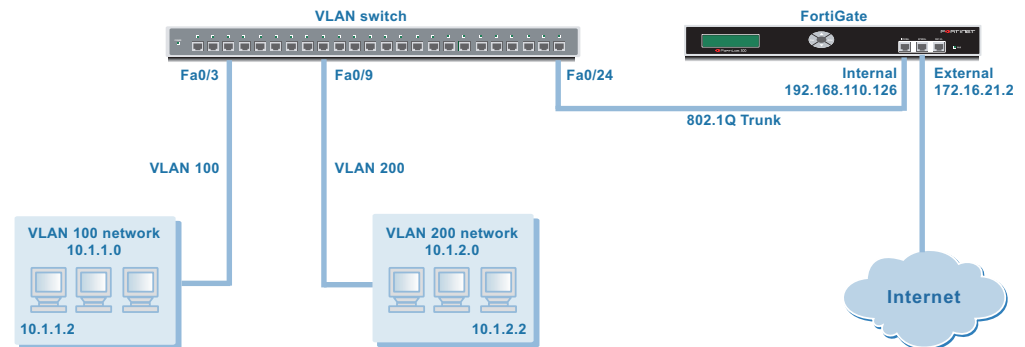
Configuring routing

In the simplest case, you need to configure a default route for packets with external destinations to the gateway of an external network. In more complex cases, you might have to configure different routes based on packet source and destination addresses. Routing is explained in the documentation provided with your FortiGate unit.

Example configuration NAT/Route mode (simple)

Figure 4 shows a simplified NAT/Route mode VLAN configuration. In this example, FortiGate internal interface connects to a Cisco 2900 VLAN switch using an 802.1Q trunk and is configured with two VLAN subinterfaces (VLAN 100 and VLAN 200). The external interface connects to the Internet and is not configured with VLAN subinterfaces.

Figure 4: FortiGate unit in Nat/Route mode



When the Cisco switch receives packets from VLAN 100 and VLAN 200, it applies VLAN ID tags and forwards the packets to local ports and across the trunk to the FortiGate unit. 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-300 unit and a Cisco 2900 switch for this example network topology.

General configuration steps

- 1 Configure the FortiGate-300 external interface.
- 2 Configure VLANs on the FortiGate-300 unit.
 - Add two VLAN subinterfaces to the Internal network interface.
 - Add Firewall addresses and address ranges for the internal and external networks.
 - Add firewall policies to allow:
 - the VLAN networks to access each other.
 - the VLAN networks to access the external network.
- 3 Configure the Cisco switch to support VLAN tags.
- 4 Test the implementation.

Configuring the FortiGate-300 unit

Start the FortiGate web-based manager to configure the FortiGate-300 unit.

Configuring the external interface - web-based manager

- 1 Go to **System > Network > Interface**.
- 2 Select Edit on the external interface.

- 3 Enter the following information for the external interface and select OK:

Addressing mode	Manual
IP/Netmask	172.16.21.2/255.255.255.0
Configure other fields as required.	

Configuring 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 - web-based manager

- 1 Go to **System > Network > Interface**.
- 2 Select Create New.
- 3 Enter the following information for VLAN_100 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
Configure other fields as required.	

- 4 Select Create New.
- 5 Enter the following information for VLAN_200 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
Configure other fields as required.	

Figure 5: VLAN subinterfaces

Name	IP	Netmask	Access	Status	
▼ internal	172.20.120.128	255.255.255.0	HTTPS,PING,SSH	Bring Down	
VLAN_100	10.1.1.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down	
VLAN_200	10.1.2.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down	
external	172.16.21.2	255.255.255.0		Bring Down	
dmz/ha	10.10.10.1	255.255.255.0	HTTPS,PING	Bring Up	

Adding VLAN subinterfaces - CLI

```

config system interface
  edit VLAN_100
    set interface internal
    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 interface internal
    set vlanid 200
    set mode static
    set ip 10.1.2.1 255.255.255.0
    set allowaccess https ping telnet
  end
end
    
```

Adding the firewall addresses - web-based manager

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.

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

Address Name	VLAN_100_Net
IP Range/Subnet	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
IP Range/Subnet	10.1.2.0/255.255.255.0

Figure 6: Firewall addresses

Create New		
Name	Address	
all	0.0.0.0/0.0.0.0	
VLAN_100_Net	10.1.1.0/255.255.255.0	
VLAN_200_Net	10.1.2.0/255.255.255.0	

Adding 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 - web-based manager

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

Interface/Zone	Source: VLAN_100, Destination: VLAN_200
Address Name	Source: VLAN_100_Net, Destination: VLAN_200_Net
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

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

Interface/Zone	Source: VLAN_200, Destination: VLAN_100
Address Name	Source: VLAN_200_Net, Destination: VLAN_100_Net
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

- 6 Select **Create New**.

7 Enter the following information and select OK:

Interface/Zone	Source: VLAN_100, Destination: external
Address Name	Source: VLAN_100_Net, Destination: all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

8 Select Create New.

9 Enter the following information and select OK:

Interface/Zone	Source: VLAN_200, Destination: external
Address Name	Source: VLAN_200_Net, Destination: all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

Adding the firewall policies - CLI

```

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

```
edit 3
    set srcintf VLAN_100
    set dstintf external
    set srcaddr VLAN_100_Net
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
next

edit 4
    set srcintf VLAN_200
    set dstintf external
    set srcaddr VLAN_200_Net
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
end
```

Configuring the Cisco switch

On the Cisco Catalyst 2900 ethernet 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.

Configuring 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 (`tracert`, `ping`) to test traffic routed through the FortiGate unit and the Cisco switch.

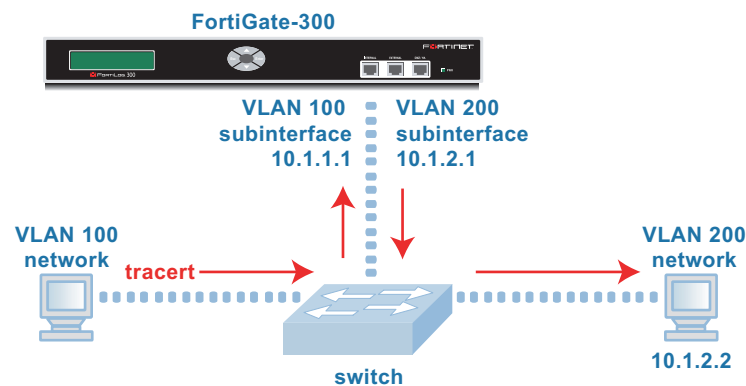
Testing traffic from VLAN 100 to VLAN 200

In this example, a route is traced between the two internal networks. The route target is a host on VLAN 200.

From VLAN 100, access a 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 7: Example trace route from VLAN 100 to VLAN 200



Testing traffic from VLAN 100 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-300 unit.

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

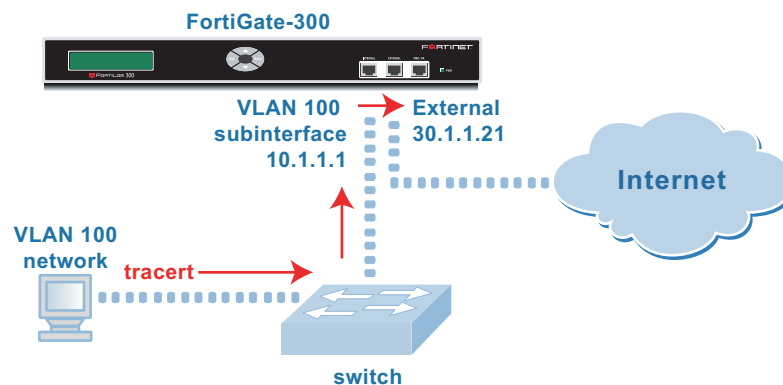
```
C:\>tracert 172.16.21.2
```

Tracing route to 172.16.83.1 over a maximum of 30 hops:

```
 1  <10 ms  <10 ms  <10 ms  10.1.1.1
 2  <10 ms  <10 ms  <10 ms  172.16.21.2
```

Trace complete.

Figure 8: Example trace route from VLAN 100 to the external network



Example configuration NAT/Route mode (complex)

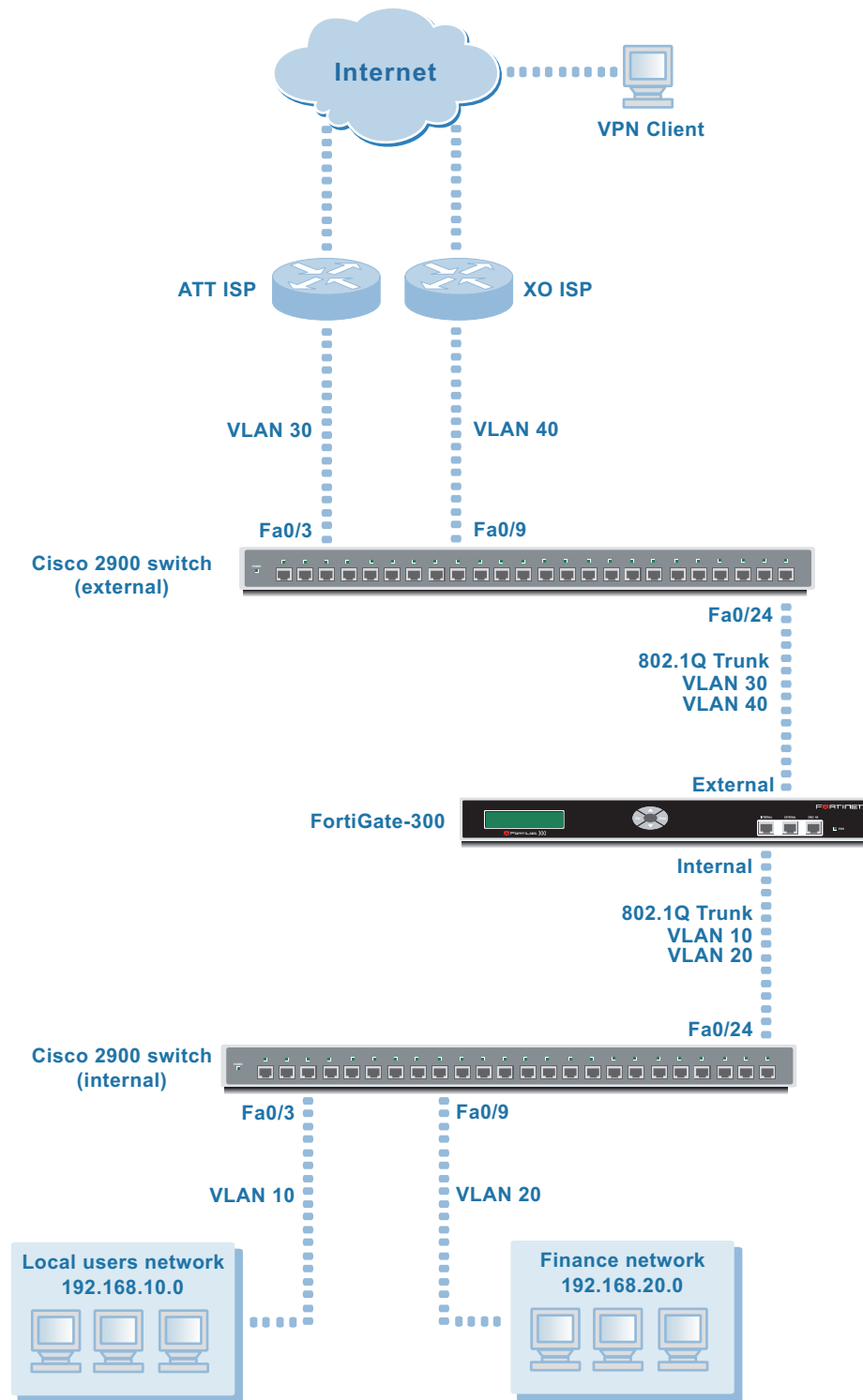
In this example, a FortiGate-300 unit operates in NAT/Route mode. Its network interfaces are configured as follows:

- The internal interface is configured with two VLAN subinterfaces: VLAN 10 for the Local users network and VLAN 20 for the Finance network. The internal interface connects to a Cisco 2900 switch using an 801.1Q trunk.
- The external interface is configured with two VLAN subinterfaces: VLAN 30 for the ATT ISP network and VLAN 40 for the XO ISP network. The internal interface connects to a Cisco 2900 switch using an 801.1Q trunk.

The FortiGate-300 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.

This section describes how to configure a FortiGate-300 unit and two 802.1Q-compliant switches for the example network topology shown in [Figure 9](#).

Figure 9: Example VLAN topology (FortiGate unit in NAT/Route mode)



General configuration steps

- 1 Configure VLANs on the FortiGate-300 unit.
 - Add the four VLAN subinterfaces.
 - Configure a default route.
 - Add addresses for the VLAN subinterfaces.
 - Add firewall policies to allow:
 - the Finance network to access the external network.
 - the Finance network to access the Local users network.
 - the Local users network to access the external networks.
- 2 Configure the FortiGate-300 IPsec VPN tunnel and encrypt policy.
- 3 Configure the VPN client.
- 4 Configure the Cisco switches.
- 5 Test the implementation.

Configuring the FortiGate-300 unit

Start the web-based manager to configure the FortiGate-300 unit.

Adding 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	192.168.20.1/255.255.255.0
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 10: VLAN subinterfaces

Name	IP	Netmask	Access	Status
internal	172.20.120.128	255.255.255.0	HTTPS,PING,SSH	Bring Down
Local-LAN	192.168.10.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down
Finance	192.168.20.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down
external	172.16.21.2	255.255.255.0	PING	Bring Down
ATT-ISP	30.1.1.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down
XO-ISP	40.1.1.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down
dmz/ha	10.10.10.1	255.255.255.0	HTTPS,PING	Bring Up

Adding the VLAN subinterfaces - CLI

```

config system interface
  edit Local-LAN
    set interface internal
    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 interface internal
    set vlanid 20
    set mode static
    set ip 192.168.20.1 255.255.255.0
    set allowaccess https ping telnet
  next

```

```

edit ATT-ISP
  set interface external
  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 interface external
  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 - web-based manager

- 1 Go to **Router > Static**.
- 2 Select Create New to add a new route.
- 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
Gateway	30.1.1.2
Device	ATT-ISP
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
Gateway	40.1.1.2
Device	XO-ISP
Distance	20

Adding a default route - CLI

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

Adding the firewall addresses - web-based manager

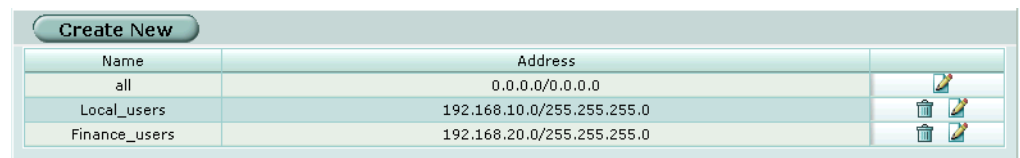
- 1 Go to **Firewall > Address**.
- 2 Select Create New.
- 3 Enter the following information and select OK:

Address Name	Local_users
IP Range/Subnet	192.168.10.0/255.255.255.0

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

Address Name	Finance_users
IP Range/Subnet	192.168.20.0/255.255.255.0

Figure 11: firewall addresses



Adding 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 192.168.20.0 255.255.255.0
end
```

Adding the firewall policies - web-based manager

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

Interface/Zone Source	Finance
Interface/Zone Destination	ATT-ISP
Address Name Source	Finance_users
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

- 4 Go to **Firewall > Policy > Finance -> XO-ISP**.
- 5 Select Create New.
- 6 Enter the following information and select OK:

Interface/Zone Source	Finance
Interface/Zone Destination	XO-ISP
Source	Finance_users
Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

- 7 Go to **Firewall > Policy**.
- 8 Select Create New.

9 Enter the following information and select OK:

Interface/Zone Source	Finance
Interface/Zone Destination	Local-LAN
Source	Finance_users
Destination	Local_users
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

10 Go to **Firewall > Policy**.

11 Select Create New.

12 Enter the following information and select OK:

Interface/Zone Source	Local-LAN
Interface/Zone Destination	ATT-ISP
Source	Local_users
Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	





















13 Go to **Firewall > Policy > Local-LAN -> XO-ISP**.

14 Select Create New.

15 Enter the following information and select OK:

Interface/Zone Source	Local-LAN
Interface/Zone Destination	XO-ISP
Source	Local_users
Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Select
Configure other fields as required.	

The list of firewall policies looks like this:

ID	Source	Dest	Schedule	Service	Action	Enable	
Create New							
Local-LAN -> ATT-ISP (1)							
4	Local_users	ATT_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	   
Local-LAN -> XO-ISP (1)							
5	Local_users	XO_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	   
Finance -> Local-LAN (1)							
3	Finance_users	Local_users	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	   
Finance -> ATT-ISP (1)							
1	Finance_users	ATT_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	   
Finance -> XO-ISP (1)							
2	Finance_users	XO_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	   

Adding the firewall policies - CLI

```

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

  edit 2
    set srcintf Finance
    set dstintf XO-ISP
    set srcaddr Finance_users
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
  next

  edit 3
    set srcintf Finance
    set dstintf Local-LAN
    set srcaddr Finance_users
    set dstaddr Local_users
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
  next

```

```
edit 4
    set srcintf Local-LAN
    set dstintf ATT-ISP
    set srcaddr Local_users
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
end

edit 5
    set srcintf Local-LAN
    set dstintf XO-ISP
    set srcaddr Local_users
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
```

Configuring the FortiGate-300 IPSec VPN tunnel and encrypt policy

In this example, one user is allowed to connect to the Local user network through a VPN tunnel from an external dial-up connection. To enable this, you need to do the following:

- Configure the VPN gateway.
- Configure the VPN tunnel.
- Define the IP address for the VPN user on the Local users network.
- Add the encrypt firewall policy to enable the connection.

Configuring the VPN gateway - web-based manager

- 1 Go to **VPN > IPSEC > Phase 1**.
- 2 Select Create New and then select Advanced.

- 3 Enter the following information, then select OK:

Gateway Name	Dialup_tunnel
Remote Gateway	Dialup User
Mode	Aggressive
Authentication Method	Preshared key
Pre-shared key	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. The client must use the same pre-shared key.
P1 Proposal	1-Encryption 3DES, Authentication SHA1 2-Encryption 3DES, Authentication MD5
DH Group	5
Keylife	28800 (seconds)
Configure other fields as required.	

Configuring the VPN gateway - CLI

```
config vpn ipsec phase1
  edit Dialup_tunnel
    set type dynamic
    set mode aggressive
    set authmethod psk
    set psksecret <pre-shared key>
    set proposal 3des-sha1 3des-md5
    set dhgrp 5
    set keylife 28800
  end
```

Configuring the VPN tunnel - web-based manager

- 1 Go to **VPN > IPSEC > Phase 2**.
- 2 Select Create New and then select Advanced.

- 3 Enter the following information, then select OK:

Tunnel Name	Dialup-client
Remote Gateway	Dialup_tunnel
P2 Proposal	1-Encryption 3DES, Authentication SHA1 2-Encryption 3DES, Authentication MD5
Enable replay detection	Select
Enable perfect forward frequency	Select
DH Group	5
Keylife	1800 (seconds)
Autokey Keep Alive	Select
Quick Mode Identities	Use selectors from policy
Configure other fields as required.	

Configuring the VPN tunnel - CLI

```

config vpn ipsec phase2
  edit Dialup-client
    set phase1name Dialup_tunnel
    set proposal 3des-sha1 3des-md5
    set replay enable
    set pfs enable
    set dhgrp 5
    set keylife_type seconds
    set keylifeseconds 1800
    set keepalive enable
  end
    
```

Defining the VPN user IP address - web-based users

The destination address used in the firewall policy determines the acceptable source address range for the remote VPN user. To allow the user to use the VPN from any host, the firewall policy could specify the “all” firewall address. This example requires that the remote user can only use the ATT-ISP network.

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

Address Name	ATT-net
IP Range/Subnet	30.1.1.0/255.255.255.0

Defining the VPN user IP address - CLI

```
config firewall address
  edit VIP_IP
    set type ipmask
    set start_ip 30.1.1.0 255.255.255.0
  end
```

Adding the encrypt policy - web-based manager

- 1 Go to **Firewall > Policy**.
- 2 Select **Create New**.
- 3 Enter the following information, then select **OK**:

Interface/Zone Source	Local-LAN
Interface/Zone Destination	ATT-ISP
Address Name/Source	Local-users
Address Name/Destination	ATT-net
Schedule	Always
Service	Any
Action	ENCRYPT
VPN Tunnel	Dialup-client
Allow Inbound	Select
Allow Outbound	Clear
Configure other fields as required.	

- 4 Place 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.

Adding the encrypt policy - CLI

```
config firewall policy
  edit 6
    set srcintf Local-LAN
    set dstintf ATT-ISP
    set srcaddr Local_users
    set dstaddr ATT-net
    set schedule always
    set service ANY
    set action encrypt
    set vpngroup Dialup-client
    set inbound enable
    set outbound disable
    set natinbound disable
    set natoutbound disable
    set status enable
  end
```

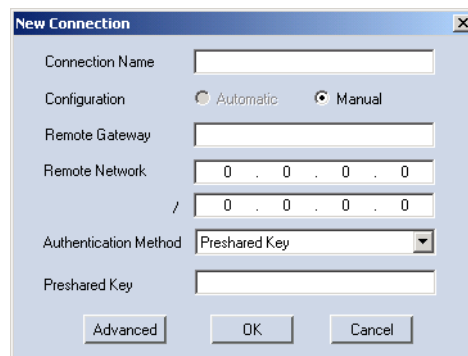
Configuring the VPN client

The Local users network allows a single inbound connection from a VPN client on the ATT ISP network. This example shows how to configure FortiClient for this purpose.

Creating a new VPN connection

- 1 Start FortiClient.
- 2 Go to **VPN > Connections** and select Add.

Figure 12: New VPN Connection

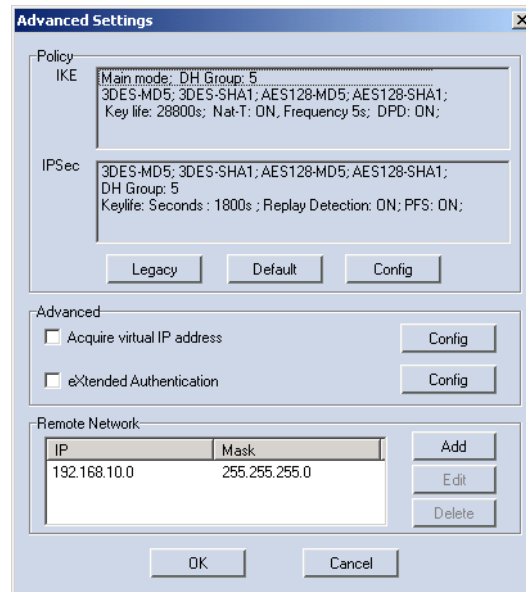


- 3 Type a name for the connection in the Connection Name field.
- 4 In the Remote Gateway IP address box, enter 30.1.1.1.
- 5 In the Remote Network address box, enter 192.168.10.0/255.255.255.0.
- 6 From the Authentication Method box select Preshared Key.
- 7 Type the pre-shared key in the Pre-Shared Key field.



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

- 8 Select Advanced.

Figure 13: Advanced Settings

- 9 Select **Acquire virtual IP address** and then select **Config**.
The **Virtual IP Acquisition** dialog box opens.
- 10 Select **Manually Set**.
- 11 Enter the following information and select **OK**.

IP	30.1.1.0
Subnet mask	255.255.255.0

- 12 Select **OK** and then select **OK** again to complete configuration of the VPN connection.

Configuring the internal Cisco switch

On the Cisco Catalyst 2900 ethernet switch connected to the internal interface, you need to define VLANs 10 and 20 in the VLAN database and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

Configuring the VLAN subinterfaces and the trunk interfaces

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 Cisco switch

On the Cisco Catalyst 2900 ethernet switch connected to the external interface, you need to define VLANs 30 and 40 in the VLAN database and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

Configuring the VLAN subinterfaces and the trunk interfaces

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

Use diagnostic commands (`tracert`, `ping`) to test traffic routed through the FortiGate unit and the Cisco switch.

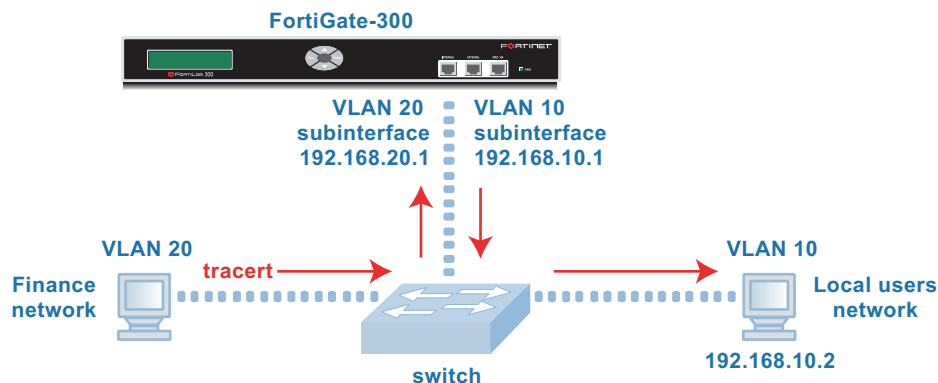
Testing traffic from VLAN 20 to VLAN 10

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 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 14: Example trace route from VLAN 20 to VLAN 10



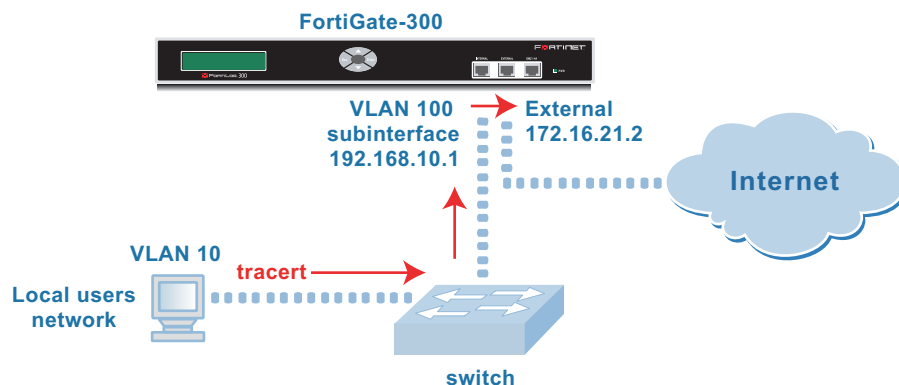
Testing traffic from VLAN 10 to the external network

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-300 unit.

From the Local users network (VLAN 10), 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  192.168.10.1
  2  <10 ms  <10 ms  <10 ms  172.16.21.2
Trace complete.
```

Figure 15: Example trace route from VLAN 10 to the external network



Using VDOMs in NAT/Route mode

Overview

Virtual Domains split your FortiGate unit into multiple separate units so that it can serve multiple organizations. Each VDOM has separate routing and firewall policies. Each interface, physical or VLAN, belongs exclusively to one virtual domain. This simplifies administration because you can see only the interfaces, routing tables and firewall policies for the VDOM you are configuring.

For more information about which parts of the configuration are domain-specific and which are global, see [“Global and virtual domain properties” on page 17](#).

Adding virtual domains

The FortiGate-300 supports two virtual domains in NAT/Route mode. The root domain is the default domain, which cannot be deleted or renamed.

To create a new virtual domain

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Create New.
- 3 Type a name in the Virtual Domain Name field and select OK.

Administration of virtual domains

Virtual domains share a common administrative model. Administrators have access to all of the virtual domains on the FortiGate unit. Administrators logging into the CLI or web-based manager always log into the root domain and then must enter the virtual domain that they want to administer.

To select a virtual domain to configure

- 1 Go to **System > Virtual domain > Virtual domains**.

Figure 16: List of virtual domains

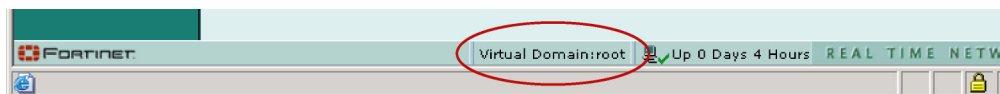
Create New			
Current: root [change]		Management: root [change]	
Max Virtual Domains: 2			
Name	Current	Management	
root	✓	✓	
domain2			🗑️

- 2 Select Change following the current virtual domain name above the table.

- 3 Choose the virtual domain to configure.
- 4 Select OK.

The footer of the web-based manager page displays the currently selected virtual domain name if the information and configuration options on the page are exclusive to the virtual domain. Otherwise, the footer displays “Virtual Domain: all”.

Figure 17: Status line virtual domain indicator



The virtual domain indicator is not shown if only the root domain exists.

Configuring virtual domains

The following procedures explain how to configure virtual domains:

- [Adding interfaces and VLAN subinterfaces to a virtual domain](#)
- [Configuring routing for a virtual domain](#)
- [Configuring firewall policies for a virtual domain](#)
- [Configuring VPNs for a virtual domain](#)

Adding interfaces and VLAN subinterfaces to a virtual domain

A virtual domain must contain at least two interfaces. These can be physical interfaces or VLAN interfaces. By default all physical interfaces are in the root virtual domain and when you create a new VLAN, the default virtual domain is root.

To add a VLAN subinterface to a virtual domain

- 1 Go to **System > Network > Interface**.
- 2 Select Create New to add a VLAN subinterface.
- 3 Enter a Name to identify the VLAN subinterface.
- 4 Select the physical interface that receives the VLAN packets intended for this VLAN subinterface.
- 5 Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.
- 6 Select the virtual domain to which to add this VLAN subinterface.
- 7 Configure the VLAN subinterface settings as you would for any FortiGate interface.
- 8 Select OK to save your changes.

The FortiGate unit adds the new VLAN subinterface to the interface that you selected in step 4.

To view the interfaces in a virtual domain

- 1 Go to **System > Network > Interface**.
- 2 Choose the Virtual domain you want to view.
The interfaces added to this virtual domain are listed.

The following procedure describes how to move an interface from one virtual domain to another. You cannot remove an interface from a virtual domain if firewall policies have been added for it. Delete the firewall policies or remove the interface from the firewall policies first.

To move an existing interface to another virtual domain

- 1 Go to **System > Network > Interface**.
- 2 Set Virtual domain to All or to the name of the virtual domain that currently contains the interface.
- 3 Select Edit for the physical interface you want to move.
- 4 Choose the Virtual Domain to which to move the interface.
- 5 Select OK.
The interface moves to the virtual domain. Firewall IP pools and virtual IPs added for this interface are deleted. You should manually delete any routes that include this interface.

Configuring routing for a virtual domain**To configure routing for a virtual domain**

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure routing.
- 4 Select OK.
- 5 Go to **Router**.
- 6 Configure routing for the current virtual domain as required.
The routing you define applies only to network traffic entering interfaces belonging to this virtual domain.

Configuring firewall policies for a virtual domain**To add firewall addresses to a virtual domain**

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure firewall addresses.
- 4 Select OK.
- 5 Go to **Firewall > Address**.
- 6 Add new firewall addresses, address ranges, and address groups to the current virtual domain.

To configure firewall policies for a virtual domain

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure firewall policies.
- 4 Select OK.
- 5 Go to **Firewall > Policy**.
- 6 Select Create new to add firewall policies to the current virtual domain.
Your firewall policies can involve only the interfaces, zones and firewall addresses that are in the current virtual domain. The firewall policies that you add are only visible when you are viewing the current virtual domain. Network traffic accepted by the interfaces and VLAN subinterfaces in this virtual domain is controlled by the firewall policies in this virtual domain

To add IP pools to a virtual domain

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure firewall IP pools.
- 4 Select OK.
- 5 Go to **Firewall > IP Pool**.
- 6 Add new IP pools as required for the current virtual domain.

To add Virtual IPs to a virtual domain

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure virtual IPs.
- 4 Select OK.
- 5 Go to **Firewall > Virtual IP**.
- 6 Add new virtual IPs as required for the current virtual domain.

Configuring VPNs for a virtual domain

Configurations for IPSec, PPTP and L2TP are VDOM-specific. Certificates are shared by all virtual domains.

To configure VPN for a virtual domain

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure VPN.
- 4 Select OK.
- 5 Go to **VPN**.
- 6 Configure IPSec VPN, PPTP, L2TP, and certificates as required.

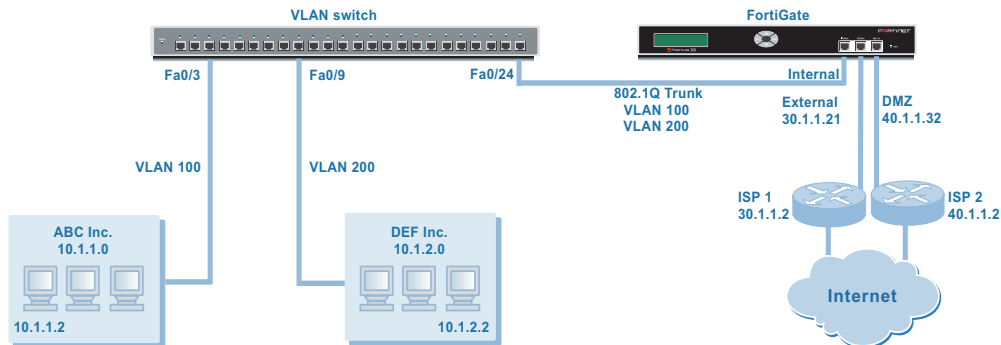
Example VDOM configuration in NAT/Route mode (simple)

Figure 18 shows a simplified NAT/Route mode VLAN configuration in which a FortiGate unit provides Internet access with real time network protection for two organizations. Inside the FortiGate unit, each organization has its own virtual domain, enabling separate configuration of network protection profiles.

A Cisco 2900 VLAN switch combines the LANs of the two organizations into an 802.1Q trunk that connects to the Internal interface of the FortiGate-300 unit. There are two VLAN subinterfaces on the Internal interface, one for VLAN 100 and one for VLAN 200.

The external and DMZ interfaces of the FortiGate unit connect to the Internet through different ISPs, one for each organization. These interfaces are not configured with VLAN subinterfaces.

Figure 18: FortiGate unit in Nat/Route mode



When the Cisco switch receives packets from VLAN 100 and VLAN 200, it applies VLAN ID tags and forwards the packets across the trunk to the FortiGate unit. The FortiGate unit has policies that allow traffic to flow from VLAN 100 to the external network and from VLAN 200 to the DMZ network.

This section describes how to configure a FortiGate-300 unit and a Cisco 2900 switch for this example network topology.

General configuration steps

- 1 Create virtual domains.
- 2 Configure the FortiGate-300 external and DMZ interfaces.
- 3 Configure each virtual domain on the FortiGate-300 unit:
 - Add a VLAN subinterface to the Internal network interface.
 - Add Firewall addresses and address ranges for the internal and external networks.
 - Add a firewall policy to allow the VLAN to access the external network.
 - Configure the default route to the ISP.
- 4 Configure the Cisco switch to support VLAN tags.
- 5 Test the implementation.

Creating virtual domains

In this example, the root domain is used for company ABC. A new virtual domain, vdomain2, is created to serve the needs of company DEF.

Creating the vdomain2 virtual domain

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Create New.
- 3 Type "vdomain2" in the Virtual Domain Name field and select OK.

Configuring the FortiGate-300 external and DMZ interfaces

Start the FortiGate web-based manager to configure the FortiGate-300 unit.

Configuring the external interface - web-based manager

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

Virtual domain	root
Addressing mode	Manual
IP/Netmask	30.1.1.21/255.255.255.0
Configure other fields as required.	

Configuring the external interface - CLI

```

config system interface
  edit external
    set vdom root
    set mode static
    set ip 30.1.1.21 255.255.255.0
  end
    
```

Configuring the DMZ interface - web-based manager

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

Virtual domain	vdomain2
Addressing mode	Manual
IP/Netmask	40.1.1.32/255.255.255.0
Configure other fields as required.	

Configuring the DMZ interface - CLI

```
config system interface
edit dmz/ha
set vdom vdomain2
set mode static
set ip 40.1.1.32 255.255.255.0
end
```

Configuring the root virtual domain

In this example, the root domain is used for company ABC. You configure it with a VLAN subinterface for VLAN_100 and a firewall policy to allow connection to the External interface.

Adding the VLAN 100 subinterface - web-based manager

- 1 Go to **System > Network > Interface**.
- 2 Select Create New.
- 3 Enter the following information for VLAN_100 and select OK:

Name	VLAN_100
Interface	internal
VLAN ID	100
Virtual Domain	root
Addressing mode	Manual
IP/Netmask	10.1.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET
Configure other fields as required.	

Figure 19: root domain interfaces and subinterfaces

Name	IP	Netmask	Access	Status
internal	172.20.120.128	255.255.255.0	HTTPS,PING,SSH	Bring Down
VLAN_100	10.1.1.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down
external	30.1.1.21	255.255.255.0	PING	Bring Down

Adding VLAN 100 subinterface - CLI

```
config system interface
edit VLAN_100
set interface internal
set vlanid 100
set vdom root
set mode static
set ip 10.1.1.1 255.255.255.0
set allowaccess https ping telnet
end
```

Selecting the root virtual domain - web-based manager

Before you follow the rest of the procedure for configuring VLAN 100, you must ensure that the current domain is root.

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the root virtual domain.

Selecting the root virtual domain - CLI

```
execute enter root
```

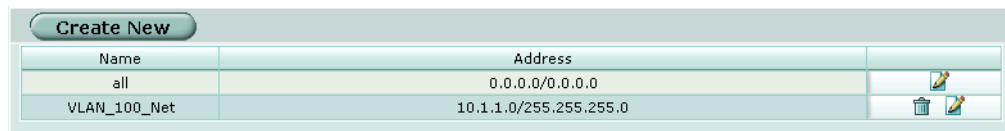
Adding root domain firewall addresses - web-based manager

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.

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

Address Name	VLAN_100_Net
IP Range/Subnet	10.1.1.0/255.255.255.0

Figure 20: root domain firewall addresses



Adding the root domain firewall addresses - CLI

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

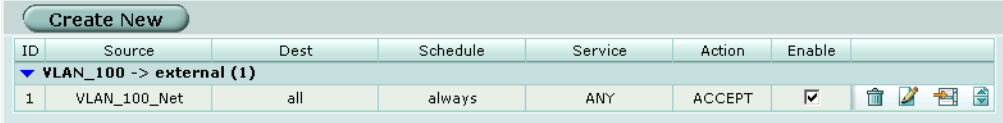
Adding the root domain firewall policy - web-based manager

- 1 Go to **Firewall > Policy**.
- 2 Select Create New.

- 3 Enter the following information and select OK:

Interface/Zone	Source: VLAN_100, Destination: external
Address Name	Source: VLAN_100_Net, Destination: all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Configure other fields as required.	

Figure 21: root domain firewall policy



ID	Source	Dest	Schedule	Service	Action	Enable
▼ VLAN_100 -> external (1)						
1	VLAN_100_Net	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>

Adding the firewall policy - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_100
    set dstintf external
    set srcaddr VLAN_100_Net
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
  end
```

Adding a default route - web-based manager

You need to define a default route to direct packets to the ISP if their destination is outside of the VLAN 100 subnet.

- 1 Go to **Router > Static**.
- 2 Select Create New to add a new route.
- 3 Enter the following information to add a default route to ISP1 for network traffic leaving the external interface and select OK:

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	30.1.1.2
Device	external
Distance	10

Figure 22: root domain routing table

Create New						
#	IP	Mask	Gateway	Device	Distance	
1	0.0.0.0	0.0.0.0	30.1.1.2	external	10	

Adding a default route - CLI

```
config router static
edit 1
set device external
set gateway 30.1.1.2
end
```

Configuring the vdomain2 virtual domain

In this example, the vdomain2 domain is used for company DEF. You configure it with a VLAN subinterface for VLAN_200 and a firewall policy to allow connection to the External interface.

Adding the VLAN 200 subinterface - web-based manager

- 1 Select Create New.
- 2 Enter the following information for VLAN_200 and select OK:

Name	VLAN_200
Interface	internal
VLAN ID	200
Virtual Domain	vdomain2
Addressing mode	Manual
IP/Netmask	10.1.2.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET
Configure other fields as required.	

Figure 23: vdomain2 interfaces and subinterfaces

Create New							Virtual Domain: vdomain2
Name	IP	Netmask	Access	Status			
▼ internal	172.20.120.128	255.255.255.0	HTTPS,PING,SSH	Bring Down			
VLAN_200	10.1.2.1	255.255.255.0	HTTPS,PING,TELNET	Bring Down			
dmz/ha	40.1.1.32	255.255.255.0	HTTPS,PING	Bring Down			

Adding VLAN 200 subinterface - CLI

```
config system interface
edit VLAN_200
set interface internal
set vlanid 200
set vdom vdomain2
set mode static
set ip 10.1.2.1 255.255.255.0
set allowaccess https ping telnet
end
```

Selecting the vdomain2 virtual domain - web-based manager

Before you follow the rest of the procedure for configuring VLAN 200, you must ensure that the current domain is vdomain2.

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the vdomain2 virtual domain.

Selecting the vdomain2 virtual domain - CLI

```
execute enter vdomain2
```

Adding the vdomain2 firewall address - web-based manager

You need to define the addresses of the VLAN 200 subnets for use in firewall policies. In the root 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.

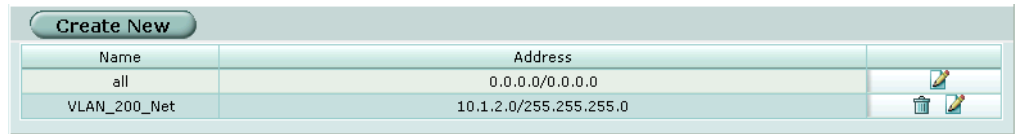
- 1 Go to **Firewall > Address**.
- 2 Select Create New.
- 3 Enter the following information and select OK:

Address Name	all
IP Range/Subnet	0.0.0.0/0.0.0.0

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

Address Name	VLAN_200_Net
IP Range/Subnet	10.1.2.0/255.255.255.0

Figure 24: Firewall addresses for vdomain2



Adding the vdomain2 firewall address - CLI

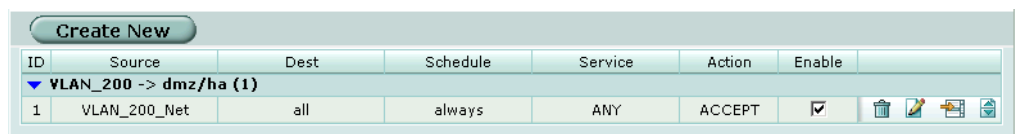
```
config firewall address
edit VLAN_200_Net
set type ipmask
set subnet 10.1.2.0 255.255.255.0
end
```

Adding the vdomain2 firewall policy - web-based manager

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

Interface/Zone	Source: VLAN_200, Destination: dmz/ha
Address Name	Source: VLAN_200_Net, Destination: all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Configure other fields as required.	

Figure 25: vdomain2 firewall policy



Adding the vdomain2 firewall policy - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_200
    set dstintf dmz/ha
    set srcaddr VLAN_200_Net
    set dstaddr all
    set schedule always
    set service ANY
    set action accept
    set nat enable
    set status enable
  end
```

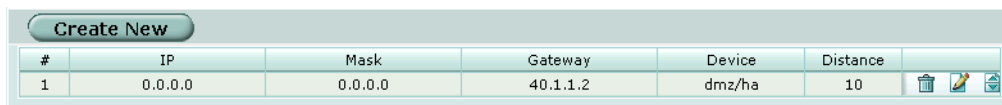
Adding a default route - web-based manager




You need to define a default route to direct packets to the ISP if their destination is outside of the VLAN 200 subnet.

- 1 Go to **Router > Static**.
- 2 Select Create New to add a new route.
- 3 Enter the following information to add a default route to ISP2 for network traffic leaving the external interface and select OK:

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	40.1.1.2
Device	dmz/ha
Distance	10

Figure 26: vdomain2 routing table



Create New						
#	IP	Mask	Gateway	Device	Distance	
1	0.0.0.0	0.0.0.0	40.1.1.2	dmz/ha	10	  

Adding a default route - CLI

```
config router static
  edit 1
    set device external
    set gateway 40.1.1.2
  end
```

Configuring the Cisco switch

On the Cisco Catalyst 2900 ethernet 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.

Configuring 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 (*tracert*, *ping*) to test traffic routed through the FortiGate unit and the Cisco switch.

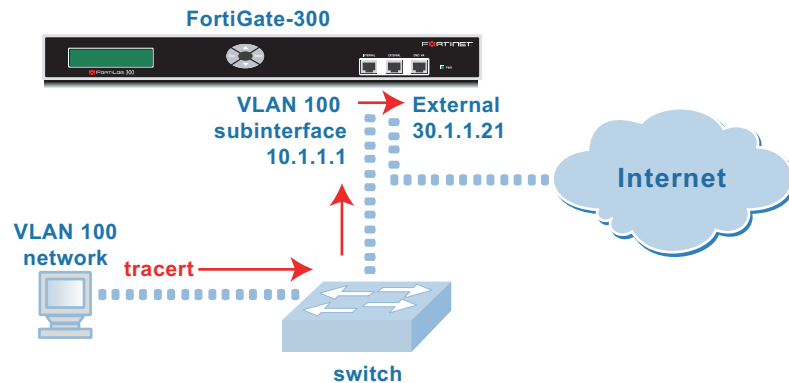
Testing traffic from VLAN 100 to the external network

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-300 unit.

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

```
C:\>tracert 30.1.1.21
Tracing route to 30.1.1.21 over a maximum of 30 hops:
  1  <10 ms  <10 ms  <10 ms  10.1.1.1
  2  <10 ms  <10 ms  <10 ms  30.1.1.21
Trace complete.
```

Figure 27: Example trace route from VLAN 100 to the external network



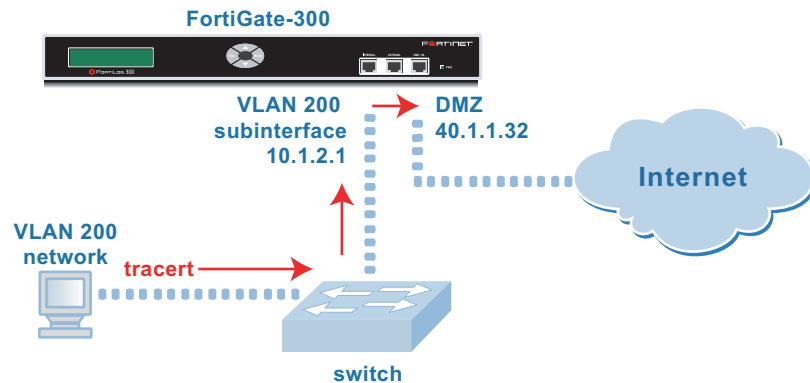
Testing traffic from VLAN 200 to the DMZ network

In this example, a route is traced from an internal network to the external network. The route target is the DMZ network interface of the FortiGate-300 unit.

From VLAN 200, access a command prompt and enter this 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  10.1.2.1
  2  <10 ms  <10 ms  <10 ms  40.1.1.32
Trace complete.
```

Figure 28: Example trace route from VLAN 200 to the DMZ network



Example VDOM configuration in NAT/Route mode (complex)

In this example, a FortiGate-300 unit operates in NAT/Route mode, serving two organizations. Two virtual domains are used. The root domain serves a school with student and instructor networks. The second domain, Commercial, serves a business with product development and sales networks. The internal and external interfaces of the FortiGate unit are connected to Cisco switches through 801.1Q trunks that carry the traffic for both virtual domains.

[Figure 29](#) illustrates this network topology. This remainder of the chapter describes how to configure a FortiGate-300 unit and two 802.1Q-compliant switches for this topology.

The root domain is configured as follows:

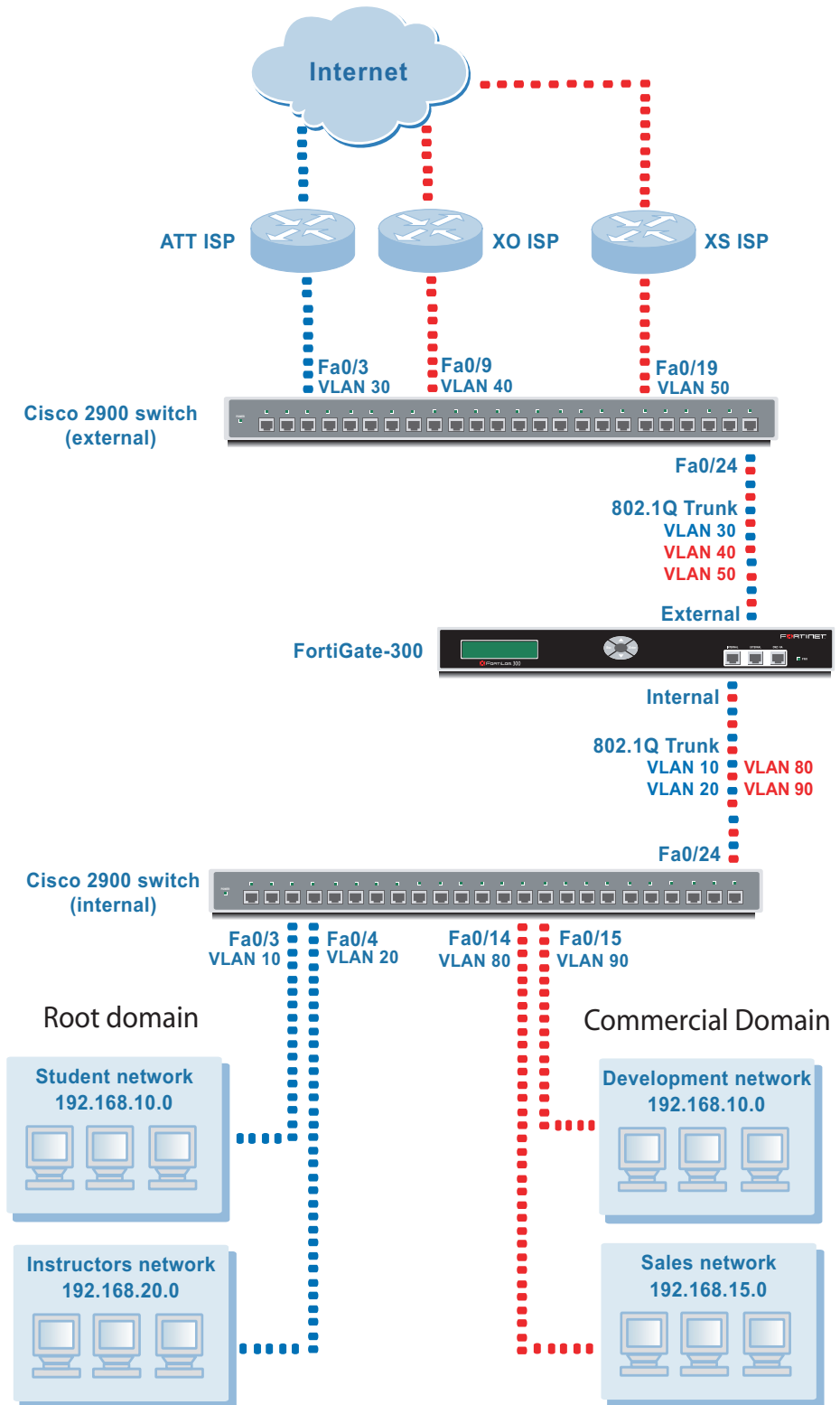
- The internal interface is configured with two VLAN subinterfaces: VLAN 10 for the students network and VLAN 20 for the instructors network.
- The external interface is configured with a VLAN subinterface, VLAN 30, for the ATT-ISP network.
- Firewall policies allow both the instructors and students networks to access the internet through the ATT-ISP network. For students there is a more strict protection profile governing their online activities.
- A firewall policy allows instructors access to the students network.

The Commercial domain is configured as follows:

- The internal interface is configured with two VLAN subinterfaces: VLAN 80 for the Sales network and VLAN 90 for the Development network.
- The external interface is configured with two VLAN subinterfaces, VLAN 40 and VLAN 50, for access to the Internet via the redundant XO-ISP and XS-ISP networks.
- Firewall policies allow access to the Internet through the XO-ISP and XS-ISP networks from both Sales and Development networks.
- Firewall policies allow access from the Sales network to the Development network and from the Development network to the Sales network.

You might have noticed that the Student network and the Development network have the same network address ranges. This does not cause a problem because the two address ranges reside in different virtual domains.

Figure 29: Example VLAN/VDOM topology (FortiGate unit in NAT/Route mode)



General configuration steps

- 1 Create the Commercial domain.
- 2 Configure the root domain:
 - Add the VLAN subinterfaces.
 - Configure a default route.
 - Add firewall addresses for the networks connected to the VLANs.
 - Add firewall policies to allow:
 - the instructors network to access the students network
 - the instructors network to access the external network
 - the students network to access the external network with a strict protection profile
- 3 Configure the Commercial domain:
 - Add the VLAN subinterfaces.
 - Configure a default route and a secondary default route.
 - Add firewall addresses for the VLANs.
 - Add firewall policies to allow:
 - the development network to access the sales network
 - the sales network to access the development network
 - the sales network to access the external network
 - the development network to access the external network
- 4 Configure the Cisco switches.
- 5 Test the implementation.

Creating the virtual domains

The root domain is present by default and cannot be deleted. You need to create the Commercial domain.

To create the Commercial virtual domain - web-based manager

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Create New.
- 3 Type "Commercial" in the Virtual Domain Name field and select OK.

To create the Commercial virtual domain - CLI

```
config system vdom
edit Commercial
end
```

Configuring the root domain

Start the web-based manager to configure the FortiGate-300 unit.

Selecting the root virtual domain

Before you follow the rest of the procedures for configuring the root domain, you must ensure that the current domain is root.

To select the root virtual domain - web-based manager

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the root virtual domain.

To select the root virtual domain - CLI

```
execute enter root
```

Adding the VLAN subinterfaces

In the root VDOM, you need two VLAN subinterfaces on the internal physical interface to receive the VLAN 10 and VLAN 20 packets from the students and instructors 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 Go to **System > Network > Interface**.
- 2 Select Create New.
- 3 Enter the following information for the students network and select OK:

Name	students
Interface	internal
VLAN ID	10
Virtual Domain	root
Addressing mode	Manual
IP/Netmask	192.168.10.1/255.255.255.0
Configure other fields as required.	

- 4 Select Create New.

- 5 Enter the following information for the instructors network and select OK:

Name	instructors
Interface	internal
VLAN ID	20
Virtual Domain	root
Addressing mode	Manual
IP/Netmask	192.168.20.1/255.255.255.0
Configure other fields as required.	

- 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
Virtual Domain	root
Addressing mode	Manual
IP/Netmask	30.1.1.1/255.255.255.0
Configure other fields as required.	

Figure 30: VLAN subinterfaces for root VDOM

Name	IP	Netmask	Access	Status
▼ internal	172.20.120.128	255.255.255.0	HTTPS,PING,SSH	Bring Down
students	192.168.10.1	255.255.255.0		Bring Down
instructors	192.168.20.1	255.255.255.0		Bring Down
▼ external	192.168.100.99	255.255.255.0		Bring Down
ATT-ISP	30.1.1.1	255.255.255.0		Bring Down
dmz/ha	10.10.10.1	255.255.255.0	HTTPS,PING	Bring Up

To add the VLAN subinterfaces - CLI

```

config system interface
  edit students
    set interface internal
    set vlanid 10
    set vdom root
    set mode static
    set ip 192.168.10.1 255.255.255.0
  next
  edit instructors
    set interface internal
    set vlanid 20
  
```

```

set vdom root
set mode static
set ip 192.168.20.1 255.255.255.0
edit ATT-ISP
set interface external
set vlanid 30
set vdom root
set mode static
set ip 30.1.1.1 255.255.255.0
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 root 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.

The root VDOM initially contains a default route, which you can edit or delete as needed. Newly-created VDOMs provide no initial default route.

To add a default route - web-based manager

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

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

To add a default route - CLI

```

config router static
edit 1
set device ATT-ISP
set gateway 30.1.1.2
next
end

```

Adding the firewall addresses

You need to define the addresses of the root VDOM subnets for use in firewall policies. In the root 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

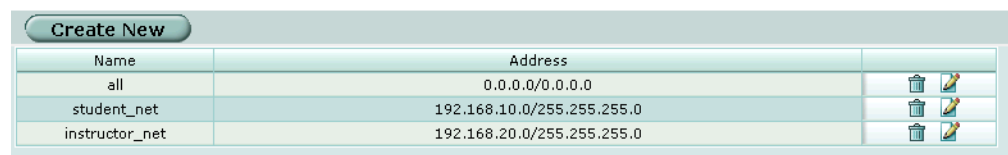
- 1 Go to **Firewall > Address**.
- 2 Select Create New.
- 3 Enter the following information and select OK:

Address Name	student_net
IP Range/Subnet	192.168.10.0/255.255.255.0

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

Address Name	instructor_net
IP Range/Subnet	192.168.20.0/255.255.255.0

Figure 31: Firewall addresses for root domain



To add firewall addresses - CLI

```
config firewall address
  edit all
    set subnet 0.0.0.0 0.0.0.0
  next
  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
end
```

Adding the firewall policies

Each internal network needs a policy to permit it to access the ATT-ISP network 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 protection profiles “strict” and “scan”. You can modify these or create custom protection profiles as needed.

To add firewall policies - web-based manager

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

Interface/Zone Source	students
Interface/Zone Destination	ATT-ISP
Address Name Source	student_net
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Protection profile	strict
Configure other fields as required.	

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

Interface/Zone Source	instructors
Interface/Zone Destination	ATT-ISP
Source	instructor_net
Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Protection profile	scan
Configure other fields as required.	

- 6 Select Create New.

7 Enter the following information and select OK:

Interface/Zone Source	instructors
Interface/Zone Destination	students
Source	instructor_net
Destination	student_net
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Configure other fields as required.	

The list of firewall policies looks like this:

Figure 32: Firewall policies for root VDOM

ID	Source	Dest	Schedule	Service	Action	Enable
▼ students -> ATT-ISP (1)						
1	student_net	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>
▼ instructors -> students (1)						
3	student_net	student_net	always	ANY	ACCEPT	<input checked="" type="checkbox"/>
▼ instructors -> ATT-ISP (1)						
2	instructor_net	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>

To add firewall policies - CLI

```

config firewall policy
  edit 1
    set srcintf students
    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 profile strict
    set nat enable
  next
  edit 2
    set srcintf instructors
    set dstintf ATT-ISP
    set srcaddr instructor_net
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set nat enable
  next
  
```

```
edit 3
  set srcintf instructors
  set dstintf students
  set srcaddr student_net
  set dstaddr student_net
  set action accept
  set schedule always
  set service ANY
  set nat enable
next
end
```

Configuring the Commercial vdomain

Start the web-based manager to configure the FortiGate-300 unit.

Selecting the Commercial virtual domain

Before you follow the rest of the procedure for configuring the Commercial domain, you must ensure that the current domain is Commercial.

To select the Commercial virtual domain - web-based manager

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the Commercial virtual domain.

To select the Commercial virtual domain - CLI

```
execute enter Commercial
```

Adding the VLAN subinterfaces

In the Commercial VDOM, you need two VLAN subinterfaces on the internal physical interface to receive the VLAN 80 and VLAN 90 packets from the Sales and Development networks. You need a VLAN subinterface on the external interface to send packets to the XO-ISP network on VLAN 40.

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 Sales network and select OK:

Name	Sales
Interface	internal
VLAN ID	80
Virtual Domain	Commercial
Addressing mode	Manual
IP/Netmask	192.168.15.1/255.255.255.0
Configure other fields as required.	

- 4 Select Create New.
- 5 Enter the following information for the Development network and select OK:

Name	Development
Interface	internal
VLAN ID	90
Virtual Domain	Commercial
Addressing mode	Manual
IP/Netmask	192.168.10.1/255.255.255.0
Configure other fields as required.	

- 6 Select Create New.
- 7 Enter the following information for the XO ISP network and select OK:

Name	XO-ISP
Interface	external
VLAN ID	40
Virtual Domain	Commercial
Addressing mode	Manual
IP/Netmask	40.1.1.1/255.255.255.0
Configure other fields as required.	

- 8 Select Create New.

- 9 Enter the following information for the XS ISP network and select OK:

Name	XS-ISP
Interface	external
VLAN ID	50
Virtual Domain	Commercial
Addressing mode	Manual
IP/Netmask	145.1.1.1/255.255.255.0
Configure other fields as required.	

Figure 33: VLAN subinterfaces for Commercial VDOM

Create New		Virtual Domain: Commercial				
Name	IP	Netmask	Access	Status		
▼ internal	172.20.120.128	255.255.255.0	HTTPS,PING,SSH	Bring Down		
Sales	192.168.15.1	255.255.255.0		Bring Down		
Development	192.168.10.1	255.255.255.0		Bring Down		
▼ external	192.168.100.99	255.255.255.0	PING	Bring Down		
XO-ISP	40.1.1.1	255.255.255.0		Bring Down		
XS-ISP	145.1.1.1	255.255.255.0		Bring Down		

To add the VLAN subinterfaces - CLI

```

config system interface
  edit Sales
    set interface internal
    set vlanid 80
    set vdom Commercial
    set mode static
    set ip 192.168.15.1 255.255.255.0
  next
  edit Development
    set interface internal
    set vlanid 90
    set vdom Commercial
    set mode static
    set ip 192.168.10.1 255.255.255.0
  next
  edit XO-ISP
    set interface external
    set vlanid 40
    set vdom Commercial
    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 Commercial
  set mode static
  set ip 145.1.1.1 255.255.255.0
end
    
```

Adding a default route

You need to define a default 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 that is connected to the ISP. As this example includes redundant ISPs, you also define a route to the secondary ISP with a greater distance.

To add a default route - web-based manager

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

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

- 4 Select Create New to add a new route.
- 5 Enter the following information to add a secondary default route to XS-ISP for network traffic leaving the external interface from the Commercial domain and select OK:

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	145.1.1.2
Device	XS-ISP
Distance	20

To add a default route - CLI

```

config router static
  edit 1
    set device XO-ISP
    set gateway 40.1.1.2
    set distance 10
  next
  edit 2
    set device XS-ISP
    set gateway 145.1.1.2
    set distance 20
end

```

Adding the firewall addresses

You need to define the addresses of the Commercial VDOM subnets for use in firewall policies. In the root 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 Go to **Firewall > Address**.
- 2 Select Create New.
- 3 Enter the following information and select OK:

Address Name	all
IP Range/Subnet	0.0.0.0/0.0.0.0

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

Address Name	development_net
IP Range/Subnet	192.168.10.0/255.255.255.0

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

Address Name	sales_net
IP Range/Subnet	192.168.15.0/255.255.255.0

Figure 34: Firewall addresses for Commercial domain

Create New		
Name	Address	
all	0.0.0.0/0.0.0.0	
development_net	192.168.10.0/255.255.255.0	
sales_net	192.168.15.0/255.255.255.0	

To add the firewall addresses - CLI

```
config firewall address
  edit all
    set subnet 0.0.0.0 0.0.0.0
  next
  edit development_net
    set subnet 192.168.10.0 255.255.255.0
  next
  edit sales_net
    set subnet 192.168.15.0 255.255.255.0
  next
  next
end
```

Adding the firewall policies

Each internal network needs a policy to permit it to access the XO-ISP and XS-ISP networks for connection to the Internet. Also, each internal network needs a policy to allow it to connect to the other internal network.

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:

Interface/Zone Source	Sales
Interface/Zone Destination	XO-ISP
Source	sales_net
Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Protection profile	scan
Configure other fields as required.	

- 4 Select Create New.

- 5 Enter the following information and select OK:

Interface/Zone Source	Sales
Interface/Zone Destination	XS-ISP
Source	sales_net
Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Protection profile	scan
Configure other fields as required.	

- 6 Select Create New.

- 7 Enter the following information and select OK:

Interface/Zone Source	Development
Interface/Zone Destination	XO-ISP
Address Name Source	development_net
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Protection profile	scan
Configure other fields as required.	

- 8 Select Create New.

- 9 Enter the following information and select OK:

Interface/Zone Source	Development
Interface/Zone Destination	XS-ISP
Address Name Source	development_net
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Protection profile	scan
Configure other fields as required.	

- 10 Select Create New.

11 Enter the following information and select OK:

Interface/Zone Source	Sales
Interface/Zone Destination	Development
Source	sales_net
Destination	development_net
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Configure other fields as required.	

12 Select Create New.

13 Enter the following information and select OK:

Interface/Zone Source	Development
Interface/Zone Destination	Sales
Source	development_net
Destination	sales_net
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	enable
Configure other fields as required.	

The list of firewall policies looks like this:

Figure 35: Firewall policies for Commercial VDOM

ID	Source	Dest	Schedule	Service	Action	Enable	
Create New							
▼ Sales -> Development (1)							
5	sales_net	development_net	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ Sales -> XO-ISP (1)							
1	sales_net	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ Sales -> XS-ISP (1)							
2	sales_net	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ Development -> Sales (1)							
6	development_net	sales_net	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ Development -> XO-ISP (1)							
3	development_net	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ Development -> XS-ISP (1)							
4	development_net	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	

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 strict
    set nat enable
next
edit 2
    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 strict
    set nat enable
next
edit 3
    set srcintf Development
    set dstintf XO-ISP
    set srcaddr development_net
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set profile_status enable
    set profile strict
    set nat enable
next
edit 4
    set srcintf Development
    set dstintf XS-ISP
    set srcaddr development_net
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set profile_status enable
    set profile strict
    set nat enable
next
```

```
edit 5
  set srcintf Sales
  set dstintf Development
  set srcaddr sales_net
  set dstaddr development_net
  set action accept
  set schedule always
  set service ANY
  set nat enable
next
edit 6
  set srcintf Development
  set dstintf Sales
  set srcaddr development_net
  set dstaddr sales_net
  set action accept
  set schedule always
  set service ANY
  set nat enable
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. The default gateway for VLAN 20 is the FortiGate VLAN 20 subinterface, and so on.

Configuring the Cisco switch

Add a configuration file to each of Cisco Catalyst 2900 ethernet switches. The configuration file defines the VLAN subinterfaces and the 802.1Q trunk interface on the switch.

Configuring the VLAN subinterfaces and the trunk interfaces

Add this file to the Cisco switch connected to the FortiGate-300 internal interface:

```
!
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

Add this file to the Cisco switch connected to the FortiGate-300 external interface:

```
!
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

Use diagnostic commands (`tracert`, `ping`) to test traffic routed through the FortiGate unit and the Cisco switch.

Testing traffic from instructors network to student network

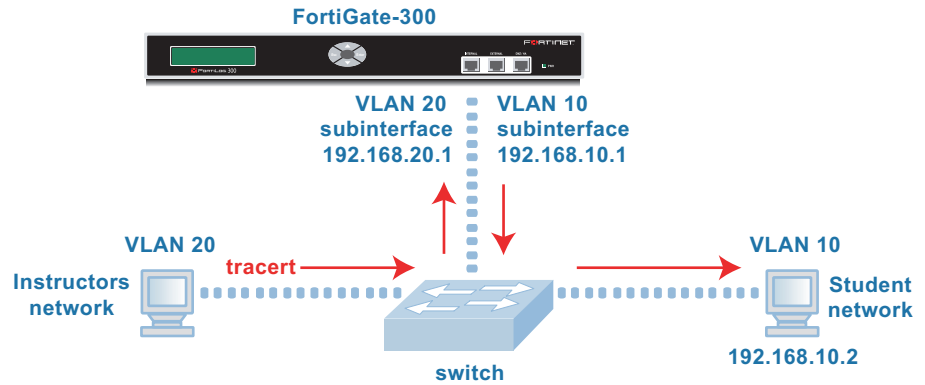
In this example, a route is traced from the instructors network to the student network. The route target is a host on the student network.

From the instructors network, access a 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:
  0  <10 ms  <10 ms  <10 ms  192.168.20.1
  1  <10 ms  <10 ms  <10 ms  192.168.10.2
Trace complete.
```

Figure 36: Example trace route from VLAN 20 to VLAN 10



Other tests

Using the preceding method, you can also test traffic from the Development network to the Sales network and vice-versa, as well as traffic from each of the internal networks to locations on the Internet.

Using VLANs and VDOMs in Transparent mode

Overview

In Transparent mode, the FortiGate unit can provide services such as antivirus scanning, web filtering, spam filtering, and intrusion protection to traffic on an IEEE 802.1Q VLAN trunk. You can insert the FortiGate unit operating in Transparent mode into the trunk without making changes to your network. In a typical configuration, the FortiGate internal interface accepts VLAN packets on a VLAN trunk from a VLAN switch or router connected to internal VLANs. The FortiGate external interface forwards tagged packets through another trunk to an external VLAN switch or router connected to external networks or the Internet. You can configure the FortiGate 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. Network protection, such as spam filtering, web filtering and anti-virus scanning, are applied through the protection profile specified in each firewall policy.

For each VLAN you are protecting with the FortiGate unit, you need to define a pair of VLAN subinterfaces and the necessary firewall policies. Usually in Transparent mode you do not permit packets to move between VLANs.

When the FortiGate unit receives a VLAN tagged packet at a physical interface, the packet is directed 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 in the same way as it does 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.

VLANs and virtual domains

When you add each VLAN subinterface, you associate it with a virtual domain. By default the FortiGate configuration includes one virtual domain, named root, and you can add as many VLAN subinterfaces as you require to this virtual domain.

You can add more virtual domains if you want to separate groups of VLAN subinterfaces into virtual domains. When using a FortiGate unit to serve multiple organizations, this simplifies administration because you see only the firewall policies for the VDOM you are configuring. For information on adding and configuring virtual domains, see [“Creating virtual domains” on page 19](#).

One essential application of virtual domains 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 virtual domain, you can solve this problem by creating a virtual domain for each VLAN. For an example of this type of configuration, see [“Example configuration Transparent mode \(multiple virtual domains\)” on page 98](#).

Configuring the FortiGate unit in Transparent mode

There are two essential steps to configure of your FortiGate unit to work with VLANs:

- Add VLAN subinterfaces
- Create firewall policies

You can also configure the protection profiles that govern virus scanning, web filtering, and spam filtering. Protection profiles are covered in the documentation for your FortiGate unit.

In Transparent mode, you can access the FortiGate unit web-based manager by connecting to an interface configured for administrative access and using HTTPS to access the management IP address. On the FortiGate-300 used as an example in this document, administrative access is enabled by default on the Internal interface and the default management IP address is 10.10.10.1. If you need more information, see the *Quick Start Guide* or *Installation Guide* for your unit.

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 4096. You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

To add VLAN subinterfaces in Transparent mode

- 1 Go to **System > Network > Interface**.
- 2 Select Create New to add a VLAN subinterface.
- 3 Enter a Name to identify the VLAN subinterface.
- 4 Select the physical interface that receives the VLAN packets intended for this VLAN subinterface.
- 5 Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.
- 6 Select the virtual domain to which to add this VLAN subinterface.

- 7 Configure other settings as required.
- 8 Select OK to save your changes.
The FortiGate unit adds the new subinterface to the interface that you selected.
- 9 Repeat Step 2 through Step 8, but choose the physical interface through which the VLAN packets exit the FortiGate unit. Use the same VLAN ID and VDOM as before.
- 10 For each of the VLAN subinterfaces you added, select Bring Up to start the interface.

Creating firewall policies

Firewall policies permit communication between the FortiGate unit 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 subjects the packets on each VLAN to antivirus and antispam scanning 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.

To add firewall policies for VLAN subinterfaces

- 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.
- 8 Select Protection Profile and select the profile from the list.
- 9 Configure other settings as required.
- 10 Select OK.

Example configuration Transparent mode (simple)

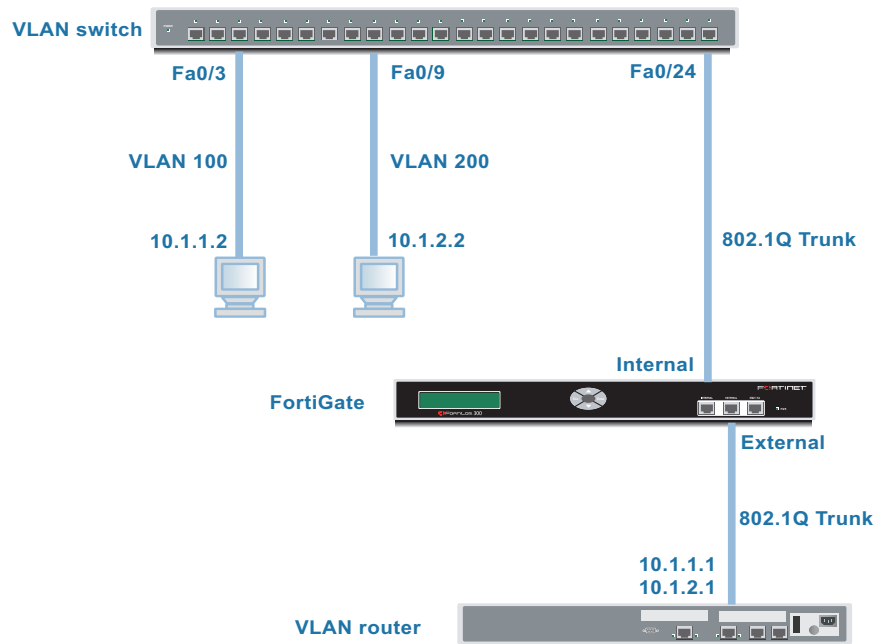
In this example, the FortiGate-300 unit is operating in Transparent mode. The FortiGate-300 unit is configured with two VLANs, one with an ID of 100 and the other with ID 200. The Internal and External physical interfaces each have two VLAN subinterfaces, one for VLAN 100 and one for VLAN 200.

The FortiGate unit is connected to a Cisco 2900 switch on its internal network interface and to a Cisco 2620 router on its external network interface. The switch and the router add VLAN IDs to packets and then forward the packets to the FortiGate unit. When the FortiGate units receives a tagged packet, it directs it from one VLAN subinterface to another.

For example, when the switch receives a packet from VLAN 100, it adds VLAN ID 100 and forwards the packet to VLAN subinterface 100 on the internal network interface on the FortiGate unit. The FortiGate unit directs the packet to VLAN subinterface 100 on the external network interface. From here the packet is forwarded to the router.

This section describes how to configure a FortiGate-300 unit, a Cisco switch, and a Cisco router, for the example network topology shown in [Figure 37](#).

Figure 37: Example VLAN topology (FortiGate unit in Transparent mode)



General configuration steps

- 1 Configure the FortiGate-300 unit.
 - Add four VLAN subinterfaces:
 - VLAN ID 100 added to internal and external network interfaces
 - VLAN ID 200 added to internal and external network interfaces
 - Add firewall policies to allow:
 - the VLAN networks to access the external network.
 - the external network to access the VLAN networks.
- 2 Configure the Cisco switch to support VLAN tags.
- 3 Configure the Cisco router to support VLAN tags.
- 4 Test the implementation.

Configuring the FortiGate-300 unit

Start the FortiGate web-based manager to configure the FortiGate-300 unit.

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
Virtual Domain	root
Configure other settings as required.	

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

Name	VLAN_100_ext
Interface	external
VLAN ID	100
Virtual Domain	root
Configure other settings as required.	

- 6 Select Create New.

7 Enter the following information and select OK:

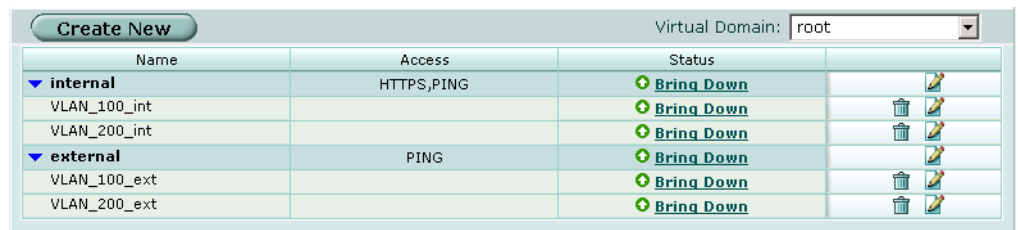
Name	VLAN_200_int
Interface	internal
VLAN ID	200
Virtual Domain	root
Configure other settings as required.	

8 Select Create New.

9 Enter the following information and select OK:

Name	VLAN_200_ext
Interface	external
VLAN ID	200
Virtual Domain	root
Configure other settings as required.	

Figure 38: VLAN subinterfaces



To add VLAN subinterfaces - CLI

```

config system interface
  edit VLAN_100_int
    set status down
    set interface internal
    set vlanid 100
  next
  edit VLAN_100_ext
    set status down
    set interface external
    set vlanid 100
  next
  edit VLAN_200_int
    set status down
    set interface internal
    set vlanid 200
  next
  
```

```

edit VLAN_200_ext
  set status down
  set interface external
  set vlanid 200
end

```

Adding the firewall policies

Firewall policies allow packets to travel from the VLAN_100_int interface to the VLAN_100_ext interface and from the VLAN_200_int interface to the VLAN_200_ext interface.

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:

Interface/Zone Source	VLAN_100_int
Interface/Zone Destination	VLAN_100_ext
Address Name Source	all
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
Configure other fields as required.	

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

Interface/Zone Source	VLAN_100_ext
Interface/Zone Destination	VLAN_100_int
Address Name Source	all
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
Configure other fields as required.	

- 6 Go to **Firewall > Policy**.
- 7 Select Create New.

8 Enter the following information and select OK:

Interface/Zone Source	VLAN_200_int
Interface/Zone Destination	VLAN_200_ext
Address Name Source	all
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
Configure other fields as required.	

9 Select Create New.

10 Enter the following information and select OK:

Interface/Zone Source	VLAN_200_ext
Interface/Zone Destination	VLAN_200_int
Address Name Source	all
Address Name Destination	all
Schedule	Always
Service	ANY
Action	ACCEPT
Configure other fields as required.	

Figure 39: Firewall policies for VLANs

Create New							
ID	Source	Dest	Schedule	Service	Action	Enable	
▼ VLAN_100_int -> VLAN_100_ext (1)							
1	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ VLAN_200_int -> VLAN_200_ext (1)							
3	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ VLAN_100_ext -> VLAN_100_int (1)							
2	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ VLAN_200_ext -> VLAN_200_int (1)							
4	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	

To add the 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 action accept
    set schedule always
    set service ANY
  next
  
```

```
edit 2
  set srcintf VLAN_100_ext
  set dstintf VLAN_100_int
  set srcaddr all
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
next
edit 3
  set srcintf VLAN_200_int
  set dstintf VLAN_200_ext
  set srcaddr all
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
next
edit 4
  set srcintf VLAN_200_ext
  set dstintf VLAN_200_int
  set srcaddr all
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
end
```

Configuring the Cisco switch

On the Cisco Catalyst 2900 ethernet 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.

Configuring 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

Configuring the Cisco router

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.)

Configuring the VLAN subinterfaces and the trunk interfaces

Add this file to the Cisco router:

```
!
interface FastEthernet0/0
!
interface FastEthernet0/0.1
  encapsulation dot1Q 100
  ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0.2
  encapsulation dot1Q 200
  ip address 10.1.2.1 255.255.255.0
!
```

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



Note: To complete the setup, configure devices on VLAN 100 and VLAN 200 with default gateways. The default gateway for VLAN 100 is the Cisco router VLAN 100 subinterface. The default gateway for VLAN 200 is the Cisco router VLAN 200 subinterface.

Testing the configuration

Use diagnostic commands (`tracert`, `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.

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

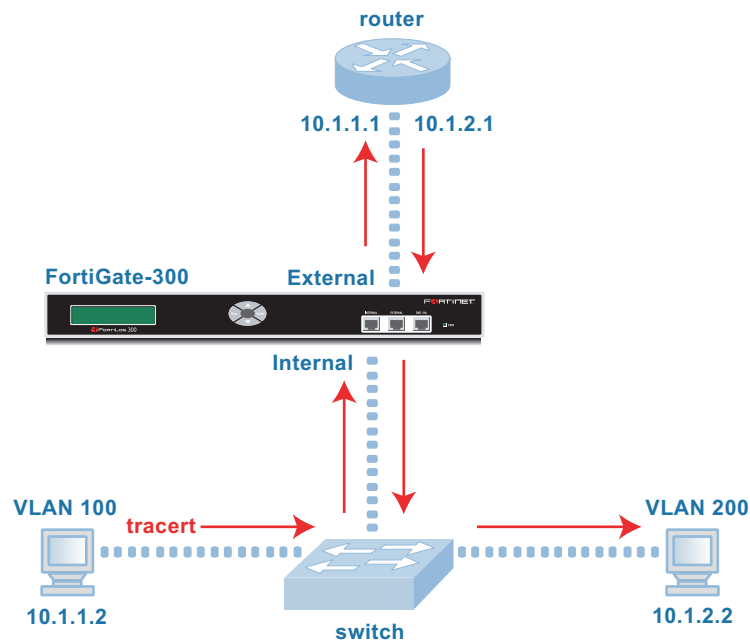
```
C:\>tracert 10.1.2.2
```

```
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.
```

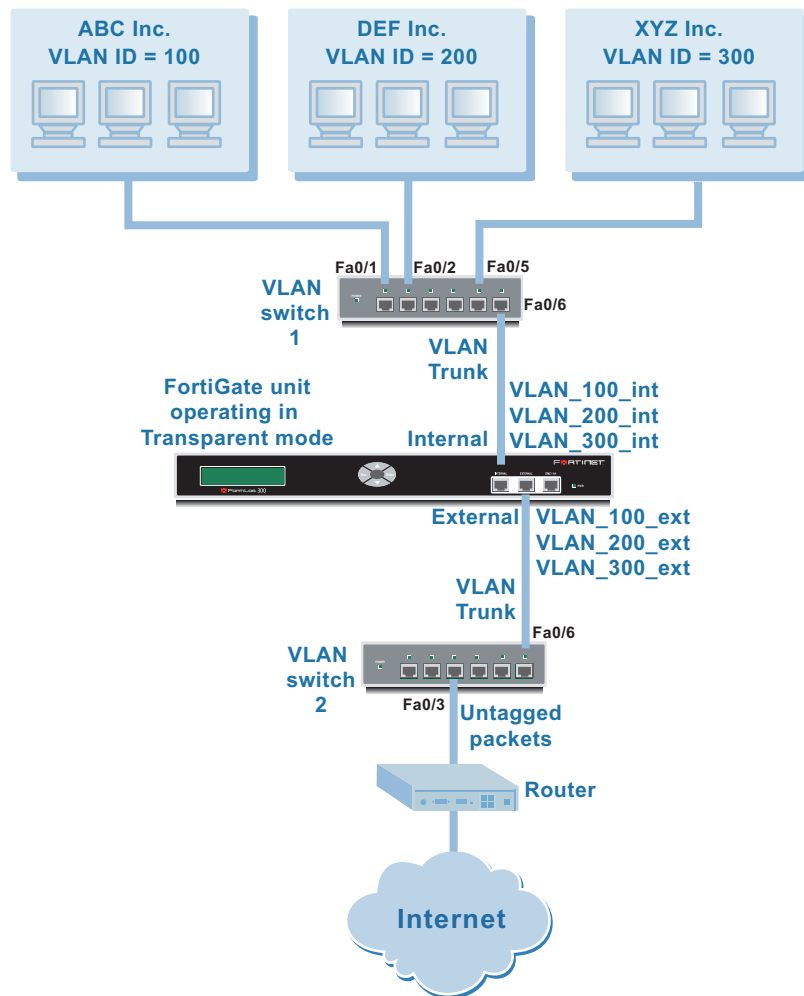
Figure 40: Example trace route from VLAN 100 to VLAN 200



Example configuration Transparent mode (multiple virtual domains)

In this example, the FortiGate-300 unit provides network protection to three organizations that quite different policies for incoming and outgoing traffic. This requires that they have different firewall policies and protection profiles. Although this might be achieved without using virtual domains, the administration is simpler using the virtual domains to view and configure only one organization’s policies at a time.

Figure 41: Transparent mode operation with multiple domains



Configuring global items

Some components of the protection profiles that you create are global, rather than per-domain.

Creating schedules

The FortiGate-300 unit in this example serves organizations that are all businesses that vary their policies according to the time of day. For simplicity, this example assumes that they all have the same lunch hours. It would be possible to accommodate different definitions of lunchtime by creating multiple schedules tailored to the needs of each organization.

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 Monday, Tuesday, Wednesday, Thursday and Friday.
- 5 Set the Start time as 11:45 and set the Stop time as 14:00.

New Recurring Schedule							
Name	lunch						
Day	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Select	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Start	Hour	11		Minute	45		
Stop	Hour	14		Minute	00		
OK				Cancel			
Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will run for 24 hours.							

- 6 Select OK.

To create a recurring schedule for lunchtime - CLI

```
config firewall schedule recurring
edit Lunch
set day monday tuesday wednesday thursday friday
saturday
set start 11:45
set end 14:00
end
```

Creating protection profiles

The FortiGate-300 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 global, but you can create as many as you need to cover the requirements of different organizations.

This example creates the following protection profiles:

Profile name	Description	Used by
BusinessOnly	Antivirus, spam filtering, banned word list, IPS. Web category filtering designed to prevent non-business activity.	ABC Inc., DEF Inc.
Lunch	Antivirus, spam filtering, banned word list, IPS. Relaxed web category filtering to allow some general-interest web browsing during lunch hour.	ABC Inc., DEF Inc.

To create the BusinessOnly protection profile - web-based manager

- 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 HTTP, FTP, IMAP, POP3, and SMTP.
- 5 Select Web Category Filtering and enable category block.
Configure categories as follows:

Potentially Liable (group)	Block
Objectionable or 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
Other	Block
- 6 Select Spam Filtering and enable RBL & ORDBL check for IMAP, POP3 and SMTP.
- 7 Select Banned word check for IMAP, POP3 and SMTP.
- 8 For Spam action, select tagged for IMAP and POP3, discard for SMTP.
- 9 Select IPS and enable IPS Signature and IPS Anomaly.
- 10 Select OK.

To create the BusinessOnly protection profile - CLI

```
config firewall profile
edit BusinessOnly
set ftp scan
set http scan catblock
set imap scan fragmail spamrbl bannedword
set pop3 scan fragmail spamrbl bannedword
set smtp scan fragmail spamrbl bannedword
set ips signature anomaly
set cat_allow 49-50-51-52-53
set cat_deny g01-g02-g03-g04-g05-g06-g08
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 enable Virus Scan for HTTP, FTP, IMAP, POP3, and SMTP.
- 5** Select Web Category Filtering and enable category block.
Configure categories as follows:

Potentially Liable (group)	Block
Objectionable or Controversial (group)	Block
Potentially Non-productive (group)	Monitor
Potentially Bandwidth Consuming (group)	Monitor
Potentially Security Violating (group)	Block
General Interest (group)	Allow
Business Oriented	Allow
Others	Allow
- 6** Select Spam Filtering and enable RBL & ORDBL check for IMAP, POP3 and SMTP.
- 7** Select Banned word check for IMAP, POP3 and SMTP.
- 8** For Spam action, select tagged for IMAP and POP3, discard for SMTP.
- 9** Select IPS and enable IPS Signature and IPS Anomaly.
- 10** Select OK.

To create the Relaxed protection profile - CLI

```
config firewall profile
edit Relaxed
set ftp scan
set http scan catblock
set imap scan
set pop3 scan
set smtp scan spamrbl
set ips anomaly
set ips signature
set cat_allow g06-g07-g08
set cat_deny g01-g02-g05
set cat_monitor g03-g04
end
```

Creating virtual domains

The FortiGate-300 supports 10 virtual domains in Transparent mode. The root domain is the default domain. It cannot be deleted or renamed. In this example, the root domain is not used. New virtual domains are created for company ABC, company DEF and company XYZ.

To create the virtual domains - web-based manager

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Create New.
- 3 Type "ABCdomain" in the Virtual Domain Name field and select OK.
- 4 Select Create New.
- 5 Type "DEFdomain" in the Virtual Domain Name field and select OK.
- 6 Select Create New.
- 7 Type "XYZdomain" in the Virtual Domain Name field 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.

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
Configure other settings as required.	

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

Name	VLAN_100_ext
Interface	external
VLAN ID	100
Virtual Domain	ABCdomain
Configure other settings as required.	

Figure 42: Interfaces for ABCdomain

Name	Access	Status	
▼ internal	HTTPS,PING	Bring Down	
VLAN_100_int		Bring Down	
▼ external	PING	Bring Down	
VLAN_100_ext		Bring Down	

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 > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the ABCdomain VDOM.

To select the ABCdomain VDOM - CLI

```
execute enter ABCdomain
```

Creating service groups

ABC Inc. does not want their 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. A firewall policy can manage only one service or one group.

To create a games and chat service group - web-based manager

- 1 Go to **Firewall > Service > Group**.
- 2 Select Create New.
- 3 Type 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 > Address**.
- 2 Select Create New.
- 3 Type “new” in the Address Name field.
- 4 Type 0.0.0.0/0.0.0.0 in the IP Range/Subnet 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 > Policy**.
- 2 Select Create New.
- 3 Enter the following information and select OK:

Interface/Zone Source	VLAN_100_int
Interface/Zone Destination	VLAN_100_ext
Address Name Source	all
Address Name Destination	all
Schedule	BusinessDay
Service	games-chat
Action	DENY
Configure other fields as required.	

This policy prevents the use of network games or chat programs during business hours.

- 4 Enter the following information and select OK:

Interface/Zone Source	VLAN_100_int
Interface/Zone Destination	VLAN_100_ext
Address Name Source	all
Address Name Destination	all
Schedule	Lunch
Service	HTTP
Action	ACCEPT
Protection Profile	Relaxed
Configure other fields as required.	

This policy relaxes the web category filtering during lunch hour.

- 5 Enter the following information and select OK:

Interface/Zone Source	VLAN_100_int
Interface/Zone Destination	VLAN_100_ext
Address Name Source	all
Address Name Destination	all
Schedule	BusinessDay
Service	HTTP
Action	ACCEPT
Protection Profile	BusinessOnly
Configure other fields as required.	

This policy provides rather strict web category filtering during business hours.

Figure 43: ABCdomain firewall policies

ID	Source	Dest	Schedule	Service	Action	Enable	
▼ VLAN_100_int -> VLAN_100_ext (3)							
1	all	all	BusinessDay	games-chat	DENY	<input checked="" type="checkbox"/>	
2	all	all	Lunch	HTTP	ACCEPT	<input checked="" type="checkbox"/>	
3	all	all	BusinessDay	HTTP	ACCEPT	<input checked="" type="checkbox"/>	

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.

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.

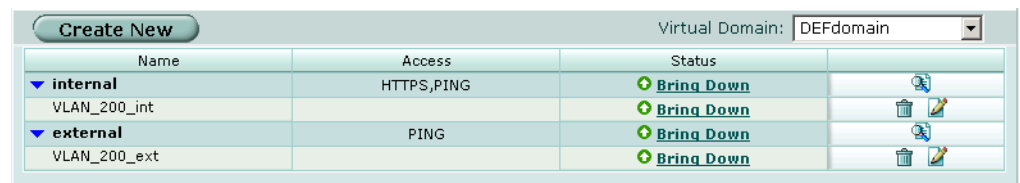
- 3 Enter the following information and select OK:

Name	VLAN_200_int
Interface	internal
VLAN ID	200
Virtual Domain	DEFdomain
Configure other settings as required.	

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

Name	VLAN_200_ext
Interface	external
VLAN ID	200
Virtual Domain	DEFdomain
Configure other settings as required.	

Figure 44: 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 domain is DEFdomain.

To select the DEFdomain VDOM - web-based manager

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.

- 3 Choose the DEFdomain VDOM.

To select the DEFdomain VDOM - CLI

```
execute enter DEFdomain
```

Creating service groups

DEF Inc. does not want their employees to use online gaming software or any online chat software except NetMeeting, which they use 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 Type 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 > Address**.
- 2 Select Create New.
- 3 Type “new” in the Address Name field.
- 4 Type 0.0.0.0/0.0.0.0 in the IP Range/Subnet 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 > Policy**.
- 2 Select Create New.
- 3 Enter the following information and select OK:

Interface/Zone Source	VLAN_200_int
Interface/Zone Destination	VLAN_200_ext
Address Name Source	all
Address Name Destination	all
Schedule	BusinessDay
Service	games-chat
Action	DENY
Configure other fields as required.	

This policy prevents the use of network games or chat programs (except NetMeeting) during business hours.

- 4 Enter the following information and select OK:

Interface/Zone Source	VLAN_200_int
Interface/Zone Destination	VLAN_200_ext
Address Name Source	all
Address Name Destination	all
Schedule	Lunch
Service	HTTP
Action	ACCEPT
Protection Profile	Relaxed
Configure other fields as required.	

This policy relaxes the web category filtering during lunch hour.

- 5 Enter the following information and select OK:

Interface/Zone Source	VLAN_200_int
Interface/Zone Destination	VLAN_200_ext
Address Name Source	all
Address Name Destination	all
Schedule	BusinessDay
Service	HTTP
Action	ACCEPT
Protection Profile	BusinessOnly
Configure other fields as required.	

This policy provides rather strict web category filtering during business hours.

- 6 Enter the following information and select OK:

Interface/Zone Source	VLAN_200_int
Interface/Zone Destination	VLAN_200_ext
Address Name Source	all
Address Name Destination	all
Schedule	always
Service	ANY
Action	ACCEPT
Protection Profile	Relaxed
Configure other fields as required.	

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 that 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 don't want any after-hours internet access.

Figure 45: DEFdomain firewall policies

ID	Source	Dest	Schedule	Service	Action	Enable	
▼ VLAN_200_int -> VLAN_200_ext (4)							
1	all	all	BusinessDay	Games	DENY	<input checked="" type="checkbox"/>	
2	all	all	Lunch	HTTP	ACCEPT	<input checked="" type="checkbox"/>	
3	all	all	BusinessDay	HTTP	ACCEPT	<input checked="" type="checkbox"/>	
4	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	

To configure DEFdomain firewall policies - CLI

```
config firewall policy
edit 1
    set srcintf VLAN_200_int
    set dstintf VLAN_200_ext
    set srcaddr all
    set dstaddr all
    set schedule BusinessDay
    set service Games
    set action deny
next
edit 2
    set srcintf VLAN_200_int
    set dstintf VLAN_200_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_200_int
    set dstintf VLAN_200_ext
    set srcaddr all
    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 dstintf VLAN_200_ext
    set srcaddr all
    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.

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_300_int
Interface	internal
VLAN ID	300
Virtual Domain	XYZdomain
Configure other settings as required.	

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

Name	VLAN_300_ext
Interface	external
VLAN ID	300
Virtual Domain	XYZdomain
Configure other settings as required.	

Figure 46: Interfaces for XYZdomain

Name	Access	Status	
▼ internal	HTTPS,PING	Bring Down	
VLAN_300_int		Bring Down	
▼ external	PING	Bring Down	
VLAN_300_ext		Bring Down	

To add the VLAN subinterfaces - CLI

```
config system interface
edit VLAN_300_int
    set interface internal
    set vlanid 300
    set vdom XYZdomain
next
edit VLAN_300_ext
    set interface external
    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 > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the XYZdomain VDOM.

To select the XYZdomain VDOM - CLI

```
execute enter 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 Type 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 Type 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 an email 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 > Address**.
- 2 Select Create New.
- 3 Type “new” in the Address Name field.
- 4 Type 0.0.0.0/0.0.0.0 in the IP Range/Subnet 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 > Policy**.
- 2 Select Create New.

3 Enter the following information and select OK:

Interface/Zone Source	VLAN_300_int
Interface/Zone Destination	VLAN_300_ext
Address Name Source	all
Address Name Destination	all
Schedule	always
Service	Email
Action	ACCEPT
Protection Profile	strict
Configure other fields as required.	

This policy provides network protection for email using the default strict protection profile. The administrator must also set up the antivirus, web filter and spam filter settings. These procedures are not described in this document.

4 Enter the following information and select OK:

Interface/Zone Source	VLAN_300_int
Interface/Zone Destination	VLAN_300_ext
Address Name Source	all
Address Name Destination	all
Schedule	always
Service	Web
Action	ACCEPT
Protection Profile	web
Configure other fields as required.	

This policy provides network protection for HTTP, HTTPS and FTP using the default web protection profile. The administrator must also set up the antivirus and web filter settings. These procedures are not described in this document.

Figure 47: XYZdomain firewall policies

The screenshot shows a web-based configuration interface for firewall policies. At the top, there is a 'Create New' button. Below it is a table with columns: ID, Source, Dest, Schedule, Service, Action, and Enable. The table contains two rows of policies. The first row is expanded to show a sub-table with columns: ID, Source, Dest, Schedule, Service, Action, and Enable. The second row is collapsed. To the right of the table are icons for deleting, editing, and creating new policies.

ID	Source	Dest	Schedule	Service	Action	Enable
▼ VLAN_300_int -> VLAN_300_ext (2)						
1	all	all	always	Email	ACCEPT	<input checked="" type="checkbox"/>
2	all	all	always	Web	ACCEPT	<input checked="" type="checkbox"/>

To configure XYZdomain firewall policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_300_int
    set dstintf VLAN_300_ext
    set srcaddr all
    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 dstintf VLAN_300_ext
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service Web
    set profile_status enable
    set profile web
  end
```

Configuring the Cisco switch

On the Cisco Catalyst 2900 ethernet switches, 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.

Configuring switch 1

Add this file to Cisco VLAN switch 1:

```
!
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 switch 2

Add this file to Cisco VLAN switch 2:

```
interface FastEthernet0/3
  switchport
  !
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

Testing the configuration

Use diagnostic commands (`tracert`, `ping`) to test traffic routed through the network.

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.fortinet.com`.

- 1 From a host on VLAN 100, access a command prompt and enter this command:

```
C:\>tracert www.fortinet.com
Tracing route to www.fortinet.com [128.242.109.135]
over a maximum of 30 hops:
  1  <10 ms  <10 ms  <10 ms  172.20.120.2
  ...
 14  172 ms  141 ms  140 ms  128.242.109.135
Trace complete.
```

- 2 Repeat for VLAN 200 and VLAN 300.

Avoiding Problems with VLANs

Overview

There are several issues that can cause problems with your VLANs:

- [Asymmetric routing](#)
- [Layer 2 traffic](#)
- [NetBIOS](#)
- [STP forwarding](#)

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 sees the response packets, but not the requests, it blocks them as invalid. Also, if the FortiGate unit sees the same packets repeated on multiple interfaces, it blocks the session as a potential attack.

These are instances of asymmetric routing. By default, FortiGate units blocks packets or drops the session when this happens. Using the Command Line Interface (CLI), you can configure the FortiGate unit to permit asymmetric routing:

```
config system global
  set asymroute enable
end
```

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 can reduce the security of your system. It is better to change routing or change how FortiGate unit connects into your network. The [Asymmetric Routing and Other FortiGate Layer-2 Installation Issues](#) technical note provides detailed examples of asymmetric routing situations and possible solutions.

Layer 2 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 the network, you need to configure FortiGate interfaces to pass them. You can do this using the CLI:

```
config system interface
  edit <name_str>
    set l2forward enable
  end
```

where <name_str> is the name of an interface.

Enabling Layer 2 traffic can cause a problem if it is possible for packets to repeatedly loop through the network. This occurs when there is more than one Layer 2 path from a source to a destination. Traffic can be impeded.

ARP traffic

Address Resolution Protocol (ARP) traffic is vital to communication on a network and is enabled on FortiGate 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.

The solution in this case is to configure multiple virtual domains on the FortiGate unit, one for each VLAN. This means one inbound and one outbound VLAN interface in each virtual domain. By default, physical interfaces are in the root domain. Do not configure any of your VLANs in the root domain. ARP packets are not forwarded between virtual domains. As a result, the switches do not receive multiple ARP packets with the same source MAC but different VLAN IDs, and the instability does not occur.

There is a more detailed discussion of this issue in the [Asymmetric Routing and Other FortiGate Layer-2 Installation Issues](#) technical note.

NetBIOS

Networked computers running Microsoft Windows operating systems rely on a WINS server to resolve host names to IP addresses. The hosts communicate with the WINS server using NetBIOS protocol. To support this type of network you need to enable the forwarding of NetBIOS requests to a WINS server. Enter the following CLI commands:

```
config system interface
  edit <interface>
    set netbios_forward enable
    set wins-ip <wins_server_ip>
  end
```

where <interface> is the name of the interface and <wins_server_ip> is the IP address of the WINS server. These commands apply only in NAT/Route mode.

STP forwarding

The FortiGate unit does not participate in the Spanning Tree protocol (STP). If you use the unit in a network topology that relies on STP for network loop protection, you need to make changes to the FortiGate configuration. Otherwise, STP sees the FortiGate unit as a blocked link and forwards the data to another path. By default, the 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:

```
config system interface
  edit <name_str>
    set l2forward enable
    set stpforward enable
  end
```

where <name_str> is the name of the interface.

Index

Numerics

802.1Q trunk 14

A

- adding VLAN subinterface
 - multiple VDOMs example 103, 107, 113
- adding VLAN subinterface, NAT/Route mode 22
 - adding to a VDOM 50
 - complex example 33
 - complex VDOM example 67, 73
 - simple example 25
 - simple VDOM example 55
- adding VLAN subinterface, Transparent mode 88
 - simple VDOM example 91
- administration
 - VDOM 17, 49
- asymmetric routing issue 119
- asymroute, permitting asymmetric routing 119

C

- Cisco router configuration
 - simple Transparent mode VDOM example 96
- Cisco switch configuration
 - complex NAT/Route VDOM example 83
 - complex NAT/Route VLAN example 46
 - simple NAT/Route example 29
 - simple NAT/Route VDOM example 62
 - simple Transparent mode VDOM example 95
 - Transparent mode multiple VDOMs example 117
- customer service 12

D

- default route, setting
 - complex NAT/Route example 35, 69
 - complex VDOM example 76
 - for VDOM 51
 - NAT/Route mode 23
 - NAT/Route VDOMs example 57
 - simple NAT/Route example 61
 - simple NAT/Route VDOM example 57

E

- example
 - complex NAT/Route mode VLAN 31
 - complex NAT/Route topology 31
 - complex NAT/Route VDOM 64
 - multiple VDOMs in Transparent mode 98
 - simple NAT/Route topology 24
 - simple NAT/Route VLAN topology 53
 - simple Transparent mode VLAN 90

F

- firewall address
 - adding for firewall policy 23
 - complex NAT/Route mode example 36, 77
 - complex NAT/Route mode VDOM example 70
 - multiple VDOMs example 109, 115
 - simple NAT/Route example 26, 56
 - simple NAT/Route VDOM example 56, 59
 - Transparent mode multi-VDOM example 105
- firewall policy
 - complex NAT/Route mode example 37
 - complex NAT/Route mode VDOM example 71, 78
 - configuring for VDOM 51
 - creating 23
 - creating, NAT/Route mode 23
 - creating, Transparent mode 89
 - multiple VDOMs example 105, 110, 115
 - simple NAT/Route example 27
 - simple NAT/Route VDOM example 56, 60
 - simple Transparent mode VDOM example 93
- firewall schedule, creating
 - multiple VDOMs example 99
- Fortinet customer service 12

I

- interface, DMZ
 - configuring, simple NAT/Route VDOM example 54
- interface, external
 - configuring, simple NAT/Route mode example 24
 - configuring, simple NAT/Route mode VDOM example 54
- IP address
 - for FortiGate interface 22
- IPX, enabling Layer 2 forwarding for 120

L

L2TP, enabling Layer 2 forwarding for 120
layer 2 forwarding, enabling 120
layer-2 switching 14
layer-3 routing 15

N

NAT/Route mode
 adding VLAN subinterface 22
 complex VLANs example 31
 configuring VLANs overview 21
NetBIOS, for Windows networks 121

P

packet
 and VDOM 16
PPTP, enabling Layer 2 forwarding for 120
protection profile
 Transparent VDOMs example 100

R

routing, setting default route
 complex NAT/Route example 35, 69
 complex VDOM example 76
 for VDOM 51
 NAT/Route mode 23
 NAT/Route VDOMs example 57
 simple NAT/Route example 61
 simple NAT/Route VDOM example 57

S

schedule, firewall
 multiple VDOMs example 99
selecting
 VDOM 19
service group
 creating, Transparent mode multiple VDOMs example 104, 109, 114
Spanning Tree Protocol, see STP
STP forwarding
subinterface
 adding to VDOM 50

T

technical support 12
testing configuration
 complex NAT/Route mode VDOM example 84
 complex NAT/Route VLAN example 47
 simple NAT/Route example 30
 simple NAT/Route VDOM example 62
 simple Transparent mode VDOM example 97

Transparent mode
 adding VLAN subinterface 88
 and VDOMs 87
 and VLANs 87
 creating firewall policies 89

V

VDOM 16
 adding 49
 adding VLAN subinterface to 50
 administration of 17, 49
 configuring 50
 configuring firewall policy for 51
 configuring routing for 51
 configuring VPN for 52
 configuring, simple NAT/Route VDOM example 55, 58
 creating, complex NAT/Route VDOM example 66
 creating, multiple VDOMs example 102
 creating, simple NAT/Route VDOM example 54
 described 49
 in Transparent mode 87
 number supported on FortiGate units 13
 overview 16
 packet handling 16
 properties exclusive to 17
 properties shared by all VDOMs 18
 selecting 19
virtual domain. See VDOM.
Virtual Private Network, see VPN.
VLAN
 configuring on Cisco switch, complex NAT/Route VLAN example 46
 in Transparent mode 87
 overview 14
 overview of NAT/Route configuration 21
VLAN ID
 and layer-2 14
 and layer-3 15
 rules for assignment 16
VLAN subinterface
 adding in NAT/Route mode 22
 adding in Transparent mode 88
 adding to a VDOM 50
 adding to VDOM, complex NAT/Route example 67, 73
 adding to VDOM, simple NAT/Route example 55
 adding, complex NAT/Route example 33
 adding, multiple VDOMS example 103, 107, 113
 adding, simple NAT/Route example 25
VPN
 client configuration 44
 configuring for VDOM 52
 encrypt policy 43
 firewall policy 43
 gateway configuration 40
 tunnel configuration 41
 user IP address 42

W

Windows networks
 enabling NetBIOS and WINS 121

WINS, enabling NetBIOS for 121

