Configuration Example

FortiGate SOHO and SMB
Version 3.0 MR5

FORTINET

www.fortinet.com

FortiGate SOHO and SMB Configuration Example
Version 3.0 MR5
24 August 2007
01-30005-0062-20070824

Trademarks
Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction

The FortiGate Configuration Example for SOHO (small office/home office) and SMB (small- to medium-sized business) provides a brief overview of FortiGate Unified Threat Management Systems, and a comprehensive example of a network implementation for a small company. This example attempts to employ some of the most common features applicable to small networks and can be easily adapted for planning your own network security implementation using a FortiGate firewall.

A complete procedure using the web-based manager is included for each network configuration task, followed by the same procedure using the command line interface (CLI).

Revision history

Document	Description of changes
01-30000-0062-20060106	First release of SOHO and SMB Guide updated for FortiOS v3.0
01-30000-0062-20060112	Added IM and P2P blocking to the help_desk protection profile.
01-30003-0062-20061506	Updated CLI, Web UI, and Graphics. Now consistant with FortiOS V3.0. MR3
01-30004-0062-20070115	Updated any references to IPS, IM, P2P and VoIP.
01-30005-0062-20070824	Updated against FortiOS V3.0. MR5

FortiGate Unified Threat Management Systems

Fortinet's award-winning FortiGate™ series of ASIC-accelerated Unified Threat Management Systems are the new generation of real-time network protection firewalls. They detect and eliminate the most damaging, content-based threats from email messages and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time without degrading network performance. In addition to providing application level protection, the FortiGate systems deliver a full range of network-level services — firewall, VPN, intrusion detection and traffic shaping — delivering complete network protection services in dedicated, easily managed platforms.

With models spanning SOHO to service providers, the FortiGate family spans the full range of network environments and offers cost effective systems for any application.

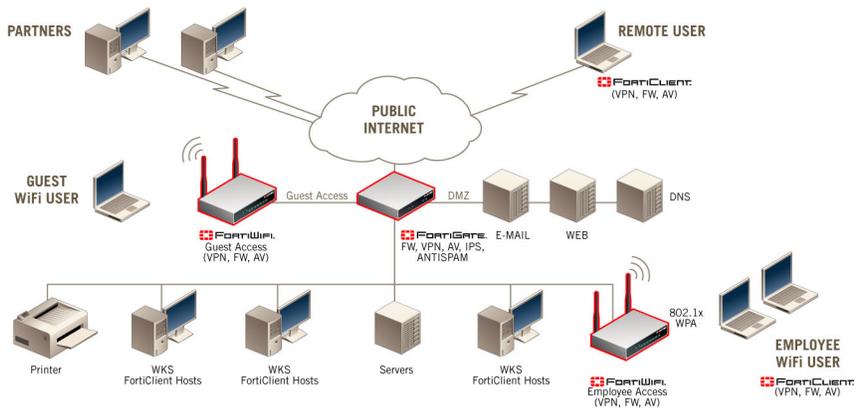**Figure 1:   FortiGate and FortiWiFi SMB model deployment**

Figure 2:   FortiGate enterprise model development
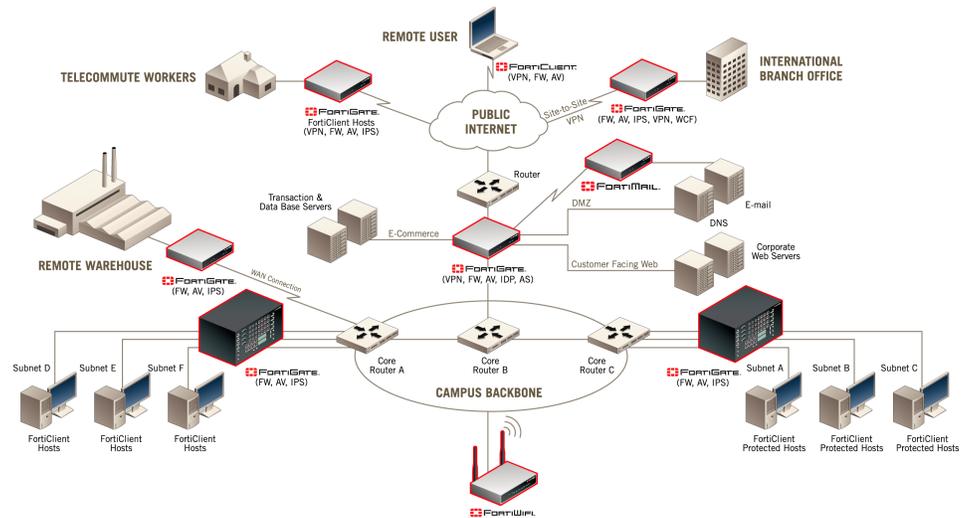
Figure 3:   FortiGate MSSP model deployment
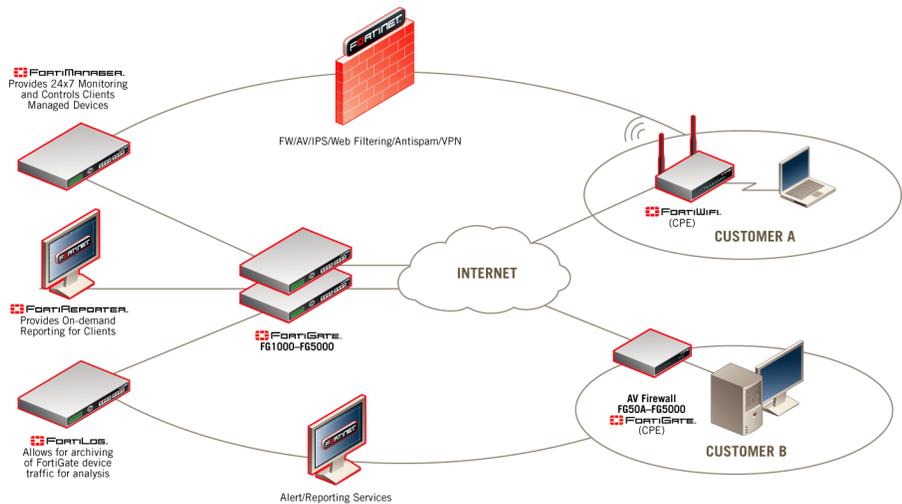
Other Fortinet products

Fortinet offers a complete range of products and services that work together to provide the most comprehensive, cost effective and manageable solutions available for protecting networks of all sizes.

FortiGuard service

FortiGuard service includes:

- virus encyclopedia
- attack encyclopedia
- vulnerability and patch list
- attack and virus definition updates
- attack and virus engine updates
- optional automatic push updates when new threats appear

FortiClient software

Fortinet's Remote FortiClient Host Security is designed to provide secure remote access to network resources for telecommuters, mobile workers, remote sites and partners. The FortiClient Host Security is an easy-to-use IPSec software client featuring an integrated personal firewall, Network Address Translation (NAT) Traversal, centralized policy management, multiple policy support for access to multiple devices, strong encryption, and a comprehensive set of tools for troubleshooting. Most popular Microsoft Windows operating systems are supported natively.

FortiManager tools

The FortiManager System is an integrated management and monitoring tool that enables enterprises and service providers to easily manage large numbers of FortiGate Unified Threat Management Systems. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full range of network protection services provide by FortiGate devices, supporting the needs of enterprises and service providers responsible for establishing and maintaining security policies across multiple, dispersed FortiGate installations.

FortiAnalyzer systems

The FortiAnalyzer Family of real-time logging systems is a series of dedicated hardware solutions that securely aggregate and analyze log data from multiple FortiGate Unified Threat Management Systems. The systems provide network administrators with a comprehensive view of network usage and security information, supporting the needs of enterprises and service providers responsible for discovering and addressing vulnerabilities across dispersed FortiGate installations. The FortiAnalyzer devices minimize the effort required to monitor and maintain acceptable use policies, to identify attack patterns and prosecute attackers, and to comply with governmental regulations regarding privacy and disclosure of security breaches. They accept and process a full range of log records provided by FortiGate devices, including traffic, event, virus, attack, content filtering, and email filtering data.

Fortinet documentation

Information about FortiGate products is available from the following FortiGate User Manual volumes:

- *FortiGate QuickStart Guide*

  Provides basin information about connecting and installing a FortiGate unit.

- *FortiGate Installation Guide*

  Described 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 generated by the FortiGate unit.

- *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 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.

The FortiGate online help also contains procedures for using the FortiGate web-based manager to configure and manage the FortiGate unit.

Comments on Fortinet technical documentation

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

Customer service and technical support

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

Please visit the Fortinet Technical Support web site at http://support.fortinet.com
to learn about the technical support services that Fortinet provides.

FORTINET

SOHO and SMB network protection

This document describes an example network and firewall configuration for a small office / home office (SOHO) or a small- to medium-sized business (SMB).

SOHO and SMB networks, in this case, refer to

- small offices
- home offices
- broadband telecommuter sites or large remote access populations
- branch offices (small- to medium-sized)
- retail stores

Note: IP addresses and domain names used in this document are examples and are not valid outside of this example.

This document includes

Example small office network

Description

Company A is a small software company performing development and providing customer support. In addition to their internal network of 15 computers, they also have several employees that work from home all or some of the time.

Company A requires secure connections for home-based workers. Like many companies, they rely heavily on email and Internet access to conduct business. They want a comprehensive security solution to detect and prevent network attacks, block viruses, and decrease spam. They want to apply different protection settings for different departments. They also want to integrate web and email servers into the security solution.

Existing topology

Figure 4:   Example SOHO network before FortiGate installation
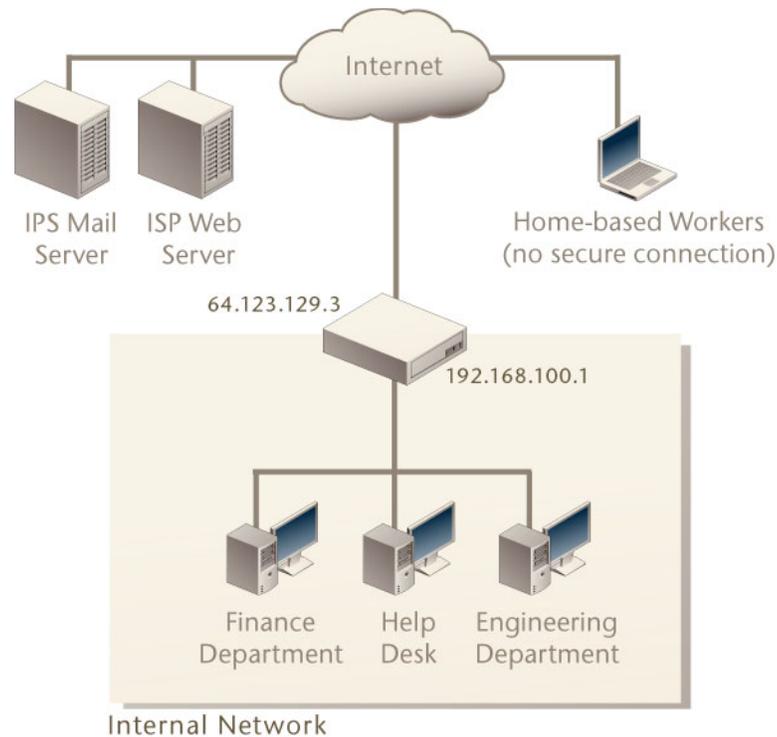
The Company A network provides limited functionality for their needs, including:

• a very basic router to manage the network traffic
• an email server hosted by the Internet Service Provider (ISP)
• a web server hosted by the ISP
• client-based antivirus software with no reliable central distribution of updates
• no secure method of providing remote connections for home-based workers

Network management and protection requirements

Company A established several goals for planning a network security solution.
Table 1 describes the company's goals and the FortiGate options that meet them.

Table 1: Company security goals and FortiGate solutions

Security Policy/Goal	FortiGate solution
Protect the internal network from attacks, intrusions, viruses, and spam.	Enable IPS, antivirus, and spam filters.
Automate network protection as much as possible to make management simpler	There are several features to make maintenance simpler: • enable automatic daily updates of antivirus and attack definitions • enable automatic "push" updates so that Fortinet updates the virus list when new threats occur • enable FortiGuard web filtering so that web requests are automatically filtered based on configured policies, with no required maintenance • enable FortiGuard Antispam, an IP address black list and spam filter service that keeps track of known or suspected spammers, to automatically block spam with no required maintenance
Provide secure access for remote workers with static or dynamic IP addresses. Use a secure VPN client solution.	Configure secure IPSec VPN tunnels for remote access employees. Use Dynamic Domain Name Server (DDNS) VPN for users with dynamic IP addresses. Use the FortiClient software to establish a secure connection between the FortiGate unit and the home-based worker. See "Configuring remote access VPN tunnels" on page 37.
Serve the web site and email from a DMZ to further protect internal data.	Place the web and email servers on the DMZ network and create appropriate policies. See "Configuring the web server" on page 42.
Block access by all employees to potentially offensive web content.	Enable FortiGuard web content filtering solution. See "Configuring web category block settings" on page 24.
Severely limit web access for certain employees (help desk) during work hours.	Create a schedule that covers business hours, create a custom web access solution, and include these in a firewall policy for specific addresses. See "Configuring settings for the Help Desk department" on page 29.

The Fortinet solution

FortiGate models for SOHOs, and SMBs

Table 2 compares the FortiGate models best-suited to the SOHO/SMB environment. All FortiGate models provide complete real-time network protection through a combination of network-based antivirus, web and email content filtering, firewall, VPN, network-based intrusion detection and prevention, and traffic shaping.

Table 2: FortiGate models for SOHO/SMB

Model	Users*	Interfaces	Summary
FortiGate-50A	1 to 5	internal, external, modem	• For small remote offices, retail stores, and telecommuters
FortiGate-60	1 to 25	internal, dmz, wan1, wan2, modem	• For small offices • Dual WAN link support for redundant Internet connections, an integrated 4-port switch, and a DMZ interface
FortiWiFi-60	1 to 25	internal, dmz, wan1, wan2, wlan, modem	• For small offices requiring wireless connectivity • All the features of the FortiGate-60
FortiGate-100A	25 to 35	internal, dmz1, dmz2, wan1, wan2	• For small business, remote/satellite offices • Includes a DMZ interface to support local email and web servers
FortiGate-200A	25 to 50	internal, dmz1, dmz2, wan1, wan2	• For small to mid-sized organizations • An optional internal high capacity hard drive gives this model internal logging capability • Front-panel LCD and keypad ease deployment
FortiGate-300A	50 to 100	Six user definable network interface ports.	• For medium-sized businesses, enterprise branch offices, and large remote access populations • An optional internal high capacity hard drive gives this model internal logging capability • Front-panel LCD and keypad ease deployment

* The number of possible users depends on the use of processor-intensive features such as antivirus and IPS.

FortiClient remote host security software

Fortinet's Remote FortiClient Host Security provides secure remote access to network resources for telecommuters, mobile workers, remote sites, and partners. The FortiClient Host Security is an easy-to-use IPSec software client featuring an integrated personal firewall, Network Address Translation (NAT) Traversal, centralized policy management, multiple policy support for access to multiple devices, strong encryption, and a comprehensive set of tools for troubleshooting. Most popular Microsoft Windows operating systems are supported natively.

The Company A decision

Company A deploys a FortiGate-100A on the network edge to provide secure remote access, network management, and network protection.

Company A requires a DMZ interface for web and email servers but they have minimal logging requirements and do not require a local disk for storage. They require more users and greater performance than the FortiGate-50A provides, making the FortiGate-100A the ideal choice.

Company A also provides home-based workers with the FortiClient software to establish secure connections between the FortiGate unit and the home-based worker.

Proposed topology

Figure 5 shows the Company A network configuration after installation of the FortiGate-100A.

Figure 5:   SOHO network topology with FortiGate-100
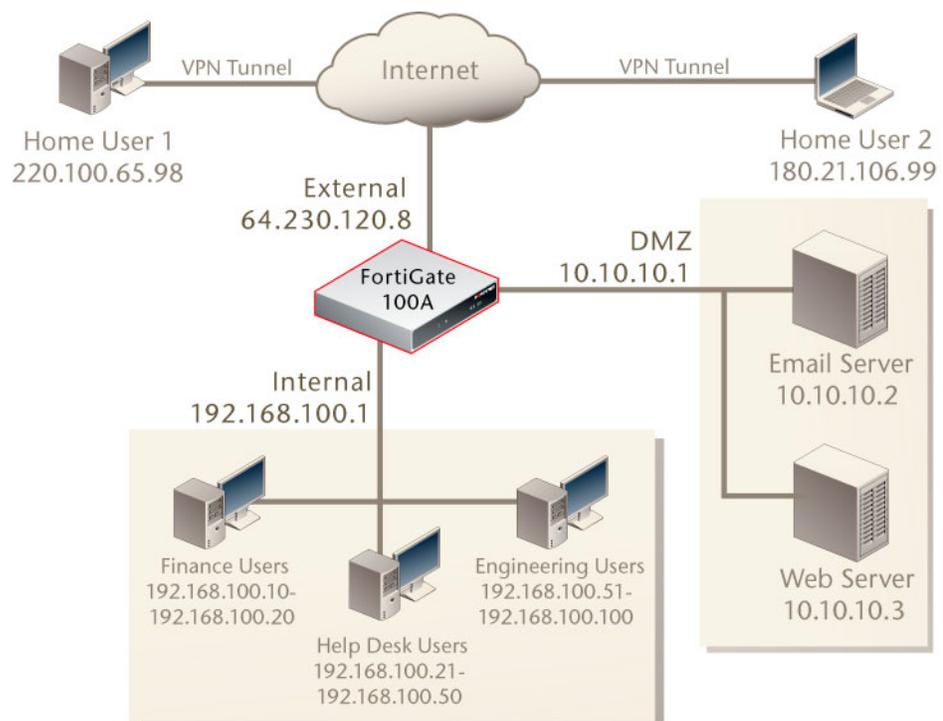
Features used in this example

The following table lists the FortiGate features implemented in the Company A example network.

System	• "Configuring FortiGate network interfaces" on page 17
	• "Configuring DNS forwarding" on page 19
	• "Scheduling automatic antivirus and attack definition updates" on page 21
	• "Setting the time and date" on page 20
	• "Configuring administrative access and passwords" on page 21
	• "Registering the FortiGate unit" on page 20
Router	• "Adding the default route" on page 18
Firewall	• "Removing the default firewall policy" on page 19
	• Adding firewall policies for different addresses and address groups, see "Configuring firewall policies for Finance and Engineering" on page 28, "Configuring firewall policies for help desk" on page 35, and "Configuring firewall policies for the VPN tunnels" on page 40
	• Adding addresses and address groups, see "Adding the Finance and Engineering department addresses" on page 23, "Adding the Help Desk department address" on page 29, "Adding addresses for home-based workers" on page 37, "Adding the web server address" on page 43, and "Adding the email server address" on page 46
	• "Creating a recurring schedule" on page 33
	• Configuring protection profiles, see "Configuring the 'standard_profile' firewall protection profile" on page 27, and "Configuring the 'help_desk' firewall protection profile" on page 33
VPN	• "Configuring remote access VPN tunnels" on page 37 (IPSec)
IPS	• enabling IPS signature and anomaly (see Configuring protection profiles)
	• "Scheduling automatic antivirus and attack definition updates" on page 21
Antivirus	• "Configuring antivirus grayware settings" on page 25
	• enabling virus scanning (see Configuring protection profiles)
	• "Scheduling automatic antivirus and attack definition updates" on page 21
Web Filter	• "Configuring web category block settings" on page 24 (FortiGuard)
	• "Creating and Configuring URL filters and filter lists" on page 30
Spam Filter	• "Configuring FortiGuard spam filter settings" on page 25

First steps

First steps includes creating a network plan and configuring the basic FortiGate settings.

- Creating a network plan
- Configuring FortiGate network interfaces

- Adding the default route
- Removing the default firewall policy
- Configuring DNS forwarding
- Setting the time and date
- Registering the FortiGate unit
- Scheduling automatic antivirus and attack definition updates
- Configuring administrative access and passwords

Creating a network plan

It is essential to collect information for the network settings and design a network topology before configuring the FortiGate unit.

Plan for growth and future needs	What is the company's projected head-count for the next 2 years? Does the company plan to have more home-based workers?
Collect all required addresses	Collect DNS IP addresses, default gateway address, VPN client IP addresses or domain names, etc. Get most of this information from the ISP.
Design a new network topology	Include all the collected addressing information in a network topology diagram.
Complete a plan for each task	For example, configuring settings for a department or user group may include:

- adding the addresses and address groups
- adding schedules if required
- configuring any required global spam filter, web filter, and antivirus settings
- creating a protection profile
- adding a firewall policy for the department

Configuring FortiGate network interfaces

Company A assigns IP addresses to the three FortiGate interfaces to identify them on their respective networks. It is important to limit administrative access to maintain security. Company A configures administrative access for each interface as follows:

Interface	Administrative access
internal	HTTPS for web-based manager access from the internal network, PING for connectivity troubleshooting, and SSH for secure access to the command line interface (CLI) from the internal network.
wan1	HTTPS for remote access to the web-based manager from the Internet.
dmz1	PING access for troubleshooting.

To configure FortiGate network interfaces

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

2   Edit the internal interface:

Addressing mode	Manual
IP/Netmask	192.168.100.1/255.255.255.0
Administrative access	HTTPS, PING, SSH

3   Select OK.

4   Edit the wan1 interface:

Addressing mode	Manual
IP/Netmask	64.230.120.8/255.255.255.0
Administrative access	HTTPS

5   Select OK.

6   Edit the dmz1 interface:

Addressing mode	Manual
IP/Netmask	10.10.10.1/255.255.255.0
Administrative access	PING

7   Select OK.

To configure the FortiGate network interfaces using the CLI

```
config system interface
  edit internal
    set ip 192.168.100.1 255.255.255.0
    set allowaccess ping https ssh
  next
  edit wan1
    set ip 64.230.120.8 255.255.255.0
    set allowaccess https
  next
  edit dmz1
    set ip 10.10.10.1 255.255.255.0
    set allowaccess ping
end
```

Adding the default route

Company A gets the default gateway address from their ISP.

To add the default route

1   Go to **Router > Static**.

2   Select Create New.

3   Enter the following information:

Destination IP/ Mask	0.0.0.0/0.0.0.0
Device	wan1
Gateway	64.230.254.39
Distance	10

FÖRTINET

4 Select OK.

> **Note:** Entering 0.0.0.0 as the IP and mask represents any IP address.

To add the default route using the CLI

```
config router static
  edit 1
    set device wan1
    set gateway 64.230.254.39
    set distance 10
end
```

Removing the default firewall policy

The FortiGate-100 comes preconfigured with a default internal -> wan1 firewall policy which allows any type of traffic from any internal source to connect to the Internet at any time. Company A removes this policy to simplify policy configuration and increase security. By deleting this policy Company A ensures that any traffic which does not match a configured policy is rejected, rather than possibly matching the default policy and passing through the FortiGate unit.

To remove the default firewall policy

1 Go to **Firewall > Policy**.

2 Expand the internal -> wan1 entry.

3 Delete policy 1 (Source: All, Dest: All).

To remove the default firewall policy using the CLI

```
config firewall policy
  delete 1
end
```

Configuring DNS forwarding

After deleting the default firewall policy, configure DNS forwarding from the internal interface to allow DNS requests and replies to pass through the firewall. DNS server addresses are usually provided by the ISP.

To configure DNS forwarding

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

2 For DNS Settings, enter the primary and secondary DNS server addresses:

Primary DNS Server 239.120.20.1
Secondary DNS Server 239.10.30.31

3 Select internal under Enable DNS forwarding.

4 Select Apply.

To configure DNS forwarding using the CLI

```
config system dns
  set autosvr disable
  set primary 239.120.20.1
```

```
        set secondary 239.10.30.31
        set fwdintf internal
end
```

Setting the time and date

Time can be set manually or updated automatically using an NTP server. Company A sets the time manually.

To set the time and date

1   Go to **System > Status** and select the 'change' link after the system time.

2   Select the correct time zone for your location.

3   Select Set Time and set the current time and date.

4   Select OK.

To configure the time zone using the CLI

```
config system global
  set timezone 04
end
```

To configure the time and date using the CLI

```
execute date <yyyy-mm-dd>
execute time <hh:mm:ss>
```

Registering the FortiGate unit

The FortiGate-100 must be registered with Fortinet to receive automatic scheduled updates and push updates. Enter the support contract number during the registration process.

Begin by logging in to the web-based manager.

To register the FortiGate unit

1   Go to **System > Status** and get the product serial number from the Unit Information section or check the label on the bottom of the FortiGate-100.

2   Go to http://support.fortinet.com and click Product Registration.

The registration page on the Fortinet support site appears.

3   Fill in all the required fields including the product model and serial number.

4   Select Finish.

Scheduling automatic antivirus and attack definition updates

Company A schedules daily antivirus and attack definition updates at 5:30 am. They also enable push updates so that critical antivirus or attack definitions are automatically delivered to the FortiGate-100 whenever a threat is imminent.

FortiProtect Distribution Network (FDN) services provide all antivirus and attack updates and information. A virus encyclopedia and an attack encyclopedia with useful protection suggestions, as well as a daily newsletter, are available on the web site at http://www.fortinet.com/FortiProtectCenter/.

To check server access and enable daily and push updates

1   Go to **System > Maintenance > FortiGuard Center**.

2   Make sure the FortiGuard Distribution Network show Available (refresh browser if required).

3   Expand the Antivirus and IPS Options blue arrow.

4   Select Allow Push Update.

5   Select Scheduled Update.

6   Select Daily and select 5 for the hour.

7   Select Apply.

Note: If you want to set the update time to something other than the top of the hour, you must use the CLI command.

To check server access and enable daily and push updates using the CLI

```
config system autoupdate push-update
  set status enable
end
config system autoupdate schedule
  set frequency daily
  set status enable
  set time 05:30
end
```

Configuring administrative access and passwords

Company A adds an administrator account and password using a new read-only access profile. This read-only administrator monitors network activity and views settings. They can notify the admin administrator if changes are required or a critical situation occurs. The read-only administrator can only access the FortiGate web-based manager from their own computer or the lab computer.

The admin administrator gets a new password (default is a blank password).

To configure a new access profile and administrator account

1   Go to **System > Admin > Access Profile**.

2   Select Create New.

3   Enter admin_monitor as the Profile Name.

4   Select Read Only.

New Access Profile			
Profile Name: admin_monitor			
Access Control	☐ **None**	☑ **Read Only**	☐ **Read-Write**
Maintenance	○	⊙	○
Admin Users	○	⊙	○
FortiGuard Update	○	⊙	○
Auth Users	○	⊙	○
System Configuration	○	⊙	○
Network Configuration	○	⊙	○
Log & Report	○	⊙	○
Web Filter Configuration	○	⊙	○
Spam Filter Configuration	○	⊙	○
Antivirus Configuration	○	⊙	○
IPS Configuration	○	⊙	○
Router Configuration	○	⊙	○
VPN Configuration	○	⊙	○
▶ Firewall Configuration	○	⊙	○
OK		Cancel	

5   Select OK.

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

7   Select Create New and enter or select the following settings:

Administrator	admin_2
Password	<psswrd>
Confirm Password	<psswrd>
Trusted Host #1	192.168.100.60 / 255.255.255.0 (administrator's computer)
Trusted Host #2	192.168.100.51 / 255.255.255.0 (lab computer)
Access Profile	admin_monitor

8   Select OK.

To configure a new access profile and administrator account using the CLI

```
config system accprofile
  edit admin_monitor
    set admingrp read
    set authgrp read
    set avgrp read
    set fwgrp read
    set ipsgrp read
    set loggrp read
    set mntgrp read
    set netgrp read
    set routegrp read
    set spamgrp read
    set sysgrp read
    set updategrp read
    set vpngrp read
    set webgrp read
```

```
      end
      config system admin
        edit admin2
          set accprofile admin_monitor
          set password <psswrd>
          set trusthost1 192.168.100.60 255.255.255.0
          set trusthost2 192.168.100.51 255.255.255.0
      end
```

To change the admin password

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

2 Select the Change password icon beside the admin administrator.

Name	Trusted Hosts	Profile	Type	
admin	0.0.0.0/0, 0.0.0.0/0, 127.0.0.1/32		Local	
admin2	192.168.100.0/24, 192.168.100.0/24, 127.0.0.1/32	admin_monitor	Local	
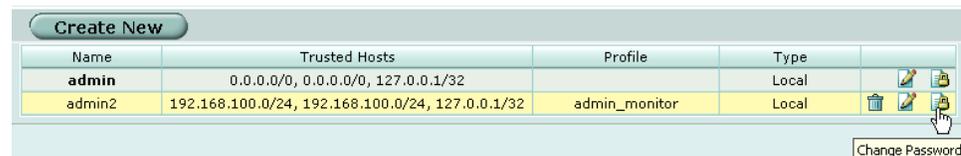
3 Enter the new password and enter it again to confirm.

4 Select OK.

To change the admin password using the CLI

```
      config system admin
        edit admin
        set password <psswrd>
      end
```

Configuring settings for Finance and Engineering departments

Goals

- Provide control of web access. Tasks include:
  - Adding the Finance and Engineering department addresses
  - Configuring web category block settings
- Protect the network from spam and outside threats. Tasks include:
  - Configuring FortiGuard spam filter settings
  - Configuring antivirus grayware settings
  - Configuring the 'standard_profile' firewall protection profile
- Control traffic and maintain security. Tasks include:
  - Configuring firewall policies for Finance and Engineering

Adding the Finance and Engineering department addresses

Firewall addresses and address groups are used to configure connections to and through the FortiGate-100. Each address represents a component of the network that requires configuration with policies.

Company A adds address ranges to the firewall for Finance and Engineering so they can be included in firewall policies. The two address ranges are included in an address group to further simplify policy configuration.

To add address ranges for Finance and Engineering

1   Go to **Firewall > Address**.

2   Select Create New and enter or select the following settings:

Address Name	Finance
Type	Subnet / IP Range
Subnet / IP Range	192.168.100.10
Interface	192.168.100.20

3   Select OK.

4   Repeat to add an address called Eng with the IP Range 192.168.100.51–
192.168.100.99.

To add address ranges for Finance and Engineering using the CLI

```
config firewall address
  edit Finance
    set type iprange
    set start-ip 192.168.100.10
    set end-ip 192.168.100.20
  next
  edit Eng
    set type iprange
    set start-ip 192.168.100.51
    set end-ip 192.168.100.99
end
```

To include the Finance and Eng addresses in an address group

1   Go to **Firewall > Address > Group**.

2   Select Create New.

3   Enter FinEng as the Group Name.

4   Use the down arrow button to move the Finance and Eng addresses into the
Members box.

5   Select OK.

**To include the Finance and Eng addresses in an address group using the
CLI**

```
config firewall addrgrp
  edit FinEng
    set member Finance Eng
end
```

Configuring web category block settings

Company A employs the FortiGuard web filtering service to block access by all
employees to offensive web sites. After ordering the FortiGuard service, licensing
information is automatically obtained from the server.

To enable the FortiGuard web filtering service

1   Go to **System > Maintenance > FortiGuard Center**.

2   Expand Web Filtering and AntiSpam Options.

3 Select Test Availability to make sure the FortiGate unit can access the FortiGuard server. After a moment, the FDN Status should change from a red/yellow flashing indicator to a solid green.

4 Select the Enable Web Filter check box.

5 Select the Enable CacheTTL check box and enter 3600 in the field.

6 Select Apply.

Note: Enabling cache means web site ratings are stored in memory so that the FortiGuard server need not be contacted each time an often-accessed site is requested.

To enable FortiGuard web filtering using the CLI

```
config system fortiguard
  set webfilter-status enable
  set webfilter-cache enable
  set webfilter-cache-ttl 3600
end
```

Configuring FortiGuard spam filter settings

Company A configures spam blocking using FortiGuard, the IP address black list and spam filtering service from Fortinet. FortiGuard works much the same as real-time blackhole lists (RBLs). The FortiGate unit accesses the FortiGuard server, compares addresses against the black list, applies proprietary filters for spam and tags, passes or blocks potential spam messages.

To enable the FortiGuard spam filtering service

1 Go to **System > Maintenance > FortiGuard Center**.

2 Expand Web Filtering and AntiSpam Options.

3 Select the Enable AntiSpam check box.

4 Select the Enable CacheTTL check box and enter 3600 in the field.

5 Select Apply.

Note: Marking email as spam allows end-users to create custom filters to block tagged spam using the keyword.

To configure the FortiGuard RBL spam filter settings using the CLI

```
config system fortiguard
  set antispam-status enable
  set antispam-cache enable
  set antispam-cache-ttl 3600
end
```

Configuring antivirus grayware settings

Company A blocks known grayware programs from being downloaded by employees. Grayware programs are unsolicited commercial software programs that get installed on computers, often without the user's consent or knowledge. The grayware category list and contents are added and updated whenever the FortiGate unit receives a virus update.

To configure grayware settings

1   Go to **AntiVirus > Config > Grayware**.

2   Select Enable for all categories except the Misc (miscellaneous) category.

Virus List	Grayware	
Category		**Enable**
▶ **Adware**		☑
▶ **BHO**		☑
▶ **Dial**		☑
▶ **Download**		☑
▶ **Game**		☑
▶ **HackerTool**		☑
▶ **Hijacker**		☑
▶ **Joke**		☑
▶ **Keylog**		☑
▶ **Misc**		☐
▶ **NMT**		☑
▶ **P2P**		☑
▶ **Plugin**		☑
▶ **RAT**		☑
▶ **Spy**		☑
▶ **Toolbar**		☑

To enable grayware using the CLI

```
config antivirus grayware Adware
  set status enable
end
config antivirus grayware BHO
  set status enable
end
config antivirus grayware Dial
  set status enable
end
config antivirus grayware Download
  set status enable
end
config antivirus grayware Game
  set status enable
end
config antivirus grayware HackerTool
  set status enable
end
config antivirus grayware Hijacker
  set status enable
end
config antivirus grayware Joke
  set status enable
end
config antivirus grayware Keylog
  set status enable
end
config antivirus grayware NMT
  set status enable
end
```

```
config antivirus grayware P2P
  set status enable
end
config antivirus grayware Plugin
  set status enable
end
config antivirus grayware RAT
  set status enable
end
config antivirus grayware Spy
  set status enable
end
config antivirus grayware Toolbar
  set status enable
end
```

Configuring the 'standard_profile' firewall protection profile

Company A configures a firewall protection profile called standard_profile to apply to the Finance and Engineering departments as well as the home-based workers. For detailed information on creating and configuring protection profiles please see the FortiGate Administration Guide.

To create and configure a protection profile

1 Go to **Firewall > Protection Profile.**

2 Select Create New.

3 Enter standard_profile as the Profile Name.

4 Select Anti-Virus and enable Virus Scan for HTTP, FTP, IMAP, POP3, and SMTP.

5 Select FortiGuard Web Filtering and select Enable FortiGuard Web Filtering.

Company A orders FortiGuard for web filtering. FortiGuard gives administrators the option of allowing, blocking, or monitoring web sites in 52 categories. Categories are divided into groups to make configuration easier. Company A configures selected categories as follows:

Potentially Liable	Block
Controversial	
Adult Materials	Block
Extremist Groups	Block
Pornography	Block
Potentially Non-productive	
Games	Block
Potentially Bandwidth Consuming	Block
Potentially Security Violating	Block
General Interest	
Job Search	Block
Shopping and Auction	Block
Personal Relationships	Block

6   Select Spam Filtering and enable SMTP for IP address BWL check and E-mail address BWL check.

7   Select IPS and enable critical level IPS Signatures and IPS Anomalies.

8   Select OK.

To configure the standard_profile firewall protection profile using the CLI

```
config firewall profile
  edit standard_profile
    set ftp scan
    set http scan fortiguard-wf
    set imap scan
    set pop3 scan
    set smtp scan spamipbwl spamemailbwl
    set ips-anomaly critical
    set ips-signature critical
    set ftgd-wf-deny g01 8 12 14 20 g04 g05 34 37 42
end
```

Configuring firewall policies for Finance and Engineering

By configuring firewall policies for specific users you can grant different levels of access to different groups as required. For detailed information on configuring firewall profiles please see the FortiGate Administration Guide.

Important points for firewall policy configuration

*   Policies are organized according to the direction of traffic from the originator of a request to the receiver of the request. For example, even though viruses may come from the external interface, the request for email or a web page comes from the internal interface. Therefore the policy protecting the network would be an internal -> wan1 policy.

*   Policies are matched to traffic in the order they appear in the policy list (not by ID number)

*   Policies should go from most exclusive to most inclusive so that the proper policies are matched. As a simple example, a policy blocking internal to external HTTP access for some employees should come before a policy that allows HTTP access for everyone.

*   Each interface can benefit from layered security created through multiple policies

Note: The following policy is an internal to wan1 policy which uses the standard_profile protection profile to provide antivirus, web category blocking, and FortiGuard spam filtering.

To configure the Finance and Engineering firewall policy

1   Go to **Firewall > Policy**.

2   Select Create New.

3   Enter or select the following settings:

Source Interface / Zone	internal
Source Address	FinEng

Destination Interface / Zone	wan1
Destination Address	All
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Enable
Protection Profile	Enable and select standard_profile

4   Select OK.

To configure the Finance and Engineering firewall policy using the CLI

```
config firewall policy
  edit 1
    set action accept
    set dstaddr all
    set dstintf wan1
    set profile-status enable
    set schedule always
    set service ANY
    set srcaddr FinEng
    set srcintf internal
    set profile standard_profile
end
```

Configuring settings for the Help Desk department

Because of a high turnover rate and a need for increased productivity in the Help Desk department, Company A implements very strict web access settings. Help desk employees can only access four web sites that they require for their work. During lunch hours, help desk employees have greater access to the web but are still blocked from using IM programs and accessing objectionable web sites.

Goals

- Provide complete control of web access. Tasks include:
  - Adding the Help Desk department address
  - Creating and Configuring URL filters and filter lists
- Enable greater access at certain times. Tasks include:
  - Creating a recurring schedule
- Control traffic and maintain security. Tasks include:
  - Configuring firewall policies for help desk

Adding the Help Desk department address

Company A adds an address range for the Help Desk department so it can be included in a separate firewall policy.

To add the help desk department address

1   Go to **Firewall > Address**.

2   Select Create New and enter or select the following settings:

Address Name	Help_Desk
Type	Subnet / IP Range
Subnet / IP Range	192.168.100.21-192.168.100.50
Interface	Any

3   Select OK.

Adding the help desk department address using the CLI

```
config firewall address
  edit Help_Desk
    set type iprange
    set start-ip 192.168.100.21
    set end-ip 192.168.100.50
end
```

Creating and Configuring URL filters and filter lists

Antivirus, spam filter, and web filter are global settings previously configured for the Finance and Engineering set up. In this step Company A adds additional web filter settings to block web access with the exception of four required web sites. Web URL block and web exempt list are then enabled in a firewall policy for help desk employees.

Before you can configure filters, you must first create a list to place the filters in.

To create a filter list for blocked URLs

1   Go to **Web Filter > URL Filter**.

2   Select Create New.

3   Enter CompanyA_Blocked_URLs as the name.

4   Select OK.

To create a filter list for blocked URLs using the CLI

```
config webfilter urlfilter
  edit # (select any unused number)
    set name CompanyA_Blocked_URLs
end
```

To configure a URL block

1   Go to **Web Filter > URL Filter**.

2   Select edit for CompanyA_Blocked_URLs.

3   Select Create New.

4   Enter the following settings:

URL	.*
Type	Simple
Action	Block

5   Select Enable.

6   Select OK.

This pattern blocks all web sites.

To configure URL block using the CLI

```
config webfilter urlfilter
  edit #
    config entries
      edit #
        set action block
        set type simple
        set status enable
      end
  end
```

Note: The edit command will only accept a number. Type "`edit ?`" for a list of URL filter lists and their corresponding number

To create a filter list for exempt URLs

1   Go to **Web Filter > URL Filter**.

2   Select Create New.

3   Enter CompanyA_Support as the name.

4   Select OK.

To create a filter list for exempt URLs using the CLI

```
config webfilter urlfilter
  edit # (select any unused number)
    set name CompanyA_Support
  end
```

To configure a filter to exempt URLs

1   Go to **Web Filter > URL Filter**.

2   Select edit for CompanyA_Support.

3   Select Create New.

4   Enter the following settings:

URL	www.CompanyAsupport.com
Type	Simple
Action	Exempt

5   Select Enable.

6   Select OK.

7   Repeat for each of the following URLs:
- intranet.CompanyA.com
- www.dictionary.com
- www.ExampleReferenceSite.com

To configure URL exempt using the CLI

```
config webfilter urlfilter
```

```
edit #
  config entries
    edit www.CompanyAsupport.com
      set action exempt
      set type simple
      set status enable
next
    edit intranet.CompanyA.com
      set action exempt
      set type simple
      set status enable
next
    edit www.dictionary.com
      set action exempt
      set type simple
      set status enable
next
    edit www.ExampleReferenceSite.com
      set action exempt
      set type simple
      set status enable
end
```

Figure 6: The URL Filter list

Ordering the filtered URLs

While the list includes all the exempt URLs the help desk needs with a global block filter, there is a problem. Since the URL Filter list is parsed from top to bottom, and the block filter appears first, every URL will match the block filter and parsing will stop. The exempt URL statements that follow will never be referenced. To fix this problem, reorder the list to put the global block filter at the end.

To order the filter URLs

1   Select the Move To icon for the ".*" URL.

2   Select After and type www.ExampleReferenceSite.com into the URL field.

3   Select OK.

To order the filtered URLs using the CLI

```
config webfilter urlfilter
  move # after #
end
```

Note: The move command will only accept a number. Type "`move ?`" for a list of URL filter lists and their corresponding numbers.

Figure 7: The properly ordered URL Filter list

Creating a recurring schedule

Company A uses this schedule in a firewall policy for help desk employees to allow greater web access during lunch hours. The schedule is in effect Monday through Saturday from 11:45am to 2pm.

To create a recurring schedule

1   Go to **Firewall > Schedule > Recurring**.

2   Select Create New.

3   Enter lunch as the name for the schedule.

4   Select the days of the week the schedule will be active.

5   Set the Start time as 11:45 and set the Stop time as 14:00.

6   Select OK.

To create a recurring schedule using the CLI

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

Configuring the 'help_desk' firewall protection profile

Company A configures two firewall protection profiles that apply strict settings for the help desk department during work hours and lunch hours. Both IM and P2P communications are blocked in both profiles. The work hours profile does not require category blocking since help desk employees are limited to only four web sites. The lunch hour profile uses extensive category blocking.

To add the work hours protection profile for help desk employees

1   Go to **Firewall > Protection Profile** and select Create New.

2   Enter help_desk_work as the Profile Name.

3   Select Anti-Virus and enable Virus Scan for HTTP, FTP, IMAP, POP3, and SMTP.

4   Select Web Filtering and enable HTTP for Web Content Block and Web Content Exempt.

5   Select Spam Filtering and enable SMTP for IP address BWL check and E-mail address BWL check.

6   Select IPS and enable critical level IPS Signatures and IPS Anomalies.

7   Select IM/P2P and enable examination of the five IM protocol types by selecting the check boxes beside their names in the column headings. Select Block Login for each of the five IM protocols

8   In the same IM/P2P section, select Block from the Action drop down for each of the six P2P protocol types.

9   Select OK.

To add the work hours protection profile for help desk employees using the CLI

```
config firewall profile
  edit help_desk
    set ftp scan
    set http scan urlfilter
    set imap scan
    set pop3 scan
    set smtp scan spamemailbwl spamipbwl
    set ips-signature critical
    set ips-anomaly critical
    set aim enable-inspect block-im
    set icq enable-inspect block-im
    set msn enable-inspect block-im
    set yahoo enable-inspect block-im

    set p2p enable
    set bittorrent block
    set edonkey block
    set gnutella block
    set kazaa block
    set skype block
    set winny block
  end
```

To add the lunch hour protection profile for help desk employees

1   Go to **Firewall > Protection Profile** and select Create New.

2   Enter help_desk_lunch as the Profile Name.

3   Select Anti-Virus and enable Virus Scan for HTTP, FTP, IMAP, POP3, and SMTP.

4   Select FortiGuard Web Filtering and enable category block.

Configure categories as follows:

Potentially Liable	Block
Controversial	Block
Potentially Non-productive	

Games	Block
Potentially Bandwidth Consuming	Block
Potentially Security Violating	Block
General Interest	
Job Search	Block
Personal Relationships	Block
Shopping and Auction	Block
Personal Vehicles	Block

5   Select Spam Filtering and enable SMTP for IP address BWL check and E-mail address BWL check.

6   Select IPS and enable critical level IPS Signatures and IPS Anomalies.

7   Select IM/P2P and enable examination of the five IM protocol types by selecting the check boxes beside their names in the column headings. Select Block Login for each of the five IM protocols

8   In the same IM/P2P section, select Block from the Action drop down for each of the six P2P protocol types.

9   Select OK.

To add the lunch hour protection profile for help desk employees using the CLI

```
config firewall profile
  edit help_desk_lunch
    set ftp scan
    set http scan fortiguard-wf
    set imap scan
    set pop3 scan
    set smtp scan spamemailbwl spamipbwl
    set ips-anomaly critical
    set ips-signature critical
    set ftgd-wf-deny g01 g02 20 g04 g05 34 37 42 48
    set aim enable-inspect block-im
    set icq enable-inspect block-im
    set msn enable-inspect block-im
    set yahoo enable-inspect block-im

    set p2p enable
    set bittorrent block
    set edonkey block
    set gnutella block
    set kazaa block
    set skype block
    set winny block
  end
```

Configuring firewall policies for help desk

Company A configures two firewall policies for the help desk employees, to implement the web block settings and use the schedule for lunch hour web access created above. For tips on firewall policies see "Important points for firewall policy configuration" on page 28.

The first policy is an internal -> wan1 policy which uses the help_desk protection profile to block most web access during working hours. The second policy goes above the first policy and uses the lunch schedule and the help_desk_lunch protection profile to allow web access at lunch.

To create and insert a policy for the help desk

1   Go to **Firewall > Policy**.

2   Expand the internal -> wan1 entry and select the Insert Policy before icon beside policy 1.

3   Enter or select the following settings:

Source Interface / Zone	internal
Source Address	Help_Desk
Destination Interface / Zone	wan1
Destination Address	All
Schedule	Always
Service	ANY
Action	ACCEPT
NAT	Enable
Protection Profile	Enable and select help_desk

4   Select OK.

5   Select the Insert Policy before icon beside policy 2.

Note: The FortiGate unit checks for matching policies in the order they appear in the list (not by policy ID number). For the 'lunch' policy to work, it must go *before* the policy using the help-desk protection profile (above).

6   Enter or select the following settings:

Source Interface / Zone	internal
Source Address	Help_Desk
Destination Interface / Zone	wan1
Destination Address	All
Schedule	lunch
Service	ANY
Action	ACCEPT
NAT	Enable
Protection Profile	Enable and select help_desk_lunch

7   Select OK.

Configuring firewall policies for help desk with the CLI

```
config firewall policy
  edit 2
    set action accept
    set dstaddr all
    set dstintf wan1
    set profile-status enable
```

```
                    set schedule always
                    set service ANY
                    set srcaddr Help_Desk
                    set srcintf internal
                    set profile help_desk
                  next
                  edit 3
                    set action accept
                    set dstaddr all
                    set dstintf wan1
                    set profile-status enable
                    set schedule lunch
                    set service ANY
                    set srcaddr Help_Desk
                    set srcintf internal
                    set profile help_desk_lunch
                  next
                  move 2 before 1
                  move 3 before 2
                end
```

Configuring remote access VPN tunnels

Goals

- Configure a secure connection for home-based workers. Tasks include:
    - Adding addresses for home-based workers
    - Configuring the FortiGate end of the IPSec VPN tunnels
- Control traffic and maintain security. Tasks include:
    - Configuring firewall policies for the VPN tunnels

Adding addresses for home-based workers

To support VPN connections to the internal network, add a firewall address for the Company A internal network.

To support a VPN connection for a home-based employee with a static IP address, add a firewall address for this employee.

Company A uses a Dynamic Domain Name Server (DDNS) VPN configuration for a home-based employee with a dynamic IP address. The DDNS VPN uses the All firewall address.

To add address for home-based workers

1   Go to **Firewall > Address**.

2   Select Create New and enter or select the following settings:

Address Name	CompanyA_Network
Type	Subnet / IP Range
Subnet / IP Range	192.168.100.0
Interface	Any

3   Select OK.

4   Select Create New and enter or select the following settings:

Address Name	Home_User_1
Type	Subnet / IP Range
Subnet / IP Range	220.100.65.98
Interface	Any

5   Select OK.

To add addresses for home-based workers using the CLI

```
config firewall address
  edit CompanyA_Network
    set subnet 192.168.100.0 255.255.255.0
  next
  edit Home_User_1
    set subnet 220.100.65.98 255.255.255.0
end
```

Configuring the FortiGate end of the IPSec VPN tunnels

Company A uses AutoIKE preshared keys to establish IPSec VPN tunnels between the internal network and the remote workers.

Home_User_1 has a static IP address with a straightforward configuration.

Home_User_2 has a dynamic IP address and therefore some preparation is required. Company A will register this home-based worker with a domain name. The DDNS servers remap the IP address to the domain name whenever Home_User_2 gets a new IP address assigned by their ISP.

Company A home-based workers use FortiClient software for VPN configuration.

To configure IPSec phase 1

1   Go to **VPN > IPSEC > Auto Key (IKE)**

2   Select Create Phase 1.

3   Enter or select the following settings for Home_User_1:

Name	Home1 (The name for the peer that connects to the Company A network.)
Remote Gateway	Static IP Address
IP Address	220.100.65.98
Local Interface	wan1
Mode	Main (ID protection) Note: The VPN peers must use the same mode.
Authentication Method	Preshared Key
Pre-shared Key	ke8S5hOqpG73Lz4 Note: 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 VPN peers must use the same preshared key.
Peer options	Accept any peer ID

4   Select OK.

5   Select Create Phase 1.

6   Enter or select the following settings for Home_User_2:

Name	Home2 (The name for the peer that connects to the Company A network.)
Remote Gateway	Dynamic DNS
Dynamic DNS	example.net
Local Interface	wan1
Mode	Main (ID protection) Note: The VPN peers must use the same mode.
Authentication Method	Preshared Key
Pre-shared Key	GT3wlf76FKN5f43U Note: 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 VPN peers must use the same preshared key.
Peer options	Accept any peer ID

7   Select OK.

Note: Both ends (peers) of the VPN tunnel must use the same mode and authentication method.

To configure IPSec phase 1 using the CLI

```
config vpn ipsec phase1
  edit Home1
    set type static
    set interface wan1
    set authmethod psk
    set psksecret ke8S5hOqpG73Lz4
    set remote-gw 220.100.65.98
    set peertype any
  next
  edit Home2
    set type ddns
    set interface wan1
    set authmethod psk
    set psksecret GT3wlf76FKN5f43U
    set remotewgw-ddns example.net
    set peertype any
  end
```

To configure IPSec phase 2

1   Go to **VPN > IPSEC > Auto Key (IKE)**

2   Select Create Phase 2.

3   Enter or select the following settings:

Name	Home1_Tunnel
Phase 1	Home1

4   Select OK.

5   Select Create Phase 2.

6   Enter or select the following settings:

Name	Home2_Tunnel
Phase 1	Home2

7   Select OK.

To configure IPSec phase 2 using the CLI

```
config vpn ipsec phase2
  edit Home1_Tunnel
    set phase1name Home1
  next
  edit Home2_Tunnel
    set phase1name Home2
end
```

Configuring firewall policies for the VPN tunnels

Company A configures specific policies for each home-based worker to ensure
secure communication between the home-based worker and the internal network.

To configure firewall policies for the VPN tunnels

1   Go to **Firewall > Policy**.

2   Select Create New and enter or select the following settings for Home_User_1:

Source Interface / Zone	internal
Source Address	CompanyA_Network
Destination Interface / Zone	wan1
Destination Address	Home_User_1
Schedule	Always
Service	ANY
Action	IPSEC
VPN Tunnel	Home1
Allow Inbound	yes
Allow outbound	yes
Inbound NAT	yes
Outbound NAT	no
Protection Profile	Enable and select standard_profile

3   Select OK

4   Select Create New and enter or select the following settings for Home_User_2:

Source Interface / Zone	internal
Source Address	CompanyA_Network
Destination Interface / Zone	wan1
Destination Address	All
Schedule	Always
Service	ANY
Action	IPSEC
VPN Tunnel	Home2_Tunnel
Allow Inbound	yes
Allow outbound	yes
Inbound NAT	yes
Outbound NAT	no
Protection Profile	Enable and select standard_profile

5   Select OK

To configure firewall policies for the VPN tunnels using the CLI

```
config firewall policy
  edit 5
    set srcintf internal
    set dstintf wan1
    set srcaddr CompanyA_Network
    set dstaddr Home_User_1
    set action ipsec
    set schedule Always
    set service ANY
    set profile-status enable
    set profile standard_profile
    set inbound enable
    set outbound enable
    set natinbound enable
    set vpntunnel Home1
  next
  edit 6
    set srcintf internal
    set dstintf wan1
    set srcaddr CompanyA_Network
    set dstaddr All
    set action ipsec
    set schedule Always
    set service ANY
    set profile_status enable
    set profile standard_profile
    set inbound enable
    set outbound enable
    set natinbound enable
    set vpntunnel Home2
  end
```

Configuring the FortiClient end of the IPSec VPN tunnels

Fortinet has a complete range of network security products. FortiClient software is a secure remote access client for Windows computers. Home-based workers can use FortiClient to establish VPN connections with remote networks. For more information about installing and configuring FortiClient please see the *FortiClient Installation Guide*.

Note: The specific configuration given in this example will only function with licensed copies of the FortiClient software. The default encryption and authentication types on the FortiGate unit are not available on the FortiClient Demo software.

To configure FortiClient for Home_User_1 and Home_User_2

1   Open the FortiClient software on Home_User_1's computer.

2   Go to **VPN > Connections**.

3   Select Add.

4   Enter the following information:

Connection Name	Home1_home (A descriptive name for the connection.)
Configuration	Manual
Remote Gateway	64.230.120.8 (The FortiGate external interface IP address.)
Remote Network	192.168.100.1 / 255.255.255.0 (The Company A internal network address and netmask.)
Authentication method	Preshared Key
Preshared key	ke8S5hOqpG73Lz4 (The preshared key entered in phase 1.)

5   Select OK.

6   Repeat on Home_User_2's computer for Home_User_2.

Configuring the web server

Goals

- Host the web server on a separate but secure DMZ network
- Hide the internal IP address of the web server. Tasks include:
    - Configuring the FortiGate unit with a virtual IP
- Control traffic and maintain security. Tasks include:
    - Adding the web server address
    - Configuring firewall policies for the web server

Alternately, Company A could have their web server hosted by an ISP. See "ISP web site and email hosting" on page 49.

Configuring the FortiGate unit with a virtual IP

With the web server located on the DMZ interface, Company A configures a virtual IP (VIP) address so that incoming requests for the web site are routed correctly. The virtual IP can be included later in wan1 -> dmz1 firewall policies.

To configure the FortiGate unit with a virtual IP

1   Go to **Firewall > Virtual IP**.

2   Select Create New and enter or select the following settings:

Name	Web_Server_VIP
External Interface	wan1
Type	Static NAT
External IP Address/ Range	64.230.125.70
Mapped IP Address/ Range	10.10.10.2

3   Select OK.

To configure a virtual IP using the CLI

```
config firewall vip
  edit Web_Server_VIP
    set extintf wan1
    set extip 64.230.125.70
    set mappedip 10.10.10.2
end
```

Adding the web server address

Company A adds the web server address to the firewall so it can be included later in firewall policies.

To add the web server address

1   Go to **Firewall > Address**.

2   Select Create New and enter or select the following settings:

Address Name	Web_Server
Type	Subnet/ IP Range
Subnet/ IP Range	10.10.10.2/255.255.255.0
Interface	Any

3   Select OK.

To add the web server address using the CLI

```
config firewall address
  edit Web_Server
    set subnet 10.10.10.2 255.255.255.0
end
```

Configuring firewall policies for the web server

wan1 -> dmz1 policies

Add a policy for users on the Internet (wan1) to access the Company A web site on the DMZ network.

To add a policy for web server access

1   Go to **Firewall > Policy**.

2   Select Create New and enter or select the following settings:

Source Interface / Zone	wan1
Source Address	All
Destination Interface / Zone	dmz1
Destination Address	Web_Server_VIP
Schedule	Always
Service	HTTP
Action	ACCEPT
Protection Profile	Enable and select standard_profile

3   Select OK.

To add a policy for web server access using the CLI

```
config firewall policy
  edit 7
    set action accept
    set schedule always
    set service HTTP
    set srcaddr all
    set srcintf wan1
    set dstaddr Web_Server_VIP
    set dstintf dmz1
    set profile-status enable
    set profile standard_profile
  end
```

dmz1 -> wan1 policies

Company A does not require any dmz1 -> wan1 policies since there is no reason
for the server to initiate requests to the external interface.

dmz1 -> internal policies

Company A does not require any dmz1 -> internal policies since there is no
reason for the server to initiate requests to the internal interface.

internal -> dmz1 policies

Add a policy for the web developer to upload an updated web site to the web
server using FTP.

To add the web master address to the firewall

1   Go to **Firewall > Address**.

2   Select Create New and enter or select the following settings:

Address Name	Web_Master_J
Type	Subnet/ IP Range

Subnet/ IP Range   192.162.100.63/255.255.255.0

Interface   Any

3   Select OK.

To add the web master address to the firewall using the CLI

```
config firewall address
  edit Web_Master_J
    set subnet 192.168.100.63 255.255.255.0
  end
```

To add a policy for web master access to the web server

1   Go to **Firewall > Policy**.

2   Select Create New and enter or select the following settings:

Source Interface / Zone   internal

Source Address   Web_Master_J

Destination Interface / Zone dmz1

Destination Address   Web_Server

Schedule   Always

Service   FTP

Action   ACCEPT

Protection Profile   Enable and select standard_profile

3   Select OK.

To add a policy for web master access to the web server using the CLI

```
config firewall policy
  edit 8
    set action accept
    set dstaddr Web_Server
    set dstintf dmz1
    set schedule always
    set service FTP
    set srcaddr Web_Master_J
    set srcintf internal
    set profile-status enable
    set profile standard_profile
  end
```

Configuring the email server

Goals

- Host the email server on a separate but secure network
- Hide the internal IP addresses of the servers. Tasks include:
  - Configuring the FortiGate unit with a virtual IP

• Control traffic and maintain security. Tasks include:

   • Adding the email server address
   • Configuring firewall policies for the email server

Alternately, Company A could have their email server hosted by an ISP. See "ISP web site and email hosting" on page 49.

Configuring the FortiGate unit with a virtual IP

With the email server on the DMZ network, Company A uses a virtual IP (VIP) address so that incoming email requests are routed correctly. Company A uses the IP address of the FortiGate wan1 interface for email and any SMTP or POP3 traffic is forwarded to the email server on the DMZ. The virtual IP can be included later in wan1 -> dmz1 firewall policies.

To configure a virtual IP

1   Go to **Firewall > Virtual IP**.

2   Select Create New and enter or select the following settings:

Name	Email_Server_VIP
External Interface	wan1
Type	Static NAT
External IP Address/ Range	64.230.120.8
Mapped IP address/ Range	10.10.10.3

3   Select OK.

To configure a virtual IP using the CLI

```
config firewall vip
  edit Email_Server_VIP
    set extintf wan1
    set extip 64.230.120.8
    set mappedip 10.10.10.3
end
```

Adding the email server address

Company A adds the email server address to the firewall so it can be included later in firewall policies.

To add the email server address to the firewall

1   Go to **Firewall > Address**.

2   Select Create New and enter or select the following settings:

Address Name	Email_Server
Type	Subnet/ IP Range
Subnet/ IP Range	10.10.10.3/255.255.255.0
Interface	Any

3   Select OK.

To add the email server address to the firewall using the CLI

```
config firewall address
  edit Email_Server
    set subnet 64.230.120.8 255.255.255.0
end
```

Configuring firewall policies for the email server

Add and configure firewall policies to allow the email servers to properly handle emails.

dmz1 –> wan1 policies

Add a firewall policy to allow the email server to forward messages to external mail servers.

To add a dmz1 -> wan1 firewall policy

1   Go to **Firewall > Policy** and select Create New.

2   Enter or select the following settings:

Source Interface / Zone	dmz1
Source Address	Email_Server
Destination Interface / Zone	wan1
Destination Address	All
Schedule	Always
Service	SMTP
Action	ACCEPT
Protection Profile	Enable and select standard_profile

3   Select OK.

To add a dmz1 -> wan1 firewall policy using the CLI

```
config firewall policy
  edit 9
    set action accept
    set dstaddr all
    set dstintf wan1
    set schedule always
    set service SMTP
    set srcaddr Email_Server
    set srcintf dmz1
    set profile-status enable
    set profile standard_profile
end
```

wan1 –> dmz1 policies

Add a policy to allow Internet email servers to forward messages to the email server.

To add a wan1 -> dmz1 firewall policy

1   Go to **Firewall > Policy** and select Create New.

2   Enter or select the following settings:

Source Interface / Zone	wan1
Source Address	All
Destination Interface / Zone	dmz1
Destination Address	Email_Server_VIP
Schedule	Always
Service	SMTP
Action	ACCEPT
Protection Profile	Enable and select standard_profile

3   Select OK.

To add a wan1 –> dmz1 firewall policy using the CLI

```
config firewall policy
  edit 10
    set action accept
    set srcintf wan1
    set srcaddr all
    set dstintf dmz1
    set dstaddr Email_Server_VIP
    set schedule always
    set service SMTP
    set profile-status enable
    set profile standard_profile
end
```

dmz1 –> internal policies

Company A does not require any dmz –> internal policies since there is no reason for the server to initiate requests to the internal network.

internal –> dmz1 policies

Company A needs to add two internal -> dmz1 policies. One policy for internal users to send outgoing messages to the server (SMTP) and a second policy for internal users to read incoming mail (POP3).

To add internal -> dmz1 firewall policies

1   Go to **Firewall > Policy** and select Create New.

2   Enter or select the following settings:

Source Interface / Zone	internal
Source Address	All
Destination Interface / Zone	dmz1
Destination Address	Email_Server
Schedule	Always
Service	SMTP

Action	ACCEPT
Protection Profile	Enable and select standard_profile

3 Select OK.

4 Select Create New and enter or select the following settings:

Source Interface / Zone	internal
Source Address	All
Destination Interface / Zone	dmz1
Destination Address	Email_Server
Schedule	Always
Service	POP3
Action	ACCEPT
Protection Profile	Enable and select standard_profile

5 Select OK.

To add internal -> dmz1 firewall policies using the CLI

```
config firewall policy
  edit 11
    set action accept
    set dstaddr Email_Server
    set dstintf dmz1
    set schedule always
    set service SMTP
    set srcaddr all
    set srcintf internal
    set profile-status enable
    set profile standard_profile
  next
  edit 12
    set action accept
    set dstaddr Email_Server
    set dstintf dmz1
    set schedule always
    set service POP3
    set srcaddr all
    set srcintf internal
    set profile_status enable
    set profile standard_profile
end
```

ISP web site and email hosting

Small companies such as Company A often find it more convenient and less costly to have their email and web servers hosted by an ISP. This scenario would change the Company A example in the following ways:

- no need to set up a separate DMZ network
- no need to create policies for external access to the web or email servers

- add an internal -> wan1 firewall policy for the web master to upload web site updates via FTP
- add an internal -> wan1 POP3 firewall policy so that users can use POP3 to download email
- add an internal -> wan1 SMTP firewall policy so that users can use SMTP to send email

Company A internal network configuration

The Company A internal network only requires a few changes to individual computers to route all traffic correctly through the FortiGate-100A.

- set the IP addresses within the prescribed ranges for each computer on the network (see Figure 5 on page 15)
- set the default gateway to the IP address of the FortiGate internal interface for each computer on the network
- set the DNS server to the IP address of the FortiGate internal interface for each computer on the network

Other features and products for SOHO

Small or branch offices can use the FortiGate unit to provide a secure connection between the branch and the main office.

Other tasks or products to consider:

- Configuring logging and alert email for critical events
- Backing up the FortiGate configuration
- Enabling Internet browsing for the home users through the VPN tunnel to ensure no unencrypted information enters or leaves the remote site
- VoIP communications between branches

Index

FEIRTINET

www.fortinet.com