



# Configuration Example

## **FortiGate Enterprise Version 3.0 MR6**

**FORTINET™**

[www.fortinet.com](http://www.fortinet.com)

*FortiGate Enterprise Configuration Example*  
Version 3.0 MR6  
March 5, 2008  
01-30006-0315-20080305

© Copyright 2008 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.

**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

<b>Introduction .....</b>	<b>7</b>
<b>FortiGate Unified Threat Management Systems .....</b>	<b>8</b>
<b>Enterprise network protection.....</b>	<b>8</b>
<b>Other Fortinet products .....</b>	<b>9</b>
FortiGuard service.....	9
FortiClient software .....	9
FortiManager system .....	9
FortiAnalyzer systems.....	9
<b>Fortinet documentation .....</b>	<b>10</b>
Fortinet Knowledge Center .....	11
Comments on Fortinet technical documentation .....	11
<b>Customer service and technical support .....</b>	<b>11</b>
<b>Example library network.....</b>	<b>13</b>
<b>Current topology and security concerns .....</b>	<b>13</b>
<b>Library requirements.....</b>	<b>14</b>
<b>The Fortinet solution .....</b>	<b>16</b>
<b>The library’s decision.....</b>	<b>16</b>
<b>Proposed topology .....</b>	<b>16</b>
<b>Features used in this example .....</b>	<b>19</b>
<b>Network addressing .....</b>	<b>20</b>
<b>Configuring the main office .....</b>	<b>21</b>
<b>Topology.....</b>	<b>21</b>
<b>High Availability (HA) .....</b>	<b>22</b>
Configuring HA.....	22
To connect the cluster units.....	22
To configure the primary unit.....	22
To configure the subordinate unit .....	23
<b>FortiGuard .....</b>	<b>23</b>
<b>IPSEC VPN.....</b>	<b>24</b>
Configuring IPSEC VPNs.....	25
To create the main office VPN connection to branch 1 .....	25
To configure the Phase 2 portion of the VPN connection to Branch 1 ..	25
<b>IP Pools.....</b>	<b>25</b>
Configuring IP pools.....	26
To add a new IP pool for public access users. ....	26
<b>User Disclaimer.....</b>	<b>26</b>
Configuring the user disclaimer.....	26

<b>Protection Profiles</b> .....	<b>27</b>
To create a protection profile.....	27
<b>Staff access</b> .....	<b>31</b>
Creating firewall policy for staff members .....	32
Step-by-step policy creation example.....	32
<b>Catalog terminals</b> .....	<b>33</b>
Creating firewall policies for catalog terminals.....	33
<b>Public access terminals</b> .....	<b>34</b>
Creating firewall policies for public access terminals.....	34
<b>Wireless access</b> .....	<b>35</b>
Security considerations.....	36
Creating schedules for wireless access.....	36
To create Monday to Thursday business hours schedule .....	36
To create Friday and Saturday business hours schedule .....	37
To create Sunday business hours schedule.....	37
Creating firewall policies for WiFi access.....	37
<b>Mail and web servers</b> .....	<b>39</b>
Creating a virtual IP for the web server.....	40
To create a virtual IP for the web server.....	40
Creating a virtual IP for the email server.....	40
To create a virtual IP for the email server.....	40
Creating a server service group .....	41
To create a server service group.....	41
Creating firewall policies to protect email and web servers .....	41
<b>The FortiWiFi-60A</b> .....	<b>42</b>
Configuring the main office FortiWiFi-60.....	42
To Configure the operation mode.....	42
<b>Configuring branch offices</b> .....	<b>44</b>
<b>Topology</b> .....	<b>44</b>
<b>Staff access</b> .....	<b>45</b>
<b>Catalog terminals</b> .....	<b>45</b>
<b>Wireless/public access</b> .....	<b>45</b>
<b>Mail and web servers</b> .....	<b>45</b>
<b>IPSEC VPN</b> .....	<b>45</b>
To create the Phase 1 portion of the VPN to the main office .....	45
To create the Phase 2 portion of the VPN to the main office .....	46
<b>Branch Firewall Policy</b> .....	<b>46</b>
Creating firewall policy for the branch office .....	46
<b>Traffic shaping</b> .....	<b>48</b>
<b>Priorities</b> .....	<b>48</b>

<b>The future.....</b>	<b>51</b>
<b>Logging.....</b>	<b>51</b>
<b>Decentralization.....</b>	<b>51</b>
<b>Staff WiFi.....</b>	<b>51</b>
<b>Further redundancy.....</b>	<b>51</b>



# Introduction

This *FortiGate Configuration Example* for enterprise-level business provides a brief overview of FortiGate Unified Threat Management Systems, and a comprehensive example of a network implementation for a large city library system, with a central main office and more than a dozen branch offices.

In this case, enterprise networks refer to

- large businesses/organizations
- government offices
- large Internet service providers

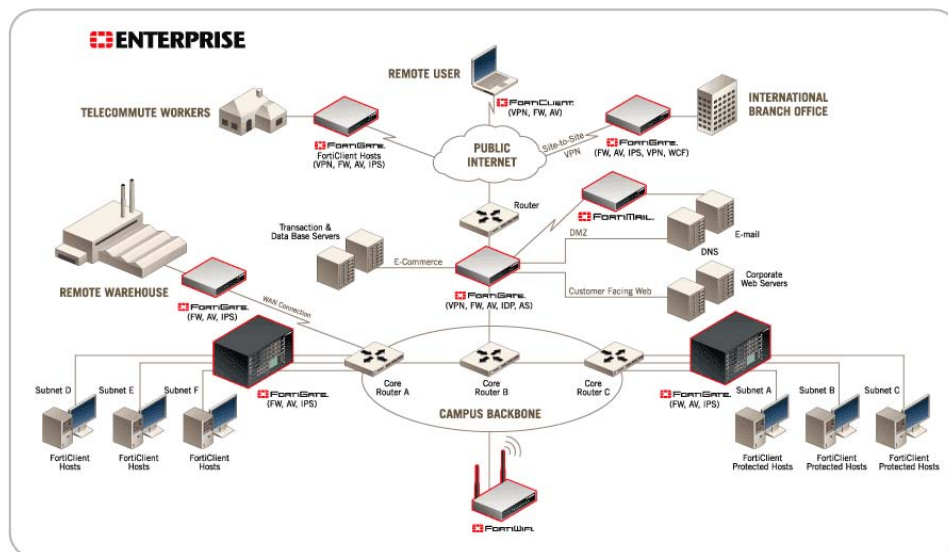
This example employs some of the most common FortiGate security features and can be adapted to planning your own network security solution.

This introduction contains the following topics:

- [FortiGate Unified Threat Management Systems](#)
- [FortiGate Unified Threat Management Systems](#)
- [Other Fortinet products](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

## 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.

## Enterprise network protection

This document describes an example network and firewall configuration for an enterprise level organization. A main office houses mail and web servers while multiple branch offices require access to those resources.



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

## 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 Subscription Services are security services created, updated and managed by a global team of Fortinet security professionals. They ensure the latest attacks are detected and blocked before harming your corporate resources or infecting your end-user computing devices. These services are created with the latest security technology and designed to operate with the lowest possible operational costs.

FortiGuard Subscription Services includes:

- FortiGuard Antivirus Service
- FortiGuard Intrusion Prevention subscription services (IPS)
- FortiGuard Web Filtering
- FortiGuard Antispam Service
- FortiGuard Premier Service

An online virus scanner and virus encyclopedia is also available for your reference. Additional information is available on the FortiGuard Center web page located at <http://www.fortinet.com/FortiGuardCenter/>.

### 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 system

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

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiGate product documentation](#) is available:

- *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*  
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*  
Available exclusively from the [Fortinet Knowledge Center](#), the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages generated by FortiGate units.
- *FortiGate High Availability User Guide*  
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*  
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*  
Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.

- *FortiGate SSL VPN User Guide*  
Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*  
Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management User Guide*  
Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*  
Describes how to configure VLANs and VDOMs in both NAT/Route and Transparent mode. Includes detailed examples.

## Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and 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](mailto:techdoc@fortinet.com).

## Customer service and technical support

Fortinet Technical Support provides services designed to make sure 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 Fortinet provides.



# Example library network

Located in a large city, the library system is anchored by a main downtown location serving most of the population, with a dozen branches spread throughout the city. Each branch is wired to the Internet but none are linked with each other by dedicated connections.

## Current topology and security concerns

Each office connects to the Internet with no standard access policy or centralized management and monitoring.

The library system does not log Internet traffic and does not have the means to do so on a system-wide basis. In the event of legal action involving network activity, the library system will need this information to protect itself.

The branches currently communicate with the main office through the Internet with no encryption. This is of particular concern because all staff members access the central email server in the main office. Email sent to or from branch office staff could be intercepted.

Both the main and branch offices are protected from the Internet by firewalls. This protection is limited to defending against unauthorized intrusion. No virus, worm, phishing, or spyware defences protect the network, resulting in computer downtime when an infection strikes.

Like the branches, the main office is protected by a single firewall device connected the Internet. Should this device fail, connectivity will be lost. The library system's web page and catalog are mission critical applications and access would be better protected by redundant hardware.

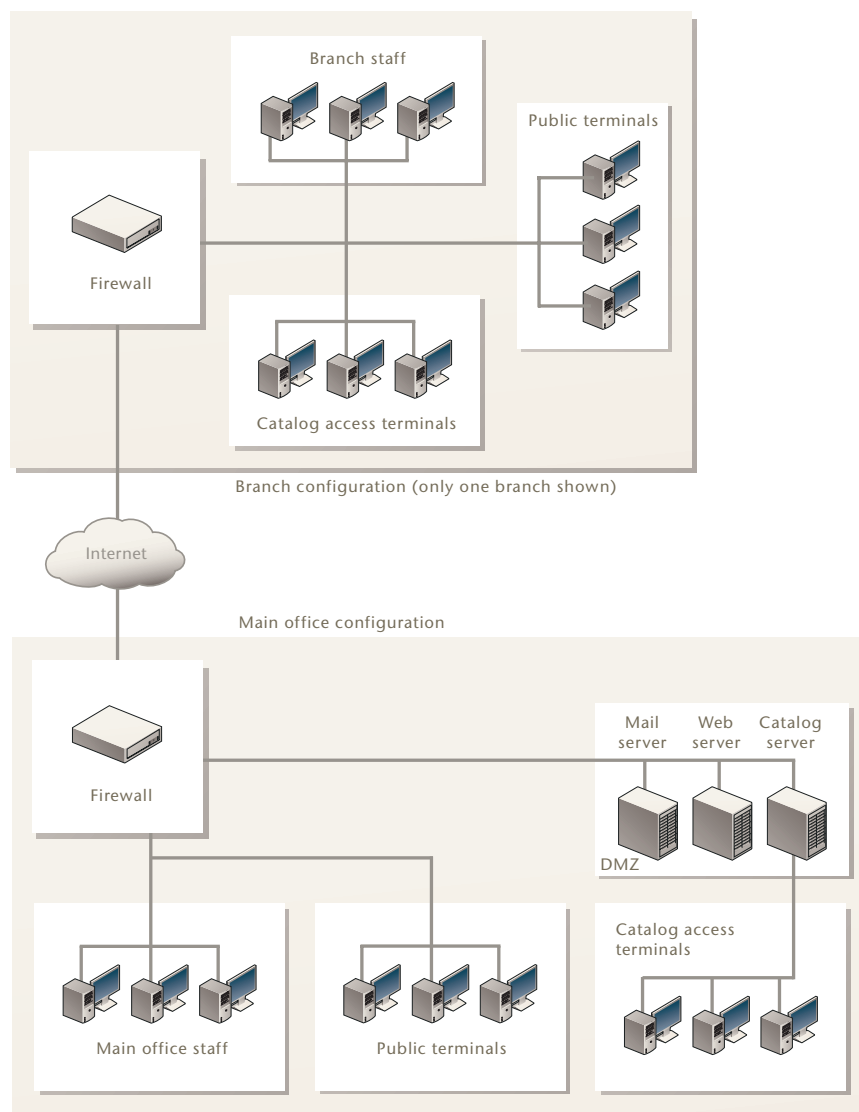
The internal network at each location has staff computers and public access terminals connected together. Concerns have been raised over possible vulnerabilities involving staff computers and public terminals sharing the same network.

Budgetary constraints limit the number of public access terminals the library can provide. With the popularity of WiFi enabled laptops, the addition of a wireless access point is an economical way to allow library patrons to access the Internet using their own equipment.

Efficient use of the library's limited public access terminals and bandwidth can be compromised by the installation and use of instant messaging and peer to peer file sharing applications.

Use of library resources to browse inappropriate content is a problem. These activities are prohibited by library policies, but there is no technical means of enforcement, leaving it to the staff to monitor usage as best they can.

Figure 1: The library system's current network topology



## Library requirements

- VPN to secure all traffic between main and branch offices.
- Public wireless Internet access for mobile clients.
- Strict separation of public access terminals from staff computers.
- An automatically maintained and updated system for stopping viruses and intrusions at the firewall.
- Instant messaging is blocked for public Internet terminals and public wireless access, but not for staff. Peer-to-peer downloads are blocked network-wide.
- All Internet traffic from branch offices travels securely to the main office and then out onto the Internet. Inbound traffic follows the reverse route. This allows a single point at which all protection profiles and policies may be applied for simplified and consistent management.

- The ability to block specific web sites and whole categories of sites from those using the public terminals and public wireless access if deemed necessary. Users granted special permission should be allowed to bypass the restrictions.
- Public access traffic originates from a different address than staff and server traffic.
- DMZ for web and email server hosting in main office.
- The library catalog is available on the library's web page allowing public access from anywhere.
- Redundant hardware for main office firewall.

# The Fortinet solution

## The library's decision

Every model of the FortiGate Dynamic Threat Prevention System offers real time network protection to detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time — without degrading network performance.

The library decided to standardize on the FortiGate-800 and the FortiWiFi-60A:

- Two FortiGate-800 units for main office. These enterprise-level devices have the processing power and speed to handle the amount of traffic expected of a large busy library system with public catalog searches, normal staff use, and on-site research using the Internet as a resource. The two units are interconnected in HA (high availability) mode to ensure uninterrupted service in the case of failure. A FortiWiFi-60A is also used to provide wireless access for patrons in main office.
- A FortiWiFi-60A for each branch office. In addition to being able to handle the amount of traffic expected of a branch office, the FortiWiFi-60A provides wireless access for library patrons.

## Proposed topology

Figure 2 shows the proposed network topology utilizing the FortiGate units. Only one branch office is shown in the diagram although more than a dozen are configured in the same way, including the VPN connection to the main office.

The VPN connections between the branch offices and the main office are a critical feature securing communication between locations.

The two FortiGate-800 units in HA mode serve as the only point through which traffic flows between the Internet and the library's network, including the branch offices. VPN connections between the main and branch offices provide the means to securely send data in either direction.

Branch Internet browsing traffic is routed to the main office through the VPN by the branch's FortiWiFi-60A. After reaching the FortiGate-800 at the main office, the traffic continues out to the Internet. Inbound traffic follows the same path back to the branch office.

With two FortiGate-800 units in HA mode serving as a single point of contact to the Internet, only two FortiGuard subscriptions are required to protect the entire network. Otherwise each branch would also need separate FortiGuard subscription. The FortiGuard web filtering service can also be configured on the FortiGate-800 units, ensuring consistent web filtering policies for all locations.

No provision is made for direct communication between branches.

Figure 2: Proposed library system network topology

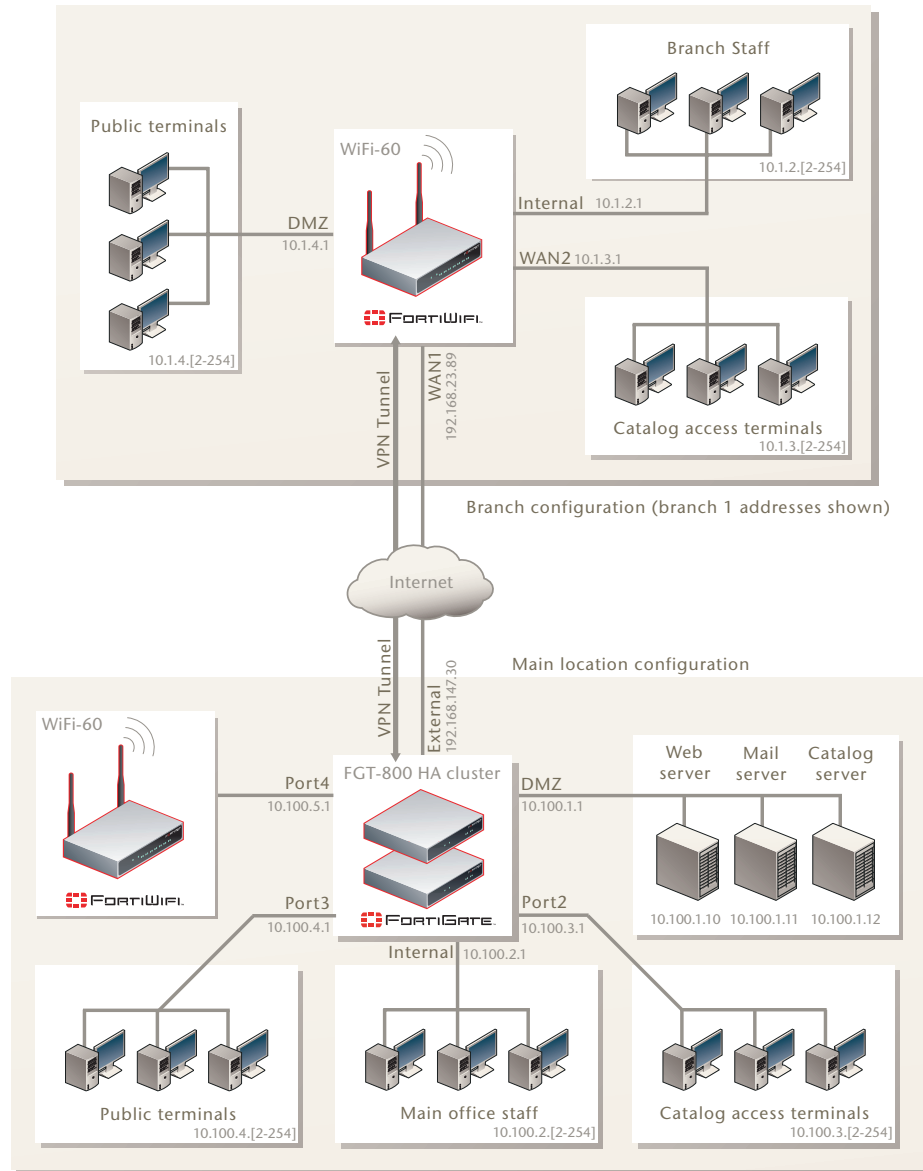


Table 1 on page 18 details the allowed connectivity between different parts of the network.

Table 1: Access permission between various parts of the network

		Connecting to:									
		Branch Staff	Branch Public Access	Branch Catalog access	Main Staff	Main Catalog	Main Public Access	Web Server	Mail Server	Catalog Server	Internet Access
Connecting from:	Branch staff		No	No	No	No	No	Yes	Yes	Yes*	Yes
	Branch Public Access	No		No	No	No	No	Yes	No	Yes*	Yes
	Branch Catalog access	No	No		No	No	No	Yes	No	Yes*	No
	Main Staff	No	No	No		No	No	Yes	Yes	Yes*	Yes
	Main Catalog	No	No	No	No		No	Yes	No	Yes*	No
	Main Public Access	No	No	No	No	No		Yes	No	Yes*	Yes
	Web Server	No	No	No	No	No	No		No	Yes	No
	Mail Server	No	No	No	No	No	No	No		No	Yes
	Catalog Server	No	No	No	No	No	No	No	No		No
	Internet	No	No	No	No	No	No	Yes	Yes†	Yes†	

†Only SMTP connections are permitted from the Internet to the mail server.

\* An indirect connection. Access to the catalog is through the library web page. Direct connections to the catalog server are not permitted.

## Features used in this example

**Table 2: Features used to fulfil requirements**

Feature requirement	Location in this example	Description
Secure communication between each branch and the main office.	<a href="#">"IPSEC VPN" on page 24</a>	Traffic between the each branch and the main office is encrypted.
WiFi access for mobile clients.	<a href="#">"Wireless access" on page 35</a>	The FortiWiFi-60A provides WiFi access.
Strict separation of public access terminals from staff computers.	<a href="#">"Topology" on page 21</a>	Traffic is permitted between network interfaces only when policies explicitly allow it.
An automatically maintained and updated system for stopping viruses and intrusions at the firewall.	<a href="#">"FortiGuard" on page 23</a>	The FortiGuard Subscription service keeps antivirus and intrusion prevention signatures up to date. Also included is a spam blacklist and a web filtering service.
Instant messaging blocked for public access, and P2P blocked system-wide.	<a href="#">"Protection profiles, IM/P2P" on page 31</a>	Since staff user traffic and public access user traffic is controlled by separate policies, different protection profiles can be created for each.
The ability to block specific sites and whole categories of sites from the public access terminals and public WiFi.	<a href="#">"Protection profiles, FortiGuard Web Filtering" on page 29</a>	The FortiGuard Web Filtering service breaks down web sites in to 56 categories. Each can be allowed or blocked.
Public access traffic originates from a different address than staff and server traffic in case of abuse.	<a href="#">"IP Pools" on page 25</a>	IP pools can have traffic controlled by one policy originate from an IP address different than the physical network interface.
Mail and web server have their own IP addresses, but share the same connection to the Internet as the rest of the main branch.	<a href="#">"Mail and web servers" on page 39</a>	Virtual IP addresses allow a single physical interface to share additional IP addresses and route traffic according to destination address.
Before they're allowed access, public access users must agree that the library takes no responsibility for what they might see on the Internet.	<a href="#">"User Disclaimer" on page 26</a>	Each policy can be set to require authentication and/or agreement to a disclaimer before access is permitted.
Redundant hardware to ensure availability.	<a href="#">"High Availability (HA)" on page 22</a>	Two FortiGate-800 units operate together to ensure a minimum interruption should a hardware failure occur.

## Network addressing

The IP addresses used on the library's internal network follow a 10.x.y.z structure with a 255.255.255.0 subnet mask, where:

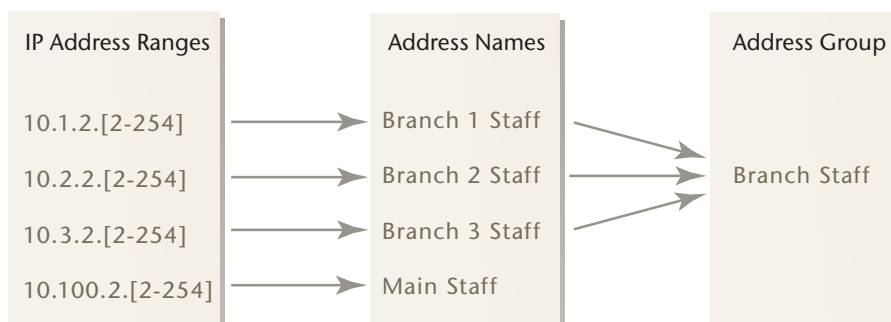
- x is the branch number. The main office uses 100 while the branches are assigned numbers starting with 1
- y indicates the purpose of the attached devices in this range:
  - 1 - servers and other infrastructure
  - 2 - staff computers
  - 3 - catalog terminals
  - 4 - public access terminals
  - 5 - public WiFi access
- z is a range of individual machines

For example, 10.3.2.15 and 10.3.2.27 are two staff members' computers in the third library branch.

Assigning IP addresses by location and purpose allows network administrators to define addresses and address ranges to descriptive names on the FortiGate unit. These address names then can also be incorporated into address groups for easy policy maintenance.

For example, the address range 10.1.2.[2-254] is assigned the name Branch\_1\_Staff on the FortiGate-800 unit. Anytime a policy is required for traffic from the staff in branch 1, this address name can be selected. Further, once an address name is specified for the staff of each branch, all of those names can be combined into an address group named Branch\_Staff so all the branch staff can be referenced as a single entity.

**Figure 3: IP address ranges are assigned names, and the names combined into address groups.**



The address names defined on the FortiGate-800 for Branch 1 traffic are Branch\_1\_Staff (10.1.2.2-10.1.2.254), Branch\_1\_Catalog (10.1.3.2-10.1.3.254), Branch\_1\_Public (10.1.4.2-10.1.4.254), and Branch\_1\_WiFi (10.1.5.2-10.1.5.254). Four address groups will be created incorporating each type of address name from all the branches: Branch\_Staff, Branch\_Catalog, Branch\_Public, and Branch\_WiFi.

At the main office, additional address names are configured for the web server (Web\_Server) and for the web and email servers combined (Servers).

Address names are configured in **Firewall > Address > Address**.

Address groups are configured in **Firewall > Address > Group**.

# Configuring the main office

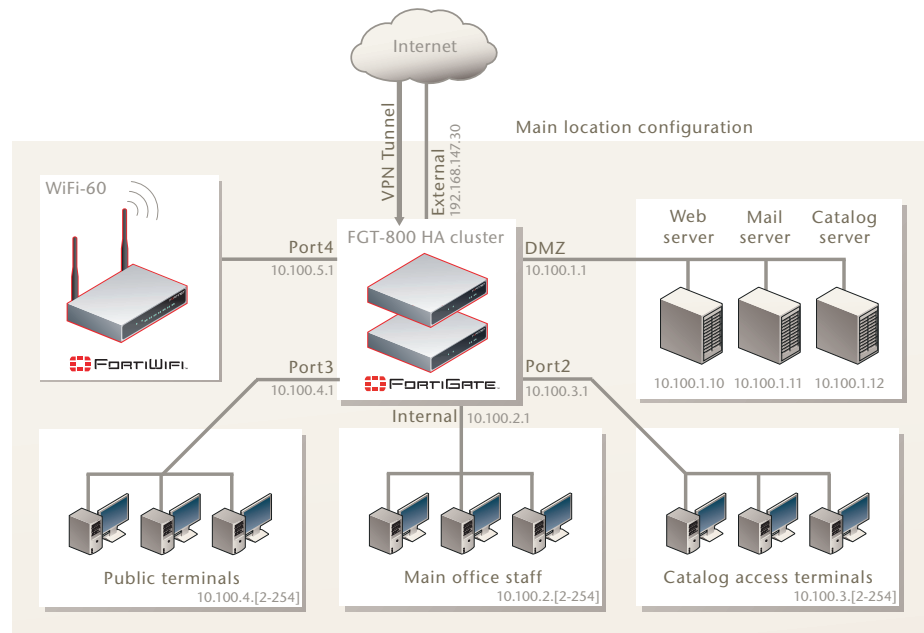
The FortiGate-800 cluster forms the hub of virtually all network communication, whether within the main office, from the branch offices to the main branch, or from anywhere in the library network to the Internet. This way, all virus scanning, spam and web filtering, as well as access restrictions can be centralized and maintained in this one place.

## Topology

The main office network layout is designed to keep the various parts of the network separate. Computers on different segments of the network cannot contact each other unless a FortiGate policy is created to allow the connection. Public terminals can access the library's web server for example, but they cannot access any machines belonging to staff members. See [Table 1 on page 18](#) for details on permitted access between different parts of the library network.

Staff computers, email and web servers, public access terminals, and WiFi connected systems are all protected by the FortiGuard service on the FortiGate-800 cluster. Push updates ensure the FortiGate unit is up to date and prepared to block viruses, worms, spyware, and attacks.

**Figure 4: Main branch network topology**



## High Availability (HA)

The two FortiGate-800 units will be connected in a high-availability (HA) cluster in active-active mode. This is a redundant configuration ensuring network traffic will be virtually uninterrupted should one unit fail. If only a single unit were present and experienced problems, the main branch would be cut-off from the Internet and the branch offices. Because the branches route their traffic through the main office, they'd also be isolated. Active-active mode has the advantage of using the processing power of the subordinate unit to increase the efficiency of antivirus scanning. The two FortiGate-800 units fulfil a mission-critical role.

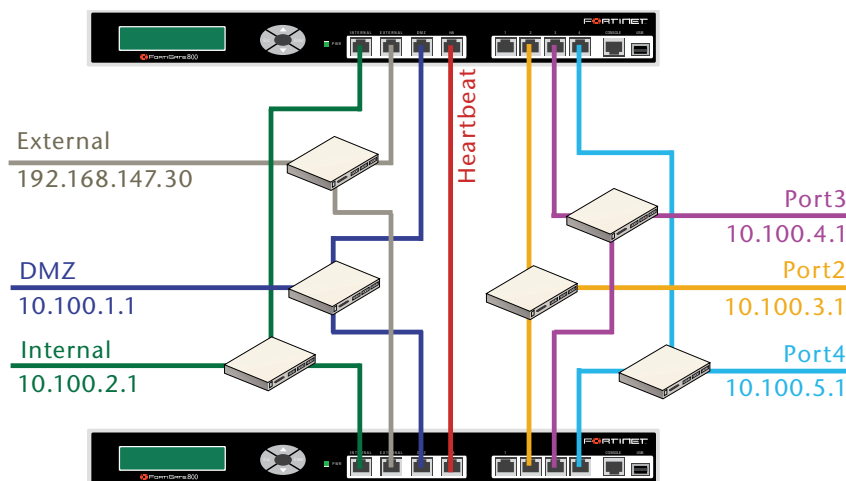
### Configuring HA

Connect the cluster units to each other and to your network. You must connect all matching interfaces in the cluster to the same hub or switch. Then you must connect these interfaces to their networks using the same hub or switch.

#### To connect the cluster units

- 1 Connect the internal interfaces of each FortiGate-800 unit to a switch or hub connected to your internal network.
- 2 Connect port2, port3, port4, external, and DMZ interfaces as described in step 1. See [Figure 5](#).
- 3 Connect the heartbeat interface of the both FortiGate-800 units using a crossover cable, or normal cables connected to a switch.

**Figure 5: HA Cluster Configuration with switches connecting redundant interfaces**



#### To configure the primary unit

- 1 Power on one of the cluster units and log in to its web based interface.
- 2 Go to **System > Config > HA** and set the mode to Active-Active.
- 3 Enter library in the Group Name field.
- 4 Enter a cluster password.
- 5 Select ha as the heartbeat interface.
- 6 Select OK.

- 7 Go to **System > Network > Interface** and set the interface IP addresses as indicated in [Figure 5 on page 22](#)

#### To configure the subordinate unit

- 1 Power on the subordinate cluster unit and log in to its web based interface.
- 2 Go to **System > Config > HA** and set the mode to Active-Active.
- 3 Change the device priority from the default 128 to 64. The FortiGate unit with the highest device priority in a cluster becomes the primary unit.
- 4 Enter library in the group name field.
- 5 Enter the cluster password.
- 6 Select ha as the heartbeat interface.
- 7 Select OK.

The two cluster units will then connect begin communication to determine which will become the primary. The primary will then transfer its own configuration data to the subordinate. In the few minutes required for this process, traffic will be interrupted. Once completed, the two clustered units will appear as a single FortiGate unit to the network.

You can now configure the cluster as if it were a single FortiGate unit.



**Note:** All the FortiGate units in a cluster must have unique host names. Default host names are the device serial numbers so unique names are automatic unless changed. If any FortiGate device host names have been changed, confirm that there is no duplication in those to be clustered.

HA is configured in **System > Config > HA**. For more information about HA, see the *FortiGate HA Overview* on the [Fortinet Technical Documentation web page](#).

## FortiGuard

Four FortiGate features take advantage of the FortiGuard Service. They are Antivirus, Intrusion Prevention, Web Filtering, and Antispam

Antivirus and intrusion prevention (IPS) signatures are updated automatically to detect new attacks and viruses with FortiGuard updates. Virus scanning and IPS are configured in protection profiles.

FortiGuard Web filtering is enabled and configured in each protection profile. When a web page is requested, the URL is sent to the FortiGuard service and the category it belongs to is returned. The FortiGate unit checks the FortiGuard Web Filtering settings and allows or blocks the web page. The FortiGuard Web Filtering is configured in protection profiles.

FortiGuard Antispam is also enabled or disabled in each protection profile. The FortiGuard service is consulted on whether each message in question is spam, and the FortiGate acts accordingly. There are a number of ways to check a message, and each method can be enabled or disabled in the protection profile. The Antispam is configured in protection profiles.

The library network is configured with the FortiGate-800 cluster performing all virus scanning, spam filtering, and FortiGuard web filtering. The settings defining how the FortiGuard Distribution Network is contacted are configured in **System > Maintenance > FortiGuard**.

## IPSEC VPN

The main office serves as a hub for the VPN connections from the branch offices. To make the generation and maintenance of the required policies simpler, interface-mode VPNs will be used. Interface-mode VPNs are configured largely the same as tunnel-mode VPNs, but the way they're use differs significantly. Interface-mode VPNs appear as network interfaces, like the DMZ, port2, and external network interfaces.

Network topology is easier to visualize because you no longer have a single interface sending and receiving both encrypted VPN traffic and unencrypted regular traffic. Instead, the physical interface handles the regular traffic, and the VPN interface handles the encrypted traffic. Further, policies no longer need to specify whether traffic is IPsec encrypted. If traffic is directed to a VPN interface, the FortiGate unit knows it is to be encrypted.

Interface-mode VPNs are used in this configuration because they will require far fewer policies. Policies for tunnel-mode VPNs require selection of a tunnel in the policy. Many tunnels can connect to a single physical interface, so the policy needs to know what traffic it is responsible for.

Since interface-mode VPNs are used as any other network interface, they can be collected into a zone and treated as a single entity. Addressing names and groups differentiate what type of user is generating the traffic, so what tunnel it comes out of isn't important in the library's configuration. All branch offices are treated the same.

For example, using tunnel-mode VPNs, 12 branches would require twelve policies to allow employees to connect directly to the email and web servers. The branch 1 policy would allow the IP range defined for staff coming from the branch 1 tunnel access to the DMZ. A second policy would allow the IP range defined for staff coming from the branch 2 tunnel access to the DMZ, and so on. Since the tunnel must be specified, there must be one policy for each tunnel, and this is just for branch staff to DMZ traffic. In the library's network configuration, there are nine traffic type/destination combinations using the VPN. This would require 108 policies for 12 branches.

To simplify things we instead give names to the address ranges based on use and location. IP address range 10.1.2.[2-255] is named Branch 1 Staff and 10.2.2.[2-255] is named Branch 2 Staff. The same procedure is followed for the remainder of the branches and all the resulting branch staff names are put into an address group called Branch Staff. All branch staff computers can be referenced with a single name. Similarly, after all the branch VPNs are created and named Branch 1, Branch 2, etc., they can be combined into a single zone named Branches.

From here, it's a simple matter to configure a single policy to handle staff traffic from all branches to the email and web servers located on the main office DMZ rather than a policy for each branch office. Should any branch require special treatment, its VPN interface can be removed from the zone and separate policies tailored to it.

## Configuring IPSEC VPNs

The VPNs secure data exchanged between each branch and the main office.

### To create the main office VPN connection to branch 1

- 1 Go to **VPN > IPSEC > Auto Key (IKE)**.
- 2 Select the Create Phase 1 button and enter Branch 1 in the Name field.
- 3 Select Static IP Address for Remote Gateway.
- 4 Enter 192.168.23.89 in the IP Address field.
- 5 Select External for the Local Interface.
- 6 Select Main (ID Protection) for the Mode.
- 7 Select Preshared Key as the Authentication Method.
- 8 Enter the preshared key in the Preshared Key field.
- 9 Select advanced and select Enable IPsec Interface Mode.



**Note:** The preshared key is a string of alphanumeric characters and should be unique for each branch. The preshared key entered at each end of the VPN connection must be identical.

### To configure the Phase 2 portion of the VPN connection to Branch 1

- 1 Go to **VPN > IPSEC > Auto Key (IKE)**.
- 2 Select the Create Phase 2 button.
- 3 Enter Main to Branch 1 in the name field.
- 4 Select Branch 1 from the Phase 1 drop down.

The advanced options can be left to their default values.

The configuration steps to create the VPN tunnel have to be repeated for each branch office to be connected in this way. Additional branches use the same Phase 1 settings except for Name, IP Address, and Preshared Key.

## IP Pools

IP Pools allow the traffic leaving an interface to use an IP address different than the one assigned to the interface itself. One use of IP pools is if the users receive a type of traffic that cannot be mapped to different ports. Without IP pools, only one user at a time could send and receive these traffic types.

In the library's case, a single IP address will be put into an IP pool named `Public_Access_Address`. All of the policies that allow traffic from the public access terminals (including the WiFi access point) will be configured to use this IP pool. The result is that any traffic from the public access terminals will appear to be coming from the IP pool address rather than the external interface's IP address. This is true even though the public access traffic will flow out of the external interface.

The purpose is to separate the public access users from the library staff from the point of view of the Internet at large. Should a library patron abuse the Internet connection by sending spam or attempting to unlawfully access to a system out on the Internet, any action taken against the source IP will not inconvenience staff. The library can continue to function normally while the problem is dealt with.

## Configuring IP pools

**To add a new IP pool for public access users.**

- 1 Go to **Firewall > Virtual IP > IP Pool** and select Create New.
- 2 Enter `Public_Access_Address` in the name field.
- 3 From the interface drop down, select external.
- 4 In the IP Range/Subnet field, enter 192.168.230.64. This address was obtained from the library's Internet service provider.
- 5 Select OK.

The IP pool named `Public_Access_Address` will now be available for selection in any policy where the destination interface is set to external, NAT is enabled, and Dynamic IP Pool is enabled.



**Note:** Although IP pools are usually created with a range of addresses, an IP pool with a single address is valid.

## User Disclaimer

When using the public terminals or wireless access, the first time a web page external to the library's network is requested, a disclaimer will pop up. This is configured in policies controlling access to the Internet. The user must agree to the stated conditions before they can continue.

### Configuring the user disclaimer

The disclaimer message is set in **System > Config > Replacement Messages > Authentication > Disclaimer page**. The default message is changed to reference the library instead of the generic 'network access provider' as shown here:

*You are about to access Internet content that is not under the control of the library. The library is therefore not responsible for any of these sites, their content, or their privacy policies. The library and its staff do not endorse or make any representations about these sites, or any information, software, or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering, copyright, trademarks, pornography, or any other material which is slanderous, defamatory or might cause offence in any other way.*

*Do you agree to the above terms?*

If the user decides not to agree to the disclaimer, a second message appears and they are not allowed to communicate with any systems out on the Internet. This second disclaimer message is set in **System > Config > Replacement Messages > Authentication > Declined disclaimer page**. The default text of this declined disclaimer is acceptable:

*Sorry, network access cannot be granted unless you agree to the disclaimer.*

The enabling this feature will be detailed in the policy configuration steps.

## Protection Profiles

Policies control whether traffic flowing through a FortiGate unit from a given source is allowed to travel to a given destination. Protection profiles are selected in each policy and define how the traffic is examined and what action may be taken based on the results of the examination. But before they can be selected in a policy, protection profiles have to be defined.

A brief overview is given for a typical protection profile, and the information required for all protection profiles, in this example, follows in table form.

For complete policy construction steps, see the *FortiGate Administration Guide*.

### To create a protection profile

- 1 Go to **Firewall > Protection Profile** and select Create New.
- 2 Enter a name and description for the profile.
- 3 Configure the following options:
  - Anti-Virus
  - Web filtering
  - FortiGuard web filtering
  - Spam filtering
  - IPS
  - Content archive
  - IM/P2P
  - VoIP
  - Logging
- 4 Select Apply.

The following tables provide all the settings of all four protection profiles used in the library network example. Each table focuses on one section of the protection profile settings:

- Protection profile name and comment, see [Table 3 on page 28](#)
- Antivirus settings, see [Table 4 on page 28](#)
- Web-Filtering, see [Table 5 on page 29](#)
- FortiGuard Web Filtering, see [Table 6 on page 29](#)
- Spam Filtering, see [Table 7 on page 30](#)
- IPS, see [Table 8 on page 30](#)
- Content Archive, see [Table 9 on page 30](#)
- IM/P2P, see [Table 10 on page 31](#)

- VoIP, see [Table 11 on page 31](#)
- Logging, see [Table 12 on page 31](#)



**Note:** The settings in the tables listed below are for the library example only. For complete protection profile information see the *FortiGate Administration Guide*.

In this example, if a setting is to be left in the default setting, it is not expanded in the tables below.

**Table 3: Protection profiles, Name and Comments**

Profile Name	Staff	Public	Servers	Web_Internal
<b>Comment (optional)</b>	Use with all policies for traffic from staff computers.	Use with all policies for traffic from the public access or WiFi.	Use for policies allowing the public access to the library web server from the Internet, or email server communication.	Use for policies allowing access to the library web server from catalog terminals.

The comment field is optional, but recommended. With many profiles, the comment can be invaluable in quickly identifying profiles.

**Table 4: Protection profiles, Antivirus settings**

Profile Name	Staff	Public	Servers	Web_Internal
<b>Virus Scan</b>	Enable for HTTP, FTP, IMAP, POP3, SMTP, IM and NNTP	Enable for HTTP, FTP, IMAP, POP3, SMTP, IM and NNTP	Enable for HTTP, FTP, IMAP, POP3, SMTP, IM and NNTP	Disable
<b>File Filter</b>	Disable	Disable	Disable	Disable
<b>Quarantine</b>	Enable for HTTP, FTP, IMAP, POP3, SMTP, IM and NNTP	Enable for HTTP, FTP, IMAP, POP3, SMTP, IM and NNTP	Enable for HTTP, FTP, IMAP, POP3, SMTP, IM and NNTP	Disable
<b>Pass Fragmented Emails</b>	Enable for IMAP, POP3, and SMTP	Enable for IMAP, POP3, and SMTP	Enable for IMAP, POP3, and SMTP	Disable
<b>Comfort Clients</b>	Enable for HTTP and FTP	Enable for HTTP and FTP	Disable	Disable
<b>Interval</b>	10	10	10	10
<b>Amount</b>	1	1	1	1
<b>Oversized File/Email</b>	Pass	Pass	Pass	Pass
<b>Threshold</b>	Default	Default	Default	Default
<b>Add signature to outgoing emails</b>	Disable	Disable	Disable	Disable



**Note:** The FortiGate unit must have either an internal hard drive or a configured FortiAnalyzer unit for the Quarantine option to appear.

**Table 5: Protection profiles, Web-Filtering**

Profile Name	Staff	Public	Servers	Web_Internal
<b>Web Content Block</b>	Disable	Disable	Disable	Disable
<b>Web Content Exempt</b>	Disable	Disable	Disable	Disable
<b>Web URL Filter</b>	Disable	Disable	Disable	Disable
<b>ActiveX Filter</b>	Disable	Disable	Disable	Disable
<b>Cookie Filter</b>	Disable	Disable	Disable	Disable
<b>Java Applet Filter</b>	Disable	Disable	Disable	Disable
<b>Web Resume Download Block</b>	Disable	Disable	Disable	Disable
<b>Block Invalid URLs</b>	Disable	Disable	Disable	Disable

Web filtering is disabled but can be enabled should a threat or abuse be discovered at a later time.

**Table 6: Protection profiles, FortiGuard Web Filtering**

Profile Name	Staff	Public	Servers	Web_Internal
<b>Enable FortiGuard Web Filtering</b>	Disable	Enable*	Disable	Disable
<b>Enable FortiGuard Web Filtering Overrides</b>	Disable	Disable	Disable	Disable
<b>Provide details for blocked HTTP 4xx and 5xx errors</b>	Disable	Enable	Disable	Disable
<b>Rate images by URL (blocked images will be replaced with blanks)</b>	Disable	Enable	Disable	Disable
<b>Allow websites when a rating error occurs</b>	Disable	Disable	Disable	Disable
<b>Strict Blocking</b>	Enable	Enable	Enable	Enable
<b>Rate URLs by domain and IP address</b>	Disable	Enable	Disable	Disable

\*The Public protection profile has FortiGuard web filtering enabled and set to block advertising, malware, and spyware categories. Additional categories can be blocked if required by library policy.

Table 7: Protection profiles, Spam Filtering

Profile Name	Staff	Public	Servers	Web_Internal
IP address check	Enable for IMAP, POP3 and SMTP	Disable	Enable for IMAP, POP3 and SMTP	Disable
URL check	Enable for IMAP, POP3 and SMTP	Disable	Enable for IMAP, POP3 and SMTP	Disable
E-mail checksum check	Enable for IMAP, POP3 and SMTP	Disable	Enable for IMAP, POP3 and SMTP	Disable
Spam submission	Enable for IMAP, POP3 and SMTP	Disable	Enable for IMAP, POP3 and SMTP	Disable
IP address BWL check	Disable	Disable	Disable	Disable
HELO DNS lookup	Disable	Disable	Disable	Disable
E-mail address BWL check	Enable for IMAP, POP3 and SMTP	Disable	Enable for IMAP, POP3 and SMTP	Disable
Return e-mail DNS check	Enable for IMAP, POP3 and SMTP	Disable	Enable for IMAP, POP3 and SMTP	Disable
Banned word check	Disable	Disable	Disable	Disable
Spam Action	Tagged	Disable	Tagged	Disable
Tag Location	Subject	Subject	Subject	Subject
Tag Format	[spam]		[spam]	

Email is not scanned for spam using the Public protection profile. Users of the public access terminals will use their own webmail accounts if checking mail, and WiFi connected users will have their own spam solutions, if desired.

Table 8: Protection profiles, IPS

Profile Name	Staff	Public	Servers	Web_Internal
	Select all_default	Select all_default	Select all_default	Disable

You can create your own IPS sensors by going to **Intrusion Protection > Signature > IPS Sensor**. The IPS option does not select denial of service (DoS) sensors. For more information, see the *FortiGate Administration Guide*.

Table 9: Protection profiles, Content Archive

Profile Name	Staff	Public	Servers	Web_Internal
All settings	Default values	Default values	Default values	Default values

The default content archive settings are ideal for the current library configuration. Should detailed logging be required, a FortiAnalyzer can be added to the network and these settings adjusted.

**Table 10: Protection profiles, IM/P2P**

Profile Name	Staff	Public	Servers	Web_Internal
<b>Block Login</b>	Disable for all IM protocols	Enable for all IM protocols	Disable	Disable
<b>Block File Transfers</b>	Disable for all IM protocols	Disable	Disable	Disable
<b>Block Audio</b>	Disable for all IM protocols	Disable	Disable	Disable
<b>Inspect Non-standard Port</b>	Enable for all IM protocols	Enable for all IM protocols	Disable	Disable
<b>Action</b>	Block for all P2P protocols	Block for all P2P protocols	Block for all P2P protocols	Block for all P2P protocols
<b>Limit (KBytes/s)</b>	n/a	n/a	n/a	n/a

Staff employees are permitted to use instant messaging while public access users are not. All users have peer to peer clients blocked.

**Table 11: Protection profiles, VoIP**

Profile Name	Staff	Public	Servers	Web_Internal
<b>All settings</b>	Default values	Default values	Default values	Default values

The library system does not currently use VoIP phones.

**Table 12: Protection profiles, Logging**

Profile Name	Staff	Public	Servers	Web_Internal
<b>All settings</b>	Enable all options except Oversized Files / E-mails and VoIP	Enable all options except Oversized Files / E-mails and VoIP	Enable all options except Oversized Files / E-mails and VoIP	Enable all options except Oversized Files / E-mails and VoIP

The logging of oversized files and email messages is disabled because oversized messages and email messages are not blocked. If blocking files and messages is ever considered, logging can be enabled to get an accurate idea of what the effects will be.

## Staff access

Staff members can access the Internet as well as directly connect to the library web and email servers.

Since the network uses private addresses and has no internal DNS server, connections to the web and email servers must be specified by IP address. The private network address will keep all communication between the server and email client on the local network and secure against interception on the Internet.

If a staff member attempts to open the library web page or connect to the email server using either server's virtual IP or fully qualified domain name, their request goes out over the Internet, and returns through the FortiGate unit. This method will make their transmission vulnerable to interception.

The web browsers on staff computers will be configured with the library web page as the default start page. Staff members' email software should be configured to use the email server's private network IP address rather than the virtual IP or fully qualified domain name. These two steps will prevent staff from having to remember the servers' IP addresses.

## Creating firewall policy for staff members

The first firewall policy for main office staff members allows full access to the Internet at all times. A second policy will allow direct access to the DMZ for staff members. A second pair of policies are required to allow branch staff members the same access.

The staff firewall policies will all use a protection profile configured specifically for staff access. Enabled features include virus scanning, spam filtering, IPS, and blocking of all P2P traffic. FortiGuard web filtering is also used to block advertising, malware, and spyware sites.

A few users may need special web and catalog server access to update information on those servers, depending on how they're configured. Special access can be allowed based on IP address or user.

A brief overview procedure is given for a typical policy, and the information required for all staff policies follows in table form. For more detailed information see the *FortiGate Administration Guide*.

### Step-by-step policy creation example

- 1 To create a policy to allow main office staff to connect to the Internet, go to **Firewall > Policy** and select Create New.
- 2 Fill in the following fields:
  - Source interface/Zone
  - Source address
  - Destination interface/Zone
  - Schedule
  - Service
  - Action
  - NAT
  - Protection Profile
  - Log allowed traffic
  - Traffic shaping
  - User authentication disclaimer
  - Comments (optional)
- 3 Select OK.

The settings required for all staff policies are provided in [Table 13](#).

**Table 13: Library staff policies**

	Main office staff connect to the Internet	Main office staff connect to library servers	Branch office staff connect to the Internet	Branch office staff connect to library servers
<b>Source Interface/Zone</b>	Internal	Internal	Branches	Branches
<b>Source Address</b>	All	All	Branch_Staff	Branch_Staff
<b>Destination Interface/Zone</b>	External	DMZ	External	DMZ
<b>Destination Address</b>	All	Servers	All	Servers
<b>Schedule</b>	Always	Always	Always	Always
<b>Service</b>	All	All	All	All
<b>Action</b>	Accept	Accept	Accept	Accept
<b>NAT</b>	Enable	Enable	Enable	Enable
<b>Protection Profile</b>	Enable and select Staff	Enable and select Staff	Enable and select Staff	Enable and select Staff
<b>Log Allowed Traffic</b>	Enable	Enable	Enable	Enable
<b>Authentication</b>	Disable	Disable	Disable	Disable
<b>Traffic Shaping</b>	Disable	Disable	Disable	Disable
<b>User Authentication Disclaimer</b>	Disable	Disable	Disable	Disable
<b>Comment (optional)</b>	Main office: staff computers connecting to the Internet.	Main office: staff computers connecting to the library servers.	Branch offices: staff computers connecting to the Internet.	Branch offices: staff computers connecting to the library servers.

## Catalog terminals

Dedicated computers are provided for the public to search the library catalog. The only application available on the catalog terminals is a web browser, and the only site the catalog terminal web browser can access is the library web page, which includes access to the catalog. The browser is configured to use the library web server's private network address as the start page.

### Creating firewall policies for catalog terminals

The policy used for the catalog access terminals only allows communication with the DMZ. Create two new policies, one for main office access and another to allow access from the branch offices.

The settings required for all catalog terminal policies in this example are provided in [Table 14 on page 34](#).

For complete policy construction steps, see the *FortiGate Administration Guide*.

**Table 14: Catalog terminal policies**

	Main office catalog terminals connect to web server	Branch office catalog terminals connect to web server
<b>Source Interface/Zone</b>	port2	Branches
<b>Source Address</b>	All	Branch_Catalog
<b>Destination Interface/Zone</b>	DMZ	DMZ
<b>Destination Address</b>	Web_Server	Web_Server
<b>Schedule</b>	Always	Always
<b>Service</b>	HTTP	HTTP
<b>Action</b>	Accept	Accept
<b>NAT</b>	Enable	Enable
<b>Protection Profile</b>	Disable	Disable
<b>Log Allowed Traffic</b>	Enable	Enable
<b>Authentication</b>	Disable	Disable
<b>Traffic Shaping</b>	Disable	Disable
<b>User Authentication Disclaimer</b>	Disable	Disable
<b>Comments (optional)</b>	Main office: catalog terminals connecting to the web server.	Branch offices: catalog terminals connecting to the web server.

## Public access terminals

Terminals are provided for library patrons to access the Internet. Protection profile settings block all instant messaging and peer to peer connections. In addition, library staff can block individual sites and entire site categories as deemed necessary. Site categories are blocked using FortiGuard web filtering configured in the protection profile.

### Creating firewall policies for public access terminals

Library users can access the Internet from the public terminals. The public terminal machines have the library's web page as the web browser's default start page. The address is the web server's private network IP so the traffic between the terminal and the web server remains on the library's network.

The settings required for all public access terminal policies in this example are provided in [Table 15 on page 35](#).

For complete policy construction steps, see the *FortiGate Administration Guide*.

Table 15: Public access terminal policies

	Main office Public access users connect to Internet	Main office public access users connect to web server	Branch offices public access users connect to Internet	Branch offices public access users connect to web server
<b>Source Interface/Zone</b>	Port3	Port3	Branches	Branches
<b>Source Address</b>	Main_Public	Main_Public	Branch_Public	Branch_Public
<b>Destination Interface/Zone</b>	External	DMZ	External	DMZ
<b>Destination Address</b>	All	Web_Server	All	Web_Server
<b>Schedule</b>	Always	Always	Always	Always
<b>Service</b>	All	HTTP	All	HTTP
<b>Action</b>	Accept	Accept	Accept	Accept
<b>NAT</b>	Enable NAT, enable Dynamic IP Pool and select Public_Access_ Address	Enable NAT.	Enable NAT, enable Dynamic IP Pool and select Public_Access_ Address	Enable NAT.
<b>Protection Profile</b>	Enable and select Public	Enable and select Web_Internal	Enable and select Public	Enable and select Web_Internal
<b>Log Allowed Traffic</b>	Enable	Enable	Enable	Enable
<b>Authentication</b>	Disable	Disable	Disable	Disable
<b>Traffic Shaping</b>	Disable	Disable	Disable	Disable
<b>User Authentication Disclaimer</b>	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Disable	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Disable
<b>Comments (optional)</b>	Main office: public access terminals connecting to the Internet.	Main office: public access terminals connecting to the library web server.	Branch offices: public access terminals connecting to the Internet.	Branch offices: public access terminals connecting to the library web server.

## Wireless access

Wireless access allow library visitors to browse the Internet from their own WiFi-enabled laptops. The same protection profile is applied to WiFi access as is used with the Public terminals so IM and P2P are blocked, and all the same FortiGuard web blocking is applied.

## Security considerations

The wireless interface of the FortiWiFi-60A will have its DHCP server assign IP addresses to users wanting to connect to the Internet. The FortiWiFi-60A will also have its SSID broadcast and set to 'library' or something similarly identifiable. Stricter security would be of limited value because anyone could request and receive access. Also, library staff would spend significant time serving as technical support to patrons not entirely familiar with their own equipment. Instead, the firewall policy applied to wireless access will limit Internet connectivity to the main office's business hours. This decision will be reviewed periodically, especially if public access is abused.

Wireless security is configured in **System > Wireless > Settings**.

The number of concurrent wireless users can be adjusted by reducing or expanding the range of addresses the DHCP server on the WiFi port has available to assign. Using this means of limiting users is only partially effective because some users may set a static address in the same subnet and gain access. To prevent this, configure the IP range specified in the address name used in the policy to have the same range the DHCP server assigns. Users can still set a static IP, but the policy will not allow any access.

The wireless DHCP server is configured in **System > Network > Interface**. Select the edit icon for the wlan interface.

## Creating schedules for wireless access

Library users can access the Internet from the WiFi connection. The policies used for WiFi incorporates a schedule to limit Internet access to only when the library is open to the public.

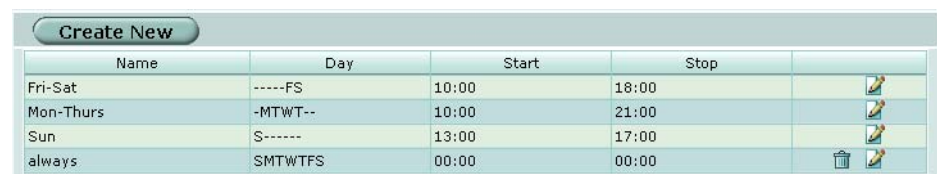
The protection profile used for library users enables virus scanning, IPS, and blocking of all P2P traffic and IM logins. Spam filtering is *not* enabled. FortiGuard web filtering is used to block malware, and spyware sites. Additional categories can be blocked if required by library policy.

The library hours are:

<b>Mon-Thurs</b>	10am - 9pm
<b>Fri-Sat</b>	10am - 6pm
<b>Sun</b>	1pm - 5pm

Because of the varying library hours through the week, three separate schedules are required, as shown in [Figure 6](#).

**Figure 6: Policy schedules**



Name	Day	Start	Stop	
Fri-Sat	----FS	10:00	18:00	
Mon-Thurs	-MTWT--	10:00	21:00	
Sun	S-----	13:00	17:00	
always	SMTWTFS	00:00	00:00	

### To create Monday to Thursday business hours schedule

- 1 Go to **Firewall > Schedule > Recurring** and select Create New.
- 2 Enter Mon-Thurs for the schedule name.

- 3 Select the check boxes for Monday, Tuesday, Wednesday, and Thursday.
- 4 Select 10 for the start hour and 00 for the start minute.
- 5 Select 21 for the end hour and 00 for the end minute.
- 6 Select OK.

#### To create Friday and Saturday business hours schedule

- 1 Go to **Firewall > Schedule > Recurring** and select Create New.
- 2 Enter Fri-Sat for the schedule name.
- 3 Select the check boxes for Friday, and Saturday.
- 4 Select 10 for the start hour and 00 for the start minute.
- 5 Select 18 for the end hour and 00 for the end minute.
- 6 Select OK.

#### To create Sunday business hours schedule

- 1 Go to **Firewall > Schedule > Recurring** and select Create New.
- 2 Enter Sun for the schedule name.
- 3 Select the check box for Sunday.
- 4 Select 13 for the start hour and 00 for the start minute.
- 5 Select 17 for the end hour and 00 for the end minute.
- 6 Select OK.

For holidays, special one-time schedules can be created. These schedules allow specifying the year, month, and day in addition to the hour and minute. Duplicate policies can be created with one-time schedules to cover holidays. Policies are parsed from top to bottom so position these special holiday policies above the regular recurring-schedule policies, otherwise the holiday policies will never come into effect.

One-time schedules are configured in **Firewall > Schedule > One-time**.

## Creating firewall policies for WiFi access

Four main office WiFi access policies are required. Three incorporate the schedules to cover the entire week and only allow access while the library is open to the public. The fourth policy allows access to the library web server.

The settings required for all main office WiFi terminal policies in this example are provided in [Table 16 on page 38](#).

For complete policy construction steps, see the *FortiGate Administration Guide*.

Table 16: Main office WiFi terminal policies

	Main office WiFi users connect to Internet (Mon-Thurs)	Main office WiFi users connect to Internet (Fri-Sat)	Main office WiFi users connect to Internet (Sunday)	Main office WiFi users connect to web library server
<b>Source Interface/Zone</b>	Port4	Port4	Port4	Port4
<b>Source Address</b>	Main_WiFi	Main_WiFi	Main_WiFi	Main_WiFi
<b>Destination Interface/Zone</b>	External	External	External	DMZ
<b>Destination Address</b>	All	All	All	Web_Server
<b>Schedule</b>	Mon-Thurs	Fri-Sat	Sun	Always
<b>Service</b>	All	All	All	HTTP
<b>Action</b>	Accept	Accept	Accept	Accept
<b>NAT</b>	Enable NAT, enable Dynamic IP Pool and select Public_Access_Address	Enable NAT, enable Dynamic IP Pool and select Public_Access_Address	Enable NAT, enable Dynamic IP Pool and select Public_Access_Address	Enable NAT.
<b>Protection Profile</b>	Enable and select Public	Enable and select Public	Enable and select Public	Enable and select Web_Internal
<b>Log Allowed Traffic</b>	Enable	Enable	Enable	Enable
<b>Authentication</b>	Disable	Disable	Disable	Disable
<b>Traffic Shaping</b>	Disable	Disable	Disable	Disable
<b>User Authentication Disclaimer</b>	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Disable
<b>Comments (optional)</b>	Main office: WiFi connecting to the Internet (Mon-Thurs).	Main office: WiFi connecting to the Internet (Fri-Sat).	Main office: WiFi connecting to the Internet (Sunday).	Main office: WiFi connecting to the library web server.

Four branch office WiFi access policies are required. Three incorporate the schedules to cover the entire week and only allow access while the library is open to the public. The fourth policy allows access to the library web server.

The settings required for all branch office WiFi terminal policies in this example are provided in [Table 17 on page 39](#).

Table 17: Branch office WiFi terminal policies

	Branch office WiFi users connect to Internet (Mon-Thurs)	Branch office WiFi users connect to Internet (Fri-Sat)	Branch office WiFi users connect to Internet (Sunday)	Branch office WiFi users connect to web library server
<b>Source Interface/Zone</b>	Branches	Branches	Branches	Branches
<b>Source Address</b>	Branch_WiFi	Branch_WiFi	Branch_WiFi	Branch_WiFi
<b>Destination Interface/Zone</b>	External	External	External	DMZ
<b>Destination Address</b>	All	All	All	Web_Server
<b>Schedule</b>	Mon-Thurs	Fri-Sat	Sun	Always
<b>Service</b>	All	All	All	HTTP
<b>Action</b>	Accept	Accept	Accept	Accept
<b>NAT</b>	Enable NAT, enable Dynamic IP Pool and select Public_Access_Address	Enable NAT, enable Dynamic IP Pool and select Public_Access_Address	Enable NAT, enable Dynamic IP Pool and select Public_Access_Address	Enable NAT.
<b>Protection Profile</b>	Enable and select Public	Enable and select Public	Enable and select Public	Enable and select Web_Internal
<b>Log Allowed Traffic</b>	Enable	Enable	Enable	Enable
<b>Authentication</b>	Disable	Disable	Disable	Disable
<b>Traffic Shaping</b>	Disable	Disable	Disable	Disable
<b>User Authentication Disclaimer</b>	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Enable User Authentication Disclaimer and leave Redirect URL field blank.	Disable
<b>Comments (optional)</b>	Branch offices: WiFi connecting to the Internet (Fri-Sat).	Branch offices: WiFi connecting to the Internet (Fri-Sat).	Branch offices: WiFi connecting to the Internet (Sun).	Branch offices: WiFi connecting to the library web server.

## Mail and web servers

Since the branch offices do not have their own email servers, all library staff email is sent or received using the main office email server. Users in branch offices connect though their VPN to the main office. Maintenance of a single server is more convenient and cost effective than each branch office having their own email server.

Staff email software will be set up with the email server's private network IP address. Specifying the virtual IP address or domain name would cause the email traffic to loop out to the Internet and return, allowing the information to be intercepted. Similarly, staff computers will be pre-configured with the library web server's internal network IP address as the start page address.

## Creating a virtual IP for the web server

The library has arranged for another external IP address which will be used for the library's Internet web presence. A virtual IP configured on the FortiGate will take any traffic directed to 172.20.16.192 on the Internet and remap it to the web server at 10.100.1.10 on the library's network. The 172.20.16.192 address can be registered with the library's domain name so anyone on the Internet entering the URL will bring up the library's page.

**Figure 7: Web server virtual IP configuration**

Add New Virtual IP Mapping	
Name	Web Server VIP
External Interface	external
Type	<input checked="" type="radio"/> Static NAT <input type="radio"/> Load Balance
External IP Address/Range	172.20.16.192
Mapped IP Address/Range	10.100.1.10
Port Forwarding	<input type="checkbox"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### To create a virtual IP for the web server

- 1 Go to **Firewall > Virtual IP** and select Create New.
- 2 Enter Web\_Server\_VIP for the virtual IP map name.
- 3 Select External from the External Interface drop down.
- 4 Select Static NAT as the Type
- 5 Enter 172.20.16.192 as the External IP Address.
- 6 Enter 10.100.1.10 as the Mapped IP Address.
- 7 Disable Port Forwarding.
- 8 Select OK.

## Creating a virtual IP for the email server

Similar to the web server, the library has another external IP address reserved for the email server. A virtual IP configured on the FortiGate will take any traffic directed to 172.20.16.120 and remap it to the web server at 10.100.1.11 transparently.

### To create a virtual IP for the email server

- 1 Go to **Firewall > Virtual IP** and select Create New.
- 2 Enter Email\_Server\_VIP for the virtual IP map name.
- 3 Select External from the External Interface drop down.
- 4 Select Static NAT as the Type

- 5 Enter 172.20.16.120 as the External IP Address.
- 6 Enter 10.100.1.11 as the Mapped IP Address.
- 7 Disable Port Forwarding.
- 8 Select OK.

## Creating a server service group

Access to and from the web and email servers can be combined into a single policy. The only difficulty is email servers exchange mail using the SMTP protocol on port 20 and contact is made with a web server using HTTP on port 80. If the policy is to restrict traffic to only the required ports, a service group is required as shown in [Figure 8](#).

**Figure 8: A service group incorporating the three server protocols**



### To create a server service group

- 1 Go to **Firewall > Service > Group** and select Create New.
- 2 Enter Servers in the Group Name field.
- 3 From the Available Services list, select HTTP
- 4 Select the right-pointing arrow icon to move HTTP to the Members list.
- 5 From the Available Services list, select SMTP
- 6 Select the right-pointing arrow icon to move SMTP to the Members list.
- 7 Select OK. The new service group will appear in the service group list.

## Creating firewall policies to protect email and web servers

An External to DMZ policy is required for access to the web and email servers. Only ports 80 (HTTP) and 25 (SMTP) need to be open.

A DMZ to External policy opening port 25 is required for the library email server to deliver messages sent to addresses outside the library system.

The settings required for all server policies in this example are provided in [Table 18 on page 41](#).

For complete policy construction steps, see the *FortiGate Administration Guide*.

**Table 18: Server policies**

	Inbound to web and email servers	Outbound from email server
<b>Source Interface/Zone</b>	External	DMZ
<b>Source Address</b>	All	Servers
<b>Destination Interface/Zone</b>	DMZ	External
<b>Destination Address</b>	Servers	All
<b>Schedule</b>	Always	Always
<b>Service</b>	Servers	SMTP

Table 18: Server policies (Continued)

	Inbound to web and email servers	Outbound from email server
<b>Action</b>	Accept	Accept
<b>NAT</b>	Enable	Enable
<b>Protection Profile</b>	Enable and select Servers	Enable and select Servers
<b>Log Allowed Traffic</b>	Enable	Enable
<b>Authentication</b>	Disable	Disable
<b>Traffic Shaping</b>	Disable	Disable
<b>User Authentication Disclaimer</b>	Disable	Disable
<b>Comments (optional)</b>	Incoming web connections and incoming email delivery from other mail servers.	Outbound email server connections.

## The FortiWiFi-60A

In the main office network, the FortiWiFi-60A is used to provide WiFi access to main library patrons with their own WiFi-capable laptops, and as a connection point to all the main office public access terminals. Since all the policies and protection profiles are configured on the FortiGate-800 cluster, the FortiWiFi-60A only has to pass the traffic along. For this reason, the FortiWiFi-60A configuration is not complex.

### Configuring the main office FortiWiFi-60.

The FortiWiFi-60A is connected as shown in the main branch network topology diagram, [Figure 4 on page 21](#).

#### To Configure the operation mode.

- 1 Go to **System > Config > Operation** and set the unit to Transparent Mode. Since the FortiWiFi-60 is within the library's network, no address translation is required.
- 2 Enter 10.100.1.99/255.255.255.0 as the Management IP/Netmask and 10.100.1.3 as the Default Gateway.
- 3 Select Apply. You will be disconnected and will have to log in to the FortiWiFi-60A using the management IP address.

Since the FortiWiFi-60A will not be examining the traffic for content, only a single simple policy is required.

The settings required for all main office WiFi-60A policies in this example are provided in [Table 19 on page 43](#).

For complete policy construction steps, see the *FortiGate Administration Guide*.

**Table 19: Main office FortiWiFi-60A policies**

	WiFi
<b>Source Interface/Zone</b>	Wlan
<b>Source Address</b>	All
<b>Destination Interface/Zone</b>	Wan1
<b>Destination Address</b>	All
<b>Schedule</b>	Always
<b>Service</b>	All
<b>Action</b>	Accept
<b>Protection Profile</b>	Disable
<b>Log Allowed Traffic</b>	Disable
<b>Authentication</b>	Disable
<b>Traffic Shaping</b>	Disable
<b>User Authentication Disclaimer</b>	Disable
<b>Comments (optional)</b>	WiFi users connected to the main office FortiWiFi-60A

Although the WiFi policy allows access at all times, the policies on the FortiGate-800 cluster restrict Internet access to library business hours.

# Configuring branch offices

The three sections of each branch's network (staff computers, catalog terminals, and public access terminals) are wired separately to different interfaces on the FortiWiFi-60A and cannot access each other.

All external communication is sent to the main office through the VPN by the FortiWiFi-60A. After reaching the FortiGate-800, the traffic continues out to the Internet. Inbound traffic follows the same course back.

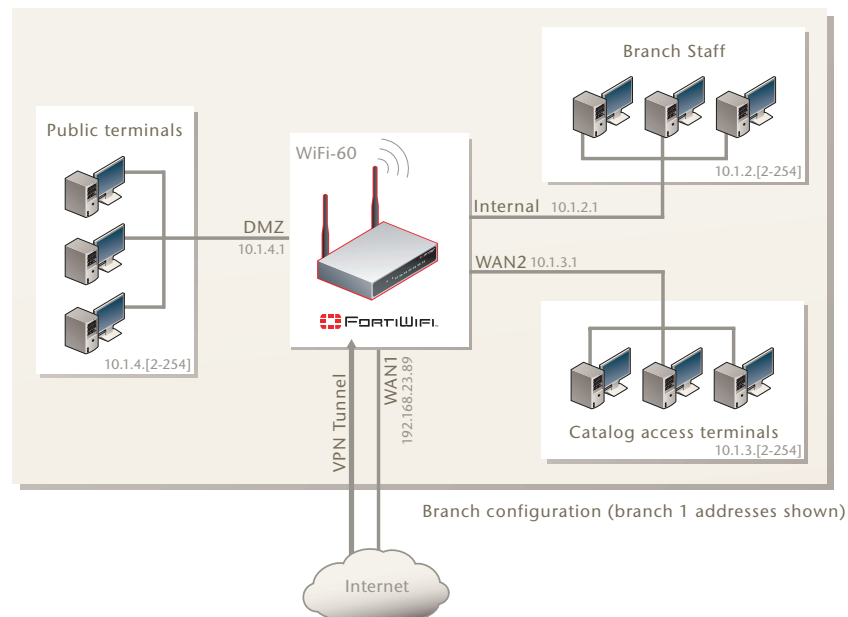
Unless they use the email and web server private IP addresses, the computers accessing the library web page and email server have their connections sent out to the Internet, then back to the servers.

## Topology

The branch network layout is designed to keep the various parts of the network separate. The staff computers and public terminals are connected to different network interfaces on the FortiGate, and those interfaces are configured to not allow direct connections between them. See [Table 1 on page 18](#) for details on permitted access between different network areas.

Staff computers, email and web servers, public access terminals, WiFi connected systems are all protected by the FortiGuard service subscription on the FortiGate-800 cluster at the main branch.

**Figure 9: Branch office network topology**



## Staff access

All staff traffic is routed through the VPN to the main branch. Requests for the email or web servers are routed to the main office DMZ while general Internet traffic is sent to the main office then out of the library network to the Internet.

## Catalog terminals

Dedicated computers are provided for library patrons to search for books and periodicals in the library's catalog. The catalog computers are configured so the only application available is a web browser, and the only site it can access is the library web page which includes access to the catalog. Requests are routed through the VPN to the web server in the library's main office.

## Wireless/public access

Public access terminals and wireless access allow library patrons to access the Internet. Profile settings deny all instant messaging and peer to peer connections. Also, main branch library staff can block individual sites and entire site categories as deemed necessary using FortiGuard web filtering.

## Mail and web servers

Branch offices do not have their own email servers. When staff members send or receive email, their email software connects to the email server in the main library location. This connection is made through the VPN between the main and branch office. Email server access is not available from the Internet at large.

## IPSEC VPN

Each branch will have a VPN connection to the main office.

### To create the Phase 1 portion of the VPN to the main office

- 1 Go to **VPN > IPSEC > Auto Key (IKE)** and Select the Create Phase 1 button.
- 2 In the Name field, enter Main\_Office.
- 3 Select Static IP for Remote Gateway.
- 4 Enter 192.168.147.30 in the IP Address field.
- 5 Select WAN1 for the Local Interface.
- 6 Select Main (ID Protection) for the Mode.
- 7 Select Preshared Key as the Authentication Method and Enter the key in the Preshared Key field.
- 8 Select advanced and select Enable IPsec Interface Mode.
- 9 Select OK.



**Note:** The preshared key is a string of alphanumeric characters and should be unique for each branch. The preshared key entered at each end of the VPN connection must be identical.

#### To create the Phase 2 portion of the VPN to the main office

- 1 Select the Create Phase 2 button.
- 2 Enter Branch 1 to Main office in the name field.
- 3 Select Main\_Office from the Phase 1 drop down.
- 4 Select OK.

The configuration steps to create the VPN tunnel have to be repeated for each branch office to be connected in this way. Additional branches use the same Phase 1 settings except for Name, IP Address, and Preshared Key.

## Branch Firewall Policy

All traffic leaving the branch, whether destined for the main office or the Internet, is controlled by a single policy. Additional policies and routing configured on the FortiGate-800 cluster at the main office direct the traffic once it arrives there.

### Creating firewall policy for the branch office

The firewall policy for all traffic leaving the branch is sent through the VPN to the main office. For simplicity, the four network interfaces we use for the internal network (internal, DMZ, WLAN, and WAN2) are collected into a zone called Inside\_Zone. This allows a single policy to control all the traffic leaving the branch.

Policies are configured in **Firewall > Policy**. Interface zones are defined in **System > Network > Zone**.

The settings required for all main office WiFi-60A policies in this example are provided in [Table 20 on page 46](#).

For complete policy construction steps, see the *FortiGate Administration Guide*.

**Table 20: Branch office FortiWiFi-60A policies**

	Branch policy
Source Interface/Zone	Inside_Zone
Source Address	All
Destination Interface/Zone	Main_Office
Destination Address	All
Schedule	Always
Service	All
Action	Accept
Protection Profile	Disable
Log Allowed Traffic	Disable
Authentication	Disable

**Table 20: Branch office FortiWiFi-60A policies (Continued)**

	<b>Branch policy</b>
<b>Traffic Shaping</b>	Disable
<b>User Authentication Disclaimer</b>	Disable
<b>Comments (optional)</b>	Policy to allow branch traffic to main office.

# Traffic shaping

Traffic shaping regulates and prioritizes traffic flow. Guaranteed bandwidth allows a minimum bandwidth to be reserved for traffic controlled by a policy. Similarly, maximum bandwidth caps the rate of traffic controlled by the policy. Finally, the traffic controlled by a policy can be assigned a high, medium or low priority. If there is not enough bandwidth to transmit all traffic, high priority traffic is processed before medium priority traffic, and medium before low priority traffic.

Traffic shaping limits are applied only to traffic controlled by the policy they're applied to. If you do not apply any traffic shaping rules to a policy, the policy is set to high priority by default. Because of this, traffic shaping is of extremely limited use if applied to some policies and not others. Enable traffic shaping on all firewall policies.

Because guaranteed bandwidth and maximum bandwidth settings are entirely dependant on the maximum bandwidth available, the current traffic, and the relative priority of each type of traffic, defining exact values for each policy is beyond the scope of this document and traffic shaping is therefore disabled in the example policies.

## Priorities

Traffic can be assigned high, medium, or low priority depending on importance. Ideally, traffic will be spread across all three priorities. If all traffic is assigned the same setting, prioritizing traffic is effectively disabled.

On the library system's network, there are four types of users accessing two services.

**Table 21: Priority of traffic based on source and destination**

	To servers	To Internet
From catalog terminals*	high	
From Internet†	high	
From public terminals/WiFi*	high	low
From staff*	high	medium

\* includes both branch and main office traffic

† includes both inbound and outbound mail server connections

On the library system's network, the most important traffic is to and from the web and mail servers. Locating research materials in the library's collection is extremely difficult without a working catalog. Email is important to staff members as they maintain important communication using it.

Staff access to the Internet is of medium priority. Although staff members do need Internet access, it's rarely as time-critical as catalog access and email.

Public access to the Internet (both from provided terminals and WiFi connections) are of the lowest priority.

Although most traffic appears to be of high importance, the most bandwidth is consumed by Internet access, partly by staff but mostly by the public terminals/WiFi.

With this in mind, a maximum bandwidth value can also be set to limit the bandwidth consumed by traffic controlled by the public policies. Since the rate entered for maximum bandwidth applies only to the traffic the policy controls, care has to be taken because public access traffic is controlled by four policies at any given time. There are branch and main office policies for public terminals and WiFi connections. The maximum bandwidth specified in each policy doesn't take into account any of the others. If you wanted to limit all public access to the Internet to no more than 200KB/s, you have to divide this value among the four active policies.



# The future

In the design of the example library network detailed in this document, decisions were made about how it should function when initially installed. Assumptions on how the network will be used may be incorrect, or usage may change over time. The network can be modified to facilitate changing usage or new requirements. For example:

## Logging

Should the library require detailed logging, a FortiAnalyzer unit can be added to the main office network. The FortiGate-800 cluster could then be configured to send traffic and event data to the FortiAnalyzer. Detailed reports can be generated to chart network utilization, Internet use, and attack activity.

Should the library switch to a VoIP telephone system, reports can also be generated on telephone usage.

## Decentralization

If a more decentralized approach is required, Internet access from branch offices could bypass the main office entirely. Branch FortiGate units would still maintain VPN-encrypted communication for secure access to the library servers. A FortiManager device would minimize the administrative effort required to deploy, configure, monitor, and maintain the security policies across all branch office FortiGate units.

## Staff WiFi

The FortiWiFi-60A supports the creation of virtual WiFi interfaces. If staff members require WiFi connectivity, a virtual WiFi interface could be created to allow them full access to staff network resources while maintaining the current limited access provided to public access users.

## Further redundancy

Although the FortiGate-800 cluster ensures minimal downtime with hardware redundancy, adding another Internet connection from a different ISP can provide connection redundancy to the main office.

The FortiWiFi-60A used in the branch offices supports the same High-Availability clustering as the FortiGate-800 so if needed, the branch offices could enjoy the same HA protection as the main office without having to upgrade to higher models.



**FORTINET™**

[www.fortinet.com](http://www.fortinet.com)

**F**ORTINET™

[www.fortinet.com](http://www.fortinet.com)