
# FortiGate™ Best Practices
# Version 1

FORTINET™

www.fortinet.com

*FortiGate™ Best Practices Technical Note*
Version 1
March 20, 2007
00-28000-0204-20070320



**Trademarks**
ABACAS, APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, 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.

**Regulatory compliance**
FCC Class A Part 15 CSA/CUS

**Caution:** If you install a battery that is not the correct type, it could explode. Dispose of used batteries according to local regulations.

# Table of Contents

# Introduction

This chapter introduces you to FortiGate Best Practices and the following topics:



## About the FortiGate Antivirus Firewall

The FortiGate Antivirus Firewall supports network-based deployment of application-level services, including virus protection and full-scan content filtering. FortiGate units improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network.

The FortiGate unit is a dedicated easily managed security device that delivers a full suite of capabilities that include:

- application-level services such as virus protection and content filtering,
- network-level services such as firewall, intrusion detection, VPN, and traffic shaping.

The FortiGate unit employs Fortinet's Accelerated Behavior and Content Analysis System (ABACAS™) technology, which leverages breakthroughs in chip design, networking, security, and content analysis. The unique ASIC-based architecture analyzes content and behavior in real-time, enabling key applications to be deployed right at the network edge where they are most effective at protecting your networks. The FortiGate series complements existing solutions, such as host-based antivirus protection, and enables new applications and services while greatly lowering costs for equipment, administration, and maintenance.

## About this document

This document is a collection of operating guidelines to ensure the most effective and secure operation of your FortiGate unit.

This document contains the following chapters:

# FortiGate documentation

Information about FortiGate products is available from the following guides:

- *FortiGate QuickStart Guide*

  Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*

  Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*

  Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*

  Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*

  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*

  Describes the structure of FortiGate log messages and provides information about the log messages that are 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 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.

# Related documentation

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

## FortiManager documentation

- *FortiManager QuickStart Guide*

  Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.
- *FortiManager System Administration Guide*

  Describes how to use the FortiManager System to manage FortiGate devices.
- *FortiManager System online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the FortiManager Console as you work.

## FortiClient documentation

- *FortiClient Host Security User Guide*

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

  Provides information and procedures for using and configuring the FortiClient software.

## FortiMail documentation

- *FortiMail Administration Guide*

  Describes how to install, configure, and manage a FortiMail unit in gateway mode and server mode, including how to configure the unit; create profiles and policies; configure antispam and antivirus filters; create user accounts; and set up logging and reporting.
- *FortiMail online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Web Mail Online Help*

  Describes how to use the FortiMail web-based email client, including how to send and receive email; how to add, import, and export addresses; and how to configure message display preferences.

## FortiLog documentation

- *FortiLog Administration Guide*

  Describes how to install and configure a FortiLog unit to collect FortiGate and FortiMail log files. It also describes how to view FortiGate and FortiMail log files, generate and view log reports, and use the FortiLog unit as a NAS server.
- *FortiLog online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

### Fortinet Knowledge Center

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

### Comments on Fortinet technical documentation

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

## Customer service and technical support

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

You can also register Fortinet products and service contracts from http://support.fortinet.com and change your registration information at any time. For information about our priority support hotline (live support), see http://support.fortinet.com.

When requesting technical support, please provide the following information:

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

# FortiGate best practices

## Overview

The FortiGate Best Practices is a collection of guidelines to ensure the most secure and reliable operation of FortiGate units in a customer environment. It is updated periodically as new issues are identified.

## General Considerations

1. For security purposes, NAT mode is preferred because all the internal or DMZ networks can have secure private addresses. NAT mode policies use network address translation to hide the addresses in a more secure zone from users in a less secure zone.
2. Use virtual domains (VDOMs) to group related interfaces or VLAN subinterfaces. Using VDOMs segments networks and creates added security by limiting the scope of threats.
3. Use Transparent mode when a network is complex and does not allow for changes in the IP addressing scheme.
4. On units running FortiOS v2.80 firmware prior to MR9, the option to automatically adjust the system for Daylight Savings Time should be disabled. A software anomaly in these versions of the firmware can cause instability. Time zones that do not observe Daylight Savings Time are not affected.

## Network hardware connectivity

1. Make sure that there is no “back door” access to the protected network. For example, if there is a wireless access point, it must be appropriately protected with password and encryption.
2. When you are running the FortiGate unit in Transparent mode, do not connect two ports to the same VLAN on a switch or to the same hub. Some Layer 2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN.
3. If you operate multiple VLANs on your FortiGate unit in Transparent mode, configure a separate virtual domain for each VLAN and do not configure any of your VLANs in the root domain. ARP packets are not forwarded between virtual domains. As a result, switches do not receive multiple ARP packets with the same source MAC but different VLAN IDs, which can cause instability.

### Wireless connectivity

1. Always enable the strongest data security that your clients support. WPA security is stronger than WEP. WEP 128-bit encryption is stronger than WEP 64-bit encryption.
2. Do not enable broadcast of your wireless network ID (SSID). This makes it more difficult for unauthorized users to discover your network.
3. If possible, reduce the transmitter power of your wireless access point so that the signal is not available beyond the areas where it is needed.

## System settings

### Backup

1. Always back up the complete FortiGate unit configuration, including VPN certificates and IPS signatures, before upgrading or downgrading the firmware.

### Administration

1. Allow management access to the FortiGate unit from trusted networks only. Better yet, allow connections for administration from specific IP addresses only using the trusted hosts feature.
2. When you create additional administrators, use access profiles to limit their access to the parts of the FortiGate unit configuration required for their roles.
3. Make sure that administrator passwords are at least six characters long and use both alphabetic and numeric characters.
4. Disable all management access to the public interface of the FortiGate unit unless for troubleshooting.
5. Do not change the administrator idle timeout from the default of five minutes.
6. Make sure that the system time and time zone are correct.
7. If your FortiGate unit has an LCD panel, restrict access to the control buttons and LCD by requiring a PIN.
8. Use a different host name on each FortiGate unit when managing multiple FortiGate units of the same model or when configuring an HA cluster.

### Antivirus and IPS definitions updates

1. Configure the FortiGate unit to accept scheduled and push updates of antivirus and attack definitions. To receive scheduled updates and push updates, you must register the FortiGate unit on the Fortinet support web page.
2. To receive scheduled FortiGuard updates and to send alert email, the FortiGate unit requires access to a valid DNS server.

# Firewall

1. Be careful when disabling or deleting firewall settings. Changes that you make to the firewall configuration using the GUI or CLI are saved and activated immediately.
2. Arrange firewall policies in the policy list from more specific to more general. The firewall searches for a matching policy starting at the top of the policy list. For example, a very general policy matches all connection attempts. When you create exceptions to a general policy, you must add them to the policy list above the general policy.
3. If you remove all policies from the firewall there are no policy matches and all connections are dropped.
4. You must add a valid user group to activate the authentication check box on the firewall policy configuration page.
5. Users can authenticate with the firewall using HTTP, Telnet, or FTP. For users to be able to authenticate, you must add an HTTP, Telnet, or FTP policy that is configured for authentication.
6. The settings for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address. Do not use Any as a service. Use subnets or specific IP addresses for source and destination addresses and use individual services or service groups.
7. Use a 32-bit subnet mask when creating a single host address, for example, 255.255.255.255.
8. Make sure to select the correct external interface when creating a new virtual IP (VIP). The external interface should be set to the interface at which the FortiGate unit receives connection requests from external networks.
9. Use the external IP of 0.0.0.0 when creating a VIP for a FortiGate unit where the external interface IP address is dynamically assigned.
10. Do not enable NAT for inbound traffic unless it is required by an application. If, for example, NAT is enabled for inbound SMTP traffic, the SMTP server might act as an open relay.
11. Traffic shaping bandwidth management is in kilobytes. You must multiply by 8 to calculate the kilobits.

# Intrusion Protection System

1. Disabling unnecessary IPS attack signatures can improve system performance and reduce the number of IPS log messages and alert emails. For example, if your network does not contain IIS web servers, you can disable the IIS signatures.
2. Administrators can change the threshold value for some attack prevention signatures such as SynFlood. Be careful to set thresholds appropriately to allow legitimate traffic. For example, with regard to ICMP flood prevention, if the administrator sets the ICMP threshold too low, normal ping traffic is blocked.
3. Use caution when enabling the diagnose sniffer CLI options during an attack on a live network, because this feature takes a lot of CPU resources.

# Antivirus

1. There are 17 file types in the default antivirus file block list. Blocking all these file types is enabled by default when you enable file blocking. Be careful to confirm that you need all these file types blocked. For instance, .doc files are blocked by default. If .doc files are sent and received as a normal part of your network traffic you can disable the blocking of .doc files.
2. FortiGate units support the quarantine of infected files on an internal hard disk, if the unit has one, or to a FortiLog unit.
3. You can configure the FortiGate unit to buffer 1 to 15 percent of available memory to store oversized files and email. The FortiGate unit then blocks a file or email that exceeds this limit instead of bypassing antivirus scanning and sending the file or email directly to the server or receiver. The FortiGate unit sends a replacement message for an oversized file or email attachment to the HTTP or email proxy client.
4. Administrators can block oversized files by selecting block for Oversized File/Email on the Content Profile tab.
5. Consider reducing the Oversize Threshold memory settings if the FortiGate unit shows persistently high memory usage.

# VPN

1. Create separate user groups for each PPTP or L2TP VPN, and for each IPSec VPN with dialup clients.
2. For PPTP and L2TP VPNs, assign VIP addresses in the subnet that clients need to access. This makes it appear as if the clients are directly connected to the target network.
3. Configure protection profiles for PPTP, L2TP, or IPSec user access. Enable the required profile in the firewall policy for each user group.
4. Firewall encryption policies for traffic that passes through an IPSec VPN tunnel should always be placed above policies with similar source and destination addresses.
5. Do not enable inbound NAT or outbound NAT for an IPSec policy unless a NAT device exists between the VPN peers.
6. Use Microsoft Point-to-Point Encryption (MPPE) to secure communications on PPTP VPNs.
7. For a multi-site IPSec VPN, use a hub-and-spoke configuration instead of a fully-meshed or partially-meshed topology.

# High Availability

1. Use active-passive HA for a more resilient session failover environment than active-active HA. In active-passive HA, session failover occurs for all traffic. Active-active HA does not provide session failover for virus scanning traffic.
2. Use Active-Active HA to distribute TCP and virus scanning among multiple cluster units. An active-active cluster may have higher throughout than a standalone FortiGate unit or than an active-passive cluster.
3. Isolate HA heartbeat interfaces from your user networks. Heartbeat packets contain sensitive cluster configuration information and can consume a considerable amount of network bandwidth. If the cluster consists of two FortiGate units, connect the heartbeat interfaces directly using a crossover cable. For larger clusters, connect the heartbeat interfaces to a separate switch that is not connected to any network.
4. Configure and connect multiple heartbeat devices so that if one heartbeat device fails, HA heartbeat traffic can continue to be transmitted using the backup heartbeat device.
5. If heartbeat traffic cannot be isolated from user networks, enable heartbeat message encryption to protect cluster information.
6. Wait until a cluster is up and running and all interfaces are connected before enabling HA monitor priorities. A monitored interface can easily become disconnected and cause failovers to occur before the cluster is fully configured and tested.
7. Monitor interfaces connected to networks that process high priority traffic so that the cluster maintains connections to these networks if a failure occurs.
8. Use SNMP, syslog, or email alerts to monitor a cluster for failover messages. Alert messages about cluster failovers may help find and diagnose network problems quickly and efficiently.

www.fortinet.com

www.fortinet.com