



**FortiGate Traffic Shaping  
Version 2.80**



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

*FortiGate Traffic Shaping Technical Note*  
Version 2.80  
March 10, 2006  
01-28000-0304-20060310

© Copyright 2005 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

#### **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.

#### **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.

# Contents

<b>Introduction .....</b>	<b>5</b>
<b>Revision history .....</b>	<b>5</b>
<b>About FortiGate traffic shaping.....</b>	<b>5</b>
<b>About this document.....</b>	<b>5</b>
<b>Fortinet documentation .....</b>	<b>5</b>
Fortinet documentation CDs .....	7
Fortinet Knowledge Center .....	7
Comments on Fortinet technical documentation .....	7
<b>Customer service and technical support .....</b>	<b>7</b>
<b>FortiGate traffic shaping .....</b>	<b>9</b>
<b>Quality of Service (QoS) and traffic shaping .....</b>	<b>9</b>
<b>FortiGate QoS .....</b>	<b>10</b>
Guaranteed bandwidth and maximum bandwidth .....	10
Traffic Priority .....	10
<b>Traffic shaping Token bucket filter .....</b>	<b>11</b>
<b>Traffic shaping considerations .....</b>	<b>12</b>
<b>Configuring FortiGate traffic shaping.....</b>	<b>13</b>



# Introduction

This chapter introduces you to FortiGate traffic shaping and the following topics:

- [Revision history](#)
- [About FortiGate traffic shaping](#)
- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

## Revision history

Version	Date	Description of changes
First Release	4 April, 2003	First draft for FortiOS v2.36
Second revision	10 March 2006	Updated for FortiOS v2.80

## About FortiGate traffic shaping

FortiGate firewalls use traffic shaping to implement Quality of Service (QoS). Using traffic shaping, you can provide better service to selected network traffic without causing interruptions to other traffic.

## About this document

This document discusses Quality of Service (QoS) and traffic shaping, describes FortiGate traffic shaping using the token bucket filter mechanism, and provides general procedures and tips on how to configure traffic shaping on FortiGate firewalls.

## 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 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 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 documentation CDs

All Fortinet documentation is available from the Fortinet documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

## 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 that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

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



# FortiGate traffic shaping

This document contains the following sections:

- [Quality of Service \(QoS\) and traffic shaping](#)
- [FortiGate QoS](#)
- [Traffic shaping Token bucket filter](#)
- [Traffic shaping considerations](#)
- [Traffic shaping considerations](#)

## Quality of Service (QoS) and traffic shaping

Quality of service (QoS) is the capability of a network to provide better service to selected network traffic without causing interruptions to other traffic. A full QoS solution identifies and prioritizes different types of traffic.

To use the FortiGate QoS feature effectively, organizations should identify the types of traffic that are important to the organization, the types of traffic that make intensive use of bandwidth, and the types of traffic that are sensitive to latency.

For example, a company may want to guarantee sufficient bandwidth for revenue producing e-commerce traffic. They need to ensure that transactions can be completed and that clients do not experience service delays and interruptions. At the same time, the company may need to ensure sufficient bandwidth for customer support and for corporate communications. Properly implemented QoS can ensure bandwidth is available on a priority basis for each of these types of traffic.

QoS is equally important for managing voice and multi-media traffic. These types of traffic use a lot of bandwidth and are sensitive to latency. Properly implemented QoS provides the bandwidth and flow required for these types of traffic while reserving some bandwidth for other traffic with lower bandwidth and less demanding latency requirements.

The Fortinet implementation of QoS uses the following techniques:

**Traffic shaping** Uses buffering and smoothing to regulate traffic flows based on packet rate. Packets that exceed thresholds are stored in a buffer for later transmission. Unlike policing, traffic shaping attempts to avoid dropping packets. It may add to latency as packets are buffered and then transmitted.

**Queuing** Used with buffering to determine the priority of packets to be transmitted. Traffic types are assigned high, medium, and low priority. If there is not enough bandwidth to transmit all traffic, high priority traffic is processed before medium, and low priority traffic.

## FortiGate QoS

FortiGate traffic shaping is available for all supported services, including H.323, TCP, UDP, ICMP, and ESP.

FortiGate QoS applies traffic shaping and queuing using individual firewall policies. FortiGate traffic shaping uses the token bucket filter technique to guarantee and limit bandwidth. See [“Traffic shaping Token bucket filter” on page 11](#) for a description of how token bucket filters work.

Guaranteed and maximum bandwidth in combination with queuing ensures minimum and maximum bandwidth is available for traffic.

Traffic shaping cannot increase the total amount of bandwidth available, but it can be used to improve the quality of bandwidth-intensive and sensitive traffic.

### Guaranteed bandwidth and maximum bandwidth

When you enter a value in the Guaranteed Bandwidth field of a firewall policy you guarantee the amount of bandwidth available for selected network traffic (in Kbytes/sec). For example, you may want to give a higher guaranteed bandwidth to your e-commerce traffic.

When you enter a value in the Maximum Bandwidth field of a firewall policy you limit the amount of bandwidth available for selected network traffic (in Kbytes/sec). For example, you may want to limit the bandwidth of IM traffic usage, so as to save some bandwidth for the more important e-commerce traffic.

The bandwidth available for traffic controlled by a policy is used for both the control and data sessions and is used for traffic in both directions. For example, if guaranteed bandwidth is applied to an internal to external FTP policy, and a user on an internal network uses FTP to put and get files, both the put and get sessions share the bandwidth available to the traffic controlled by the policy.

The guaranteed and maximum bandwidth available for a policy is the total bandwidth available to all traffic controlled by the policy. If multiple users start multiple communications session using the same policy, all of these communications sessions must share from the bandwidth available for the policy.

However, bandwidth availability is not shared between multiple instances of using the same service if these multiple instances are controlled by different policies. For example, you can create one FTP policy to limit the amount of bandwidth available for FTP for one network address and create another FTP policy with a different bandwidth availability for another network address.

### Traffic Priority

Set traffic priority to manage the relative priorities of different types of traffic.

Priority management can be used to provide additional QoS for sensitive traffic. Important and latency-sensitive traffic should be assigned a high priority. Less important and less sensitive traffic should be assigned a low priority.

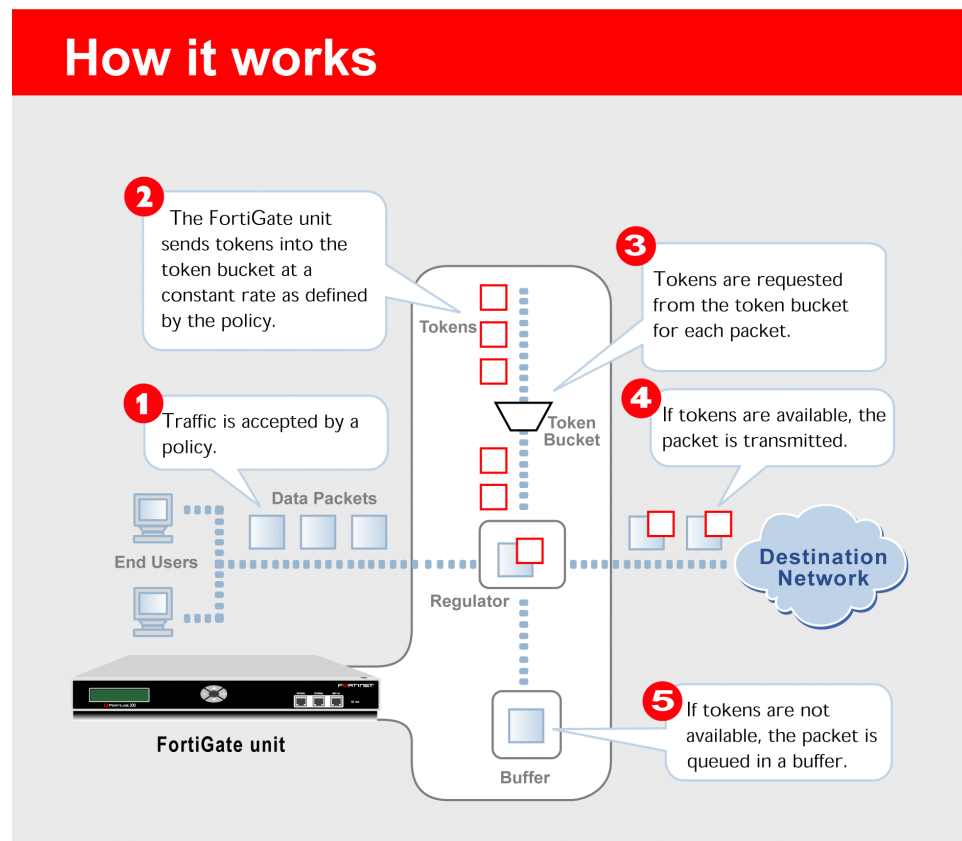
The FortiGate Antivirus Firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.

For example, you can add policies to guarantee bandwidth for voice and e-commerce traffic. Then you can assign a high priority to the policy that controls voice traffic and a medium priority to the policy that controls e-commerce traffic. During a busy time, if both voice and e-commerce traffic are competing for bandwidth, the higher priority voice traffic will be transmitted before the e-commerce traffic.

## Traffic shaping Token bucket filter

A traffic shaping token bucket filter is a dampening function that delays some traffic by buffering bursts that exceed predefined rates. FortiGate traffic shaping uses a token bucket filter to control traffic flow. The token bucket filter is a pure traffic shaper that does not schedule traffic. It is non-work-conserving and may throttle itself, even if packets are available, to ensure that the configured rate is not exceeded.

Figure 1: Token bucket filter mechanism for traffic shaping



A token bucket uses a system counter defined by the equation  $R = B/T$ .

Where:

- R** Is the mean rate in KBytes per second. This is the rate at which the bucket fills with tokens. No peak rate is defined. The mean rate specifies how much data can be sent or forwarded per unit time on average. The mean rate is equivalent to the maximum bandwidth.
- B** Is the burst size. This is the capacity of the bucket (also called the committed burst (Bc) size). The burst size specifies in KBytes per burst how much traffic can be sent within a given unit of time without creating scheduling concerns. The burst size is equivalent to the guaranteed bandwidth.
- T** Is the time interval (also called the measurement interval). The time interval specifies the time in seconds per burst.

The token bucket acts as a regulator using the following mechanism:

- Tokens are added to the bucket at a the mean rate (R). The bucket has a specified capacity. Each token represents the ability to send a certain number of bytes into the network. For example, if the token represents 500 bytes, the regulator function of the bucket could request three tokens for a 1,500-byte packet and one token for a 500-byte packet. Every packet must use up one or more tokens. In our example, a packet smaller than 500 bytes will still use one token. Even a zero-sized packet will use a token.
- If the bucket fills to capacity (B), newly arriving tokens are discarded. Therefore, the maximum burst size is limited to the size of the bucket.
- To allow a packet through, the regulator function of the bucket requests a number of tokens equal to the packet size.
- If there are not enough tokens in the bucket, the packet is buffered in a queue until the bucket has enough tokens.
- Traffic shaping guarantees burst size and timing so that the flow will never send packets more quickly than the capacity of the token bucket plus the time interval multiplied by the established rate at which tokens are placed in the bucket.
- Traffic shaping guarantees that the overall transmission rate does not exceed the established rate at which tokens are placed in the bucket.

## Traffic shaping considerations

Traffic shaping will by definition attempt to “normalize” traffic peaks/bursts and can be configured to prioritize certain flows over others. But there is a physical limitation to the amount of data which can be buffered and for how long. Once these thresholds have been surpassed, frames and packets will be dropped, and sessions will be affected. Incorrect traffic shaping configurations may actually further degrade certain network flows, since the excessive discarding of packets can create additional overhead at the upper layers, which may be attempting to recover from these errors.

A basic traffic shaping example would be to prioritize certain traffic flows at the detriment of other traffic which can be discarded. This would mean that you accept to sacrifice certain performance and stability on traffic X, in order to increase or guarantee performance and stability to traffic Y.

If for example you are applying bandwidth limitations to certain flows, you must accept the fact that these sessions can be limited and therefore negatively impacted.

Traffic shaping which is applied to a firewall policy, is enforced for traffic which may flow in either direction. Therefore a session which may be setup by an internal host to an external one, via a Internal -> External policy, will have Traffic shaping applied even if the data stream is then coming from external to internal. For example, an FTP "get" or a SMTP server connecting to an external one, in order to retrieve email.

Also note that traffic shaping is effective for normal IP traffic at normal traffic rates. Traffic shaping is not effective during extremely high-traffic situations where the traffic is exceeding the FortiGate unit's capacity. Packets must be received by the FortiGate unit before they are subject to traffic shaping. If the FortiGate unit cannot process all of the traffic it receives, then dropped packets, delays, and latency are likely to occur.

To ensure that traffic shaping is working at its best, ensure that the interface ethernet statistics are clean of errors, collisions or buffer overruns. If these are not clean, then FortiGate and switch settings may require adjusting.

To make traffic shaping work efficiently, be sure to observe the following rules:

- Enable traffic shaping on all firewall policies. If you do not apply any traffic shaping rule to a policy, the policy is set to high priority by default.
- Distribute firewall policies over all three priority queues (low, medium and high).
- Be sure that the sum of all Guaranteed Bandwidth in all firewall policies is significantly less than the bandwidth capacity of the interface.

## Configuring FortiGate traffic shaping

You enable and specify traffic shaping settings when you configure firewall policies.

### To configure traffic shaping

- 1 Go to **Firewall > Policy**.
- 2 When you create a new policy or edit a policy, select the Traffic Shaping option.
- 3 Configure the following three options:
  - Guaranteed Bandwidth
  - Maximum Bandwidth
  - Traffic Priority



**Note:** If you set both guaranteed bandwidth and maximum bandwidth to 0 (zero), the policy does not allow any traffic.



**F**ORTINET™

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

**FORTINET™**

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