



The FortiGate™-2000 Network Protection Gateway– The Next Generation Architecture for Gigabit Content Processing

White Paper

Abstract

August, 2002

The FortiGate-2000 Network Protection Gateway (NPG) is a service provider/telco class product that addresses the most stringent security requirements of large enterprises and service providers. With a uniquely designed architecture, the FortiGate-2000 NPG delivers unparalleled reliability and performance for today's applications, and also provides expandability to address future needs. Both application-level services such as antivirus and content filtering, and network level services including firewall, VPN, and network based IDS (NIDS) are provided with real-time performance.

This white paper describes the FortiGate-2000 system architecture, and explains how high reliability and performance are achieved using this unique design. The paper also explains how the FortiGate-2000 architecture offers superior investment protection.

© 2002 Fortinet, Inc. All rights reserved.

The information contained in this document represents the current view of Fortinet, Inc. on the issues discussed as of the date of publication.

This document is for informational purposes only. FORTINET MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Fortinet Corporation.

Fortinet may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Fortinet, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

Fortinet, FortiGate, FortiASIC, are either registered trademarks or trademarks of Fortinet Inc., in the United States and/or other countries.

Fortinet Inc.

3333 Octavius Drive

Santa Clara, CA 95054; USA

Contents

Introduction to the FortiGate-2000 NPG	4
FortiGate-2000 Features and Functions	5
The FortiGate-2000 FortiOS Advantages	6
The FortiGate-2000 Content Processing Hardware Architecture	9
For More Information	13

Introduction to the FortiGate-2000 NPG

In the summer and fall of 2001, many companies suffered significant costs and inconvenience from the Code Red and Nimda worms. The combined damage to enterprises worldwide has been estimated at more than US\$10Bn. These incidents introduced a new type of Internet attack, now commonly known as a blended threat, which went completely undetected by conventional network protection systems.

Traditional network security solutions, such as firewall and VPN gateways, were unable to prevent these attacks, and as such most organizations now realize that these limited tools do not provide sufficient protection for their networks. Existing host-based virus and worm scanning products provide the only line of defense against such attacks, because conventional firewall technologies leave the network “front door” wide open. And while it seems obvious that these threats should be detected and stopped before they penetrate exterior defense and reach host computers, until now no product has emerged that can detect and eliminate content-based attacks at the network edge without compromising performance.

Enterprises and service providers need integrated solutions that address all of the threats endangering the corporate network, from security threats such as viruses, worms, and intrusions, to inappropriate use of the web and other threats to organizational productivity. In addition, they need these comprehensive network services to be delivered at gigabit performance, with high reliability and availability, and with headroom to accommodate new functions as dictated by changing business needs and the constant advance of network threats.

The FortiGate-2000 Network Protection Gateway (NPG) is a gigabit-capacity, content processing gateway. The FortiGate 2000 NPG features the world’s first Application Specific Integrated Circuit (ASIC)-based, network edge system that provides real-time virus scanning, content filtering, virtual private networking (VPN), stateful inspection and NAT firewall, and network based Intrusion Detection in a single, easily managed unit. The unique modular architecture of the FortiGate-2000 NPG includes critical components such as a real-time operating system, symmetric multi-processing, dual CPU management module, a high speed backplane, a content processing acceleration unit, and high availability via stateful failover. This architecture delivers unparalleled performance and reliability, and allows for integration of new technologies and applications over time. The FortiGate 2000 NPG is the world’s first and most scalable integrated network protection gateway operating at both the application and network layers.

The FortiGate Product Family: The FortiGate-2000 NPG is a member of the FortiGate family of Network Protection Gateways (NPGs). Each member of the FortiGate family is a dedicated, hardware-based unit that delivers complete network protection services deployed at the network edge. Based on Fortinet’s ABACAS™ (Accelerated Behavior and Content Analysis System) technology and FortiASIC™ Content Processor, the FortiGate series breaks the Content Processing Barrier – providing the significant computational power required to handle processing intensive tasks such as virus scanning and content filtering, combined with firewall, VPN, intrusion detection, and traffic shaping functions. The FortiGate Series provides the most cost-effective, convenient, and powerful network protection available. The FortiGate family includes FortiGate 50 and 100 for the SOHO/branch office market, FortiGate 200, 300, and 400 for the small-medium-sized enterprises (SME), and the FortiGate 500 and 2000 targeting large enterprise and service provider environments.

FortiGate-2000 Features and Benefits

The FortiGate-2000 NPG delivers carrier-class performance that meets the needs of large enterprise and service provider networks. It provides today's networking customers with unmatched security, reliability, and performance. In



addition to stateful inspection firewall functionality and high-performance IPSec encryption, the FortiGate-2000 NPG recognizes and eliminates all of the viruses reported by the WildList virus organization, filters and blocks over 2 million websites that contain undesirable content, and detects (and potentially blocks) over 1300 intrusion attacks. The system performance scales up to 2Gbps, with support for over 500,000 concurrent sessions. The following list provides highlights of the FortiGate-2000 NPG:

- Hardware acceleration to ensure real-time performance
- High-performance, stateful inspection firewall
- Automatically updated virus and worm definitions block 100% of the viruses and worms in the wild; Signature and macro virus scanning eliminated threats from all email attachments, web content and downloads
- Content filtering blocks web plug-ins such as ActiveX, Java Applets, and Cookies
- High availability via stateful fail-over
- Industry standard IPSec, PPTP, and L2TP VPNs provide secure communication between networks and clients using DES and 3DES encryption

The FortiGate-2000 NPG can be installed at the customer premises at the junction between the corporate network and the Internet, or within the service provider's infrastructure. It provides 2 Fiber/Copper Gigabit Ports and 4 10/100 BaseTX ports. In a typical deployment, the FortiGate-2000 NPG processes all packets and content traveling to and from the public network (e.g., the Internet). The FortiGate 2000 NPG allows or denies traffic based on the policy configuration. Different modes of operation are available, such as NAT (Network Address Translation) mode, Transparent mode, and Route mode. The FortiGate 2000 NPG includes a high-availability port and fail-over logic to support redundant configurations, making it ideal for mission-critical applications.

A partial list of benefits brought by the FortiGate 2000 NPG include:

- Closes the vulnerability window on worms and viruses through content processing at the network level without affecting network performance, an especially important consideration for service providers and enterprises. For service providers, virus scanning may represent a new service revenue stream
- Supplements or replaces current existing security solutions; In "green field" applications, reduces initial capital expenditures (CAPEX) by 50-80%.
- Integrated administration increases manageability and reduces ongoing operating expenses (OPEX) by 20-50%.
- Zero interruption to business during fail-over

The high performance, reliability, and high flexibility offered by the FortiGate 2000 NPG are built upon a solid architecture foundation. In the following sections we will examine the two integral components in the FortiGate architecture: the security-hardened, proprietary FortiOS, and the modular FortiGate hardware system architecture.

The FortiGate 2000 NPG FortiOS: Features and Advantages

Fortinet's FortiOS is a purpose built, proprietary, real-time, and security-hardened operating system that provides the support for the virus scanning, content filtering, stateful inspection firewall, IP security (IPSec) VPN, network based IDS, and traffic shaping applications provided on all FortiGate platforms. The following sections highlight features in the FortiOS design that enables the application-layer and network layer functions to be delivered at high performance, high reliability, and with high flexibility/expandability.

High Performance Parallel Processing: The FortiGate 2000 NPG is designed with dual-CPU's. Using symmetric multi-processing technology, the FortiOS effectively splits and coordinates different tasks between the two processors. At any given time, both processors are loaded at their optimal processing level. The overhead associated with job division and coordination is minimized using a Fortinet proprietary algorithm.

Real-time Architecture: In contrast to a non-real time OS (e.g., the different flavors of Linux that many firewall and VPN appliances are based on), the FortiOS is a real-time operating system optimized for data flow processing. In a non-real time operating system, the kernel doesn't always respond to an interrupt triggered by an incoming data packet waiting to be processed; this not only increases the queuing time for packets, but also leads to inefficient use of the system resources (e.g., memory) and therefore increases packet loss rate. The design of FortiOS integrates intelligent queue and pipeline management, and system interrupts associated with packet arrival/processing receive immediate attention. The "queuing time" of packets waiting in line is therefore minimal and predictable. At the same time, hardware acceleration (see later sections) based on the FortiGate Content Processing Acceleration Module minimizes the processing time for all types of traffic, which, combined with minimized queuing time, delivers the best real-time user experience.

Real-Time Content Level Intelligence: Conventional security gateway designs fall into two categories: Stateful packet inspection (flow-based) designs, and application proxy designs. In a flow-based gateway, security policies are defined and executed largely at the packet level (although stateful inspection does keep the context of sessions for certain types of traffic). This approach lends itself to high processing speed and high throughput since packets are forwarded immediately after processing; however, since the processing is at the packet level, the system doesn't understand the higher-layer languages (i.e., protocols) or objects (e.g. files) and therefore cannot identify malicious scripts, virus attacks, or undesirable content. In contrast, in a proxy based system, the security gateway terminates incoming and outgoing sessions, inspects packets, reassembles them into their original stream, understands the current state in a session, and is able to inspect the content for any violation of predefined or dynamically generated security or network policies. The pros and the cons of this approach are the inverse of the flow based approach: Proxy based gateways are intelligent enough to operate at the application layer and can therefore perform content-level processing. However, reassembling all the packets and inspecting the stream takes significant computing resources, and as such proxy-based gateways usually suffer low performance.

The FortiGate 2000 NPG (as well as the rest of the product family) is designed to take advantage of the benefits of flow-based and proxy-based designs while mitigating their weaknesses. The FortiOS is designed with both a flow-based inspection engine and multiple application layer

proxies (HTTP, SMTP, POP3, IMAP, etc.). The patent-pending design delivers optimal coordination between the packet inspection engine and the proxies. The hardware acceleration provided by the FortiASIC and FortiGate Content Acceleration Unit in the FortiGate 2000 NPG provides the intelligence of a proxy-based system with the performance typically obtainable only from a flow-based system. This unique design represents a major technological breakthrough and is the subject of numerous pending patents. As a result, the FortiGate 2000 NPG is not only capable of the conventional network level security functions such as firewall, VPN, and NIDS, but also capable of handling the application layer security functions including virus and worm scanning, URL and keyword based content filtering, and secure, cross-firewall Voice over IP (VoIP), all delivered at very high speeds at the network edge.

Complete Network Protection with Complete Investment Protection: Another benefit of the FortiOS design is the ability to readily accommodate new functions and applications. The modular design enables new proxies to be added or modified easily. No changes are needed to the overall operating system architecture (or the hardware system architecture) to accommodate new protocols and services.

The ability of the FortiOS to accommodate Voice over IP (VoIP) NAT traversal support represents a perfect example of the operating system's flexibility. VoIP applications, which are increasingly rapidly in popularity, have been a challenge to deploy because the sophisticated VoIP protocols (e.g. H.323, MGCP, SIP, etc.) cannot be handled securely by conventional network address translation (NAT) firewalls. Without proxy ability, VoIP gateways require network administrators to open "holes" in their firewall in order to pass VoIP traffic. Of course, these holes can be exploited by intruders who can utilize voice traffic to spoof a firewall and gain unauthorized network access.

If a network protection gateway can be made to understand the complex VoIP protocols, they can process VoIP traffic securely, without opening indiscriminate "holes" that let VoIP as well as potentially damaging traffic through. As mentioned above, flow-based gateways generally lack the intelligence to understand sophisticated, high-level protocols, and conventional proxy-based designs lack the performance necessary to process latency-sensitive voice traffic without introducing unacceptable jitter and delay. This is where the FortiOS stands out: It easily accommodates an H.323-proxy that parses the body of H.323 messages. The high-performance FortiOS kernel, along with the purpose-built content-processing acceleration hardware, enables the FortiGate series to adapt to new applications without a major hardware upgrade or system redesign.

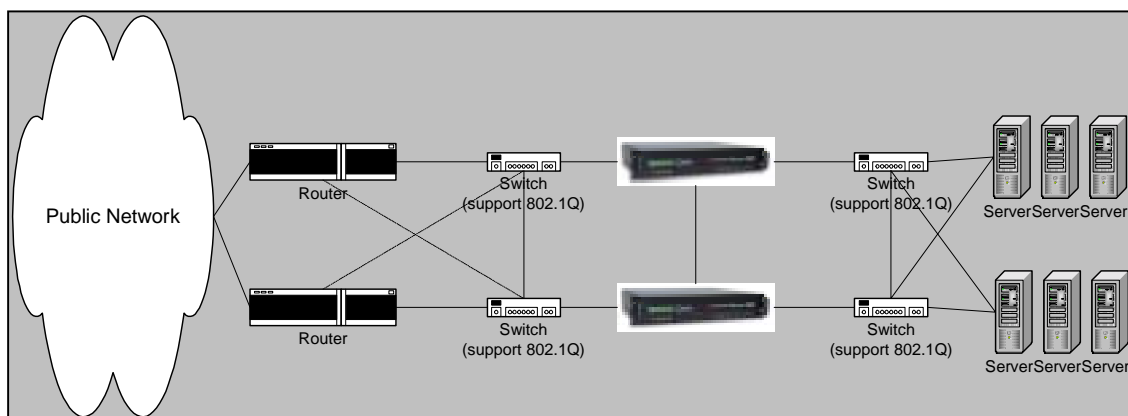
Virtual System Support Providing Compartmentalized Security: Large enterprises and managed service providers can both benefit from the ability to make a single FortiGate unit behave as if it contained numerous, independent "virtual systems" that provide dedicated services, with unique policies, for individual departments or customers.

Virtual system support has been designed into the FortiGate architecture. One or multiple VLANs complying with 802.1Q standard can be mapped to one virtual system, and switches/routers with VLAN trunking support will be interfaced with the physical ports of the FortiGate 2000 NPG. Up to 500 virtual systems will be provided on FortiGate 2000 NPG. Role-based administration will allow different administrators to manage only those virtual systems for which they're authorized, enabling them to create and maintain their own security policy sets, addresses and address groups, as well as monitor system status.

An Architecture to Deliver Closed-loop Protection: A major problem with conventional intrusion detection systems is suggested by the name itself – they’re “detection” systems only, and provide notification but do not protect against or prevent attacks. A primary reason for this limitation stems from the fact that most IDSs – like firewalls, antivirus scanners, and the like - are point solutions that don’t talk to each other.

The FortiOS platform forms a common framework that seamlessly and naturally integrates all of the applications that it supports. When the FortiGate NIDS detects an attack, it can take one or more preventative actions, such as resetting the connection, dropping the packets associated with the attack, alerting the firewall to block the attack (by either temporary blocking the source address or temporarily blocking the port under attack), or waiting to act until the attack indicator has passed a certain “threshold.” This is “closed loop” protection, a powerful concept that turns passive detection into proactive prevention.

FortiGate Redundancy Protocol (FGRP) for High Availability (HA): FortiGate NPGs are commonly deployed in mission critical environments, such as service provider infrastructures or in large enterprises that cannot tolerate a service loss due to a single point of failure. For these situations, customers deploy a redundant pair of FortiGate units, and take advantage of the FortiGate Redundancy Protocol (FGRP), to assure stateful failover in the unlikely event of a failure in one of the NPGs.



Like other well-known protocols that support high-availability, such as VRRP and HSRP for router fail-over, FGRP provides stateful fail-over for secure sessions. FGRP contains several technology components, including:

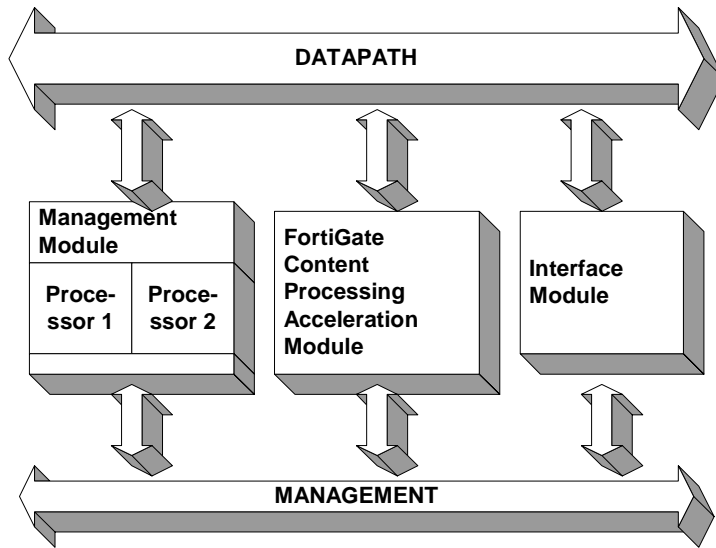
- Configurable heartbeat monitoring – The FortiGate units continuously ping each other to verify that each partner in the redundant pair is healthy. If one box fails or loses power, traffic will be serviced by the remaining unit.
- Link status monitoring: The NPGs monitor the status of traffic on upstream and downstream switches/routers, and will force a switchover from the standby to the active unit in order to maintain connectivity.

Using the capabilities of FGRP, FortiGate-2000 NPGs can be configured to work in a fully redundant environment where there’s no single point of failure (see diagram above). FortiGate-2000 can be configured to support hot-standby mode or active-active load sharing mode.

The FortiGate-2000 Content Processing Hardware Architecture

The hardware system architecture of the FortiGate-2000 NPG is purpose built to deliver gigabit throughput and optimized for layer 7 content processing as well as layer 2 and layer 3 packet level processing. The system contains four major components:

1. The Content Processing Acceleration Module (CPAM) – There are two components in the FortiGate-2000 NPG - each one of which is made up of one FortiASIC CP-I content processor chip and a FortiGate Content Processing Acceleration Unit (FCPAU). The FCPAU has a dedicated,



- programmable content inspection processor that works with other purpose built hardware components that have been optimized for intensive content search, pattern matching, and data analysis – the most time consuming processes in virus scanning, content filtering, and network based intrusion detection. The FortiASIC chip contains a patents-pending content processing engine, as well as a crypto acceleration engine and a firewall security policy engine built in. These engines handle, respectively, anti virus and worm detection, NIDS signature detection, acceleration of DES, 3DES, and AES, encryption, and NAT and firewall policy enforcement. The CPAM module has dedicated fast memory, and thus requires little interaction with the system memory on the management module via the system bus. This efficient data movement architecture contributes to the FortiGate-2000 NPG's very high throughput for application-level content processing.
2. The Management Module (MM) – The MM is based on a dual CPU design using two Pentium class high performance processors operating at 1Ghz. The management module is responsible for flow control, and for processing of exception packets and streams that are not handled efficiently by the Content Processing Acceleration Module. The MM also supports the various management interfaces and related functions (GUI, CLI, SNMP, etc.)
 3. The Backplane Bus Module (BBM) – The BBM made up of the Datapath and the Management bus. This module features a multi-bus design where control information and data exchange happen on two different buses – control information travels on the Management path, and data exchange between modules travels on the Datapath, providing multi-Gbps of traffic-carrying capacity. This design facilitates highly efficient communication between the different modules.
 4. The Interface Module (IM) – The IM supports the input/output interfaces, which include 2 Gigabit copper/fiber ports and 4 10/100 BaseTX ports. Traffic enters and leaves the

FortiGate-2000 NPG system through these physical ports. Depending on the nature of the traffic, packets are routed to the Management Module or the Content Processing Acceleration Module for processing. Note that if VLAN/virtual system support is enabled, data flowing in through one physical interface can represent traffic from multiple sub networks subject to different security policies.

The following sections focus on the content processing module and describe how the FortiGate-2000 NPG achieves very high application layer processing performance with its uniquely designed hardware acceleration.

Content Processing Acceleration Engine: The FortiASIC – CP1 Content Processor

FortiASIC-CP1 Content Processor– The FortiASIC CP1 , along with the FortiOS operating system, form the core of Fortinet’s ABACAS™ technology. The FortiASIC-CP1 combines high performance stream encryption and content scanning acceleration simultaneously to provide a comprehensive content processing solution on a single chip.



Using modular design, four powerful data processing engines are included in the FortiASIC CP1:

The signature scanning engine – This engine supports high-speed scanning for virus, worm, and intrusion attack signatures, as well as banned content. A key component of the signature scanning engine is the pattern matching module, which is designed to match an entire file, byte by byte, against a database of signatures that indicate the presence of viruses, worms, attacks, or blacklisted content.

Virus and worm signatures are stored in a dedicated, high-speed memory which is directly accessed by the FortiASIC CP1 without moving any data across the Datapath. This approach completely decouples scanning activity from packet movement, enabling the FortiGate-2000 NPG to provide application-layer processing without degrading overall system performance.

When traffic from one of the following application layer protocols – HTTP, SMTP, POP3, and IMAP – arrives at FortiGate NPG, the FortiOS directs the packets to the FortiASIC chip, which assembles the packets into files in the dedicated scanning memory. The FortiASIC scanning engine matches data against the signature database in the high-speed memory directly connected to it. Once the scanning is done FortiASIC interacts with the Management Module to notify the scanning result and receives the next batch of data. The operation is performed until an attack is detected or the entire file is scanned.

The crypto engine – FortiASIC CP1 offers a high performance cryptographic engine that supports DES, Triple-DES and AES encryption,. Triple-DES throughput for the FortiASIC CP1 tops 600Mbps.

The security policy engine – This subsystem provides packet and protocol parsing, and is key to enabling rapid matching of packet flows to policies. The policy engine handles firewall functions

such as address translation and stateful inspection, and also manages packet reassembly and fragmentation.

FortiGate Content Processing Acceleration Unit (FCPAU)



The FortiGate-2000 includes a FortiGate Content Processing Accelerator Unit (FCPAU) as an additional acceleration engine to further speed up application layer processing. FCPAU is functionally similar to the FortiASIC. The FortiOS intelligently splits tasks of content processing, data encryption, and security policy processing between FortiASIC and FCPAU.

The FCPAU plays an important role in the processing-intensive tasks associated with establishing and managing sessions, and includes a Public Key Cryptography engine to accelerate key generation and exchange. The FCPAU is programmable and can be software upgraded to accommodate new algorithms and applications.

High Reliability Inherent in the FortiGate NPG System Architecture

The FortiGate-2000 NPG is designed to meet the demanding requirements of service providers and large enterprises; reliability is the top architectural consideration in the design and is built-in from ground up:

- At component level, only high quality components (sourced from ISO-9000 certified vendors) are used in the FortiGate-2000 NPG.
- The dual processor architecture enables either CPU to take over the load in the event that one of the CPUs fails.
- Error Checking and Correction memory is employed to prevent intermittent memory failures.
- Redundant, hot-swappable power supplies and redundant, hot-swappable fan assemblies assure continuous operation and enable online repairs with no down-time.

For maximum reliability, the FortiGate 2000 NPG can be configured in a redundant, high-availability mode as mentioned in the FortiOS section. A hot standby unit maintains current sessions in the event of a unit failure.

Conclusions

The FortiGate-2000 is an integral member of the FortiGate NPG family, a series of products that are designed to handle not only network layer security but also the application level functions including virus and worm scanning, and content filtering.

Built on a security-hardened, real time operating system, with stateful failover redundancy logic, and accelerated by the patent pending FortiASIC and FortiGate Content Processing Acceleration Unit, FortiGate-2000 is an unparalleled network protection gateway. It meets the performance and reliability requirements of enterprises and service providers, and delivers extremely high security. The architecture enables rapid addition of new services without the need to change hardware. With integrated security and content management functions running in a single unit, upfront acquisition costs and ongoing administration costs are significantly reduced. The result is improved organizational security and productivity, with dramatically lower costs, and rapid return on investment.

For More Information

More information about Fortinet secure gateway products is available from the following sources.

Business Information

Please visit us at www.fortinet.com.

Potential Partners

Please contact us at partner@fortinet.com or visit us at www.fortinet.com.

Additional Resources

Please contact us at (1) 408-235-7700 for engineering/technical support.