

Next-Generation Security for Enterprise Networks

Summary

Since the concept of a 'next-generation firewall' was introduced several years ago by Gartner, many network security vendors have introduced their own next-generation firewalls to address this product category - but with varying results. Some next-generation firewalls fail to include important next-generation features as well as adequate traditional network protections because they lack a proven platform on which to build these features. As more threats leverage web-based applications and services to enter corporate networks, enterprises and service providers are deploying next-generation firewalls at faster pace in an effort to control applications and block these new methods of attack. Industry analysts caution, however, that many next-generation firewalls still lack basic network security features and organizations should deploy them in conjunction with other layers of security to deliver comprehensive security. They warn that once in the wild, viruses, malware and traditional methods of attack never go away. Therefore organizations must consider all security threats, both known and unknown, when selecting an enterprise network security platform.

Contents

Summary 2

Introduction 4

Enterprise and Service Provider Challenges 4

 Old Security Threats Never Go Away 4

 Accelerating Evolution of New Threats 5

 Web-based Attacks Increase Data Breach Costs 5

 Web 2.0 Applications 5

 Traditional Firewalls No Longer Effective 5

 Migration to Next-Generation Networks 6

The Next Step in Security Evolution: Next-Generation Security Platforms 6

 Next-Generation Security Technologies 6

 Application Control 7

 Integrated Intrusion Prevention System (IPS) 9

 Data Loss Prevention (DLP) 11

 Web Content Filtering 12

 Dual-stack IPv4 and IPv6 Support 13

 Integrated Wireless Controller 13

 Centralized Management 14

 Core Security Technologies 14

 Firewall - Stateful Traffic Inspection and Packet Filtering 14

 Virtual Private Network (VPN) 15

 URL Filtering 16

 Antivirus/ Antispyware 17

 Antispam 17

Conclusion 19

About Fortinet 20

About FortiOS 20

Introduction

The term 'next-generation firewall' (NGFW) came into popular use in 2009 with the publication of a Gartner report titled "Defining the Next Generation Firewall", and refers to a firewall that offers specific features to address changes in both the way business processes use IT and the ways attacks try to compromise business systems¹. In order to defend networks against the latest threats, NGFWs should include, at a minimum, an integrated intrusion prevention system (IPS) with deep packet scanning, the ability to identify and control applications running over a network, and the ability to verify a user's identity and enforce access policies accordingly.

Unfortunately, some NGFWs not only fail to provide these advanced next-generation features to guard against new attacks; they also fail to provide a mature platform of core network protections to block existing attacks. This is why industry analysts still caution that NGFW features are most effective when used in conjunction with other layers of security controls. In order to block all threats, NGFWs must also include traditional packet filtering, network address translation, stateful protocol inspection, and virtual private network (VPN) capabilities¹. In other words, to deliver the promised protections, NGFWs must be built on a solid, field-proven base of traditional or core network protections before attempting to add next-generation security features such as application control and deep packet inspection.

Enterprise and Service Provider Challenges

Old Security Threats Never Go Away

Once in the wild, viruses, malware and traditional methods of attacking networks and users never go away. Over the past four years, for example, successful malware strains such as the Koobface virus have built a very large attack base through relentless variation and the ability to exploit and spread across multiple social networking platforms. The Koobface virus has leveraged some of the most popular web-based applications including MySpace, Twitter and Facebook² to steal personal information and credentials from unsuspecting users.

The Koobface virus is not unique in its success or in its ability to exploit known vulnerabilities for an extended period of time. In fact, many exploits enjoy prolonged lives simply because vendors of widely used applications are reluctant to add user protections, such as strong passwords or SSL encryption, for fear of slowing user acquisition and feature development. This has the effect of placing responsibility for security entirely upon the enterprises and service providers whose employees and customers use these popular web-based applications.

Likewise, many enterprises and end users remain susceptible to a myriad of known attacks due to a simple failure to patch known vulnerabilities, outdated equipment and malware signatures, or a failure to properly setup and deploy security devices. Since many of these vulnerabilities have been known for years, they are well documented, and any 'script kiddie' can easily learn to exploit them to attack unpatched systems³. When developing a security strategy, organizations must plan to protect against not just current threats, but all threats, known and unknown.

¹ Gartner, Inc., Defining the Next-generation Firewall, October 2009

² Koobface Worm Variant Circulating on Facebook, SC Magazine December 2008; Koobface Variants Explode, SC Magazine, July 2009; New Koobface Campaign Hits Facebook, SC Magazine, June 2011

³ LulzSec Disbands: The Attacks Live On, Infosec Island, June 2011

Accelerating Evolution of New Threats

Web-based Attacks Increase Data Breach Costs

The Internet's standards-based web interface and incredible number of applications have made it the medium of choice for hackers and thieves looking for new ways to steal information, disrupt services and perform other malicious activities for financial gain. Corrupting computers and networks, and stealing personal data through web-borne viruses, worms and Trojan applications is now commonplace. In fact, web-based attacks were the root cause of 31 percent of data breaches last year, up from 24 percent in 2009 and 12 percent in 2008⁴.

Ever more sophisticated attacks leverage technology and social engineering to trick users into executing malicious payloads that harvest confidential information. The most prevalent threat types include spyware, phishing, instant messaging, peer-to-peer file sharing, streaming media, social media and blended network attacks. The resulting number of data breaches, including identity theft, credit card information theft, fraud, etc. increase every year and cause real damage. In 2010, the average cost of a data breach reached \$214 per compromised record and averaged \$7.2 million per data breach event⁴, an increase of 6% over 2009.

Web 2.0 Applications

In addition to adoption by millions of consumers, many organizations have also recently integrated social media applications including Twitter feeds, Facebook pages, and YouTube videos into their everyday business practices. These Web 2.0 applications enable instantaneous, always-on communications between employees, business partners and even temporary contractors, bringing great leaps in productivity and increasing profits. As might be expected, allowing these consumer-oriented applications with user-generated content into the enterprise raises a myriad of security concerns. Web 2.0 applications can tunnel through trusted ports, use proprietary encryption algorithms and even masquerade as other applications to evade detection and blocking by traditional firewalls. This makes it much easier to transmit content undetected and unimpeded from inside of a 'secure' enterprise network to the outside world and vice versa. Web 2.0 applications also create a green-field opportunity for a new generation of viruses and threats to breach traditional network security firewalls.

Traditional Firewalls No Longer Effective

Stateful firewalls with packet filtering capabilities used to be highly successful at blocking unwanted applications simply because most applications communicated over networks by using specific and unchanging computer ports and protocols. Should an administrator decide that an application was unsafe, they could quickly prevent users from accessing it by modifying the firewall policy to block the associated ports and protocols. However, traditional port-based protection is no longer practical. For example, blocking port-80 would block access to the web entirely, and this is simply not an option for most enterprises today. Some traditional network security technologies are shown below in Fig. 1.

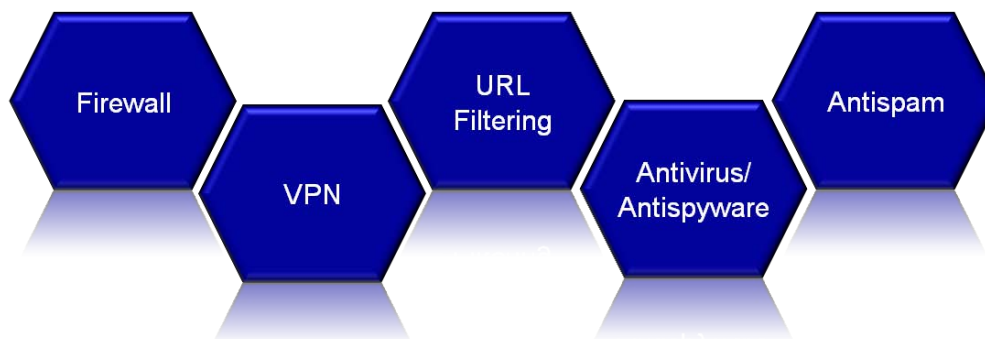


Figure 1: Traditional Network Security Technologies are Necessary but Incomplete

⁴ 2010 Annual Study: Global Cost of a Data Breach, Ponemon Institute, LLC

Migration to Next-Generation Networks

As enterprises and service providers realize that their existing networks are not adequate to support their long-term and sometimes even short-term growth plans, they are rapidly migrating to faster, more flexible network architectures. These next-generation networks are being tasked with demanding chores; from providing large branch offices with secure access to critical information, to powering virtualized data centers and low-latency cloud-based applications, to delivering reliable high-quality business and security services to multiple globally dispersed customers.

Next-generation networks must be flexible enough to simultaneously support high volumes of IPv4 and IPv6 traffic as well as rich media protocols without slowing down, and most importantly, they must provide a competitive advantage for those businesses that deploy them. In order to maintain high throughput and reliability, these complex networks must have security devices that won't become chokepoints as they inspect and filter traffic for threats and malware. In order to protect next-generation networks against both known and new threats, these security devices must be based on field-proven, highly-scalable, and easy-to-manage platforms.

The Next Step in Security Evolution: Next-Generation Security Platforms

Next-generation networks require the complete protection that many so-called NGFWs cannot provide. As enterprises and service providers migrate to more complex multi-protocol network architectures with higher data rates and traffic volumes, they require highly flexible security platforms that can evolve and scale. NGFWs that do not offer both traditional and advanced threat protection cannot protect these high-performance environments. Instead, organizations need next-generation security platforms and related devices that are flexible enough to provide protection against both known and unknown threats, while scaling to accommodate business growth and new services. A field-proven, scalable platform of core security technologies, as well as next-generation security capabilities are required to protect enterprise and service provider networks now, and into the future.

FortiGate® consolidated security appliances from Fortinet are field-proven, purpose-built security platforms that include rock-solid core security technologies, as well as protections against next-generation threats and malware. Since Fortinet develops all security technologies in-house, instead of licensing crucial security features from third-parties, all FortiGate platforms include finely tuned, hardware-accelerated protections that are able to quickly integrate new security technologies and scale effortlessly with any size of fast-growing business and any network environment.

Next-Generation Security Technologies

Businesses are realizing that traditional security solutions such as firewalls, intrusion detection systems and host-based antivirus are no longer adequate to protect against new, sophisticated attacks. The potential for data loss and damage to corporate networks increases every year as criminals find new ways to penetrate defenses. In addition, as government regulations and legal requirements such as PCI DSS, HIPAA and the HITECH Act begin to hold company executives accountable for their employee's actions, corporate executives and IT professionals alike are becoming more concerned about what their employees are viewing and downloading from the Internet. FortiGate security platforms include a wealth of proven next-generation security technologies to protect against the latest threats. Some next-generation network security technologies are shown below in Fig. 2.

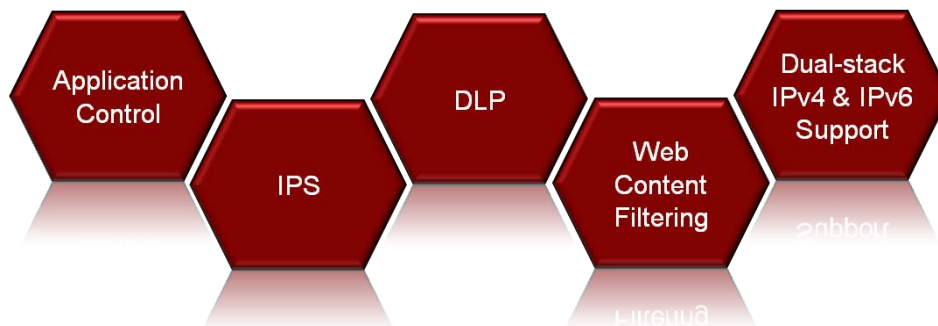


Figure 2: Next-Generation Network Security Technologies

Application Control

A primary requirement and driver for adoption of next-generation firewalls is application control. In order to prevent data loss and mitigate new threats, organizations must be able to effectively control legacy applications as well as the new breed of Internet-based applications. Next-generation application control must be able to detect, monitor, and control the usage of applications and any associated traffic flows at gateways and at endpoints, regardless of ports and protocols used. In addition, an association must be made between the application and the end user before the proper access rights and security policy can be assigned.

Using Fortinet Application Control, businesses can detect and restrict the use of applications on their networks and endpoints based on application classification, behavioral analysis, and end user association. Network administrators can define and enforce policies for thousands of applications running on next-generation networks and endpoints. They can detect and control Web 2.0 applications such as Facebook, Skype, Twitter and Salesforce.com at a granular level, regardless of ports and protocols used.

Application control lists

Administrators can control applications explicitly by entering them into an application control list in the firewall policy. In addition, they can create multiple application control lists, each configured to allow, block, monitor or shape network traffic associated with a unique list of applications. An application control ‘whitelist’ is appropriate for use in a high security network, as it allows only traffic from listed applications to pass through the gateway. An application control ‘blacklist’ on the other hand, blocks only listed applications. Default application control lists are provided with Fortinet application control to allow fast configuration. Fortinet application control lists are easily accessed and modified through the FortiGate ‘single pane of glass’ management console, shown below in Fig. 3.

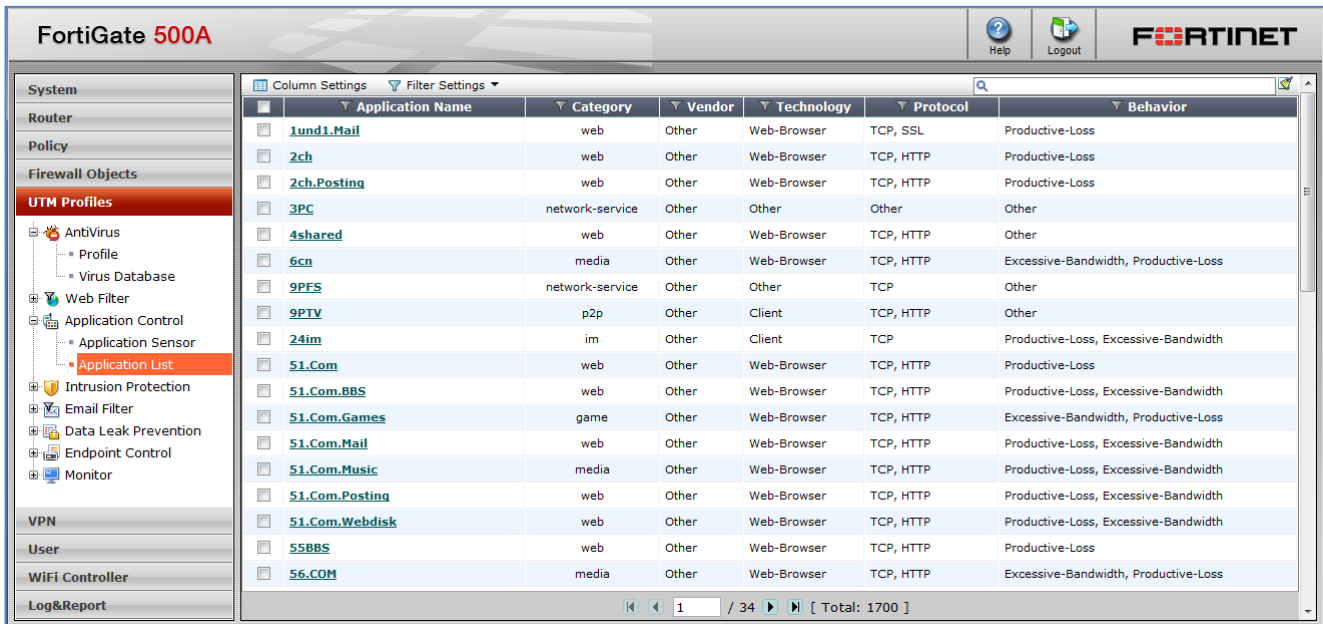


Figure 3: FortiGate Application Control List

Detecting encrypted application traffic

Fortinet Application Control also inspects encrypted application traffic. Protocol decoders normalize and discover traffic from applications attempting to evade detection via obfuscation techniques, such as using non-standard ports and protocols. Following identification and decryption, application traffic is either blocked, or allowed and scanned for malicious payloads. In addition, application control protocol decoders detect and decrypt tunnelled IPsec VPN and SSL VPN traffic prior to inspection, ensuring total network visibility. Application control even decrypts and inspects traffic using encrypted communications protocols, such as HTTPS, POP3S, SMTPS and IMAPS.

FortiGuard® application control database

Once it decodes network traffic, the FortiGate next-generation security platform can identify applications by their unique signatures. Fortinet Application Control leverages one of the largest application signature databases available – the FortiGuard Application Control Database. This enables FortiGate appliances to detect more than 1,600 unique web-based applications, software programs, network services and network traffic protocols, as well as unknown applications from unknown sources. The FortiGuard Application Control Database is continually refreshed with signatures for new applications, as well as new versions of existing applications.

Associating the end user with applications

When a user attempts to access network resources, the FortiGate appliance will identify the user from a list of names, IP addresses and Active Directory group memberships that it maintains locally. The connection request will be allowed only if the user belongs to one of the permitted user groups, and the assigned firewall policy will be applied to all traffic to and from that user.

Application control granularity

Fortinet Application Control can also distinguish between multiple applications available from a single social networking site. For example, it can identify and apply policies individually to application traffic from Facebook Chat and Facebook Video. In addition, traffic shaping can be enabled to restrict network bandwidth available to some applications while giving priority to others.

Application traffic shaping

Application traffic shaping allows administrators to limit or guarantee the network bandwidth available to all applications or individual applications specified in an application list entry. Traffic shaping can also be configured on a time-sensitive basis to restrict user access or bandwidth available to applications during certain times of the day.

Application monitoring and reporting

The application monitoring and reporting feature collects application traffic information and displays it using visual trend charts. This provides administrators with a quick way to gain insight into application usage on their network. Administrators can select from several different types of charts to display data graphically. Default trend charts are available for quick analysis.

Application control packet logging

Fortinet Application Control packet logging saves network packets generated by applications for additional analysis, such as forensic investigation or identification of false positives. FortiGate consolidated security appliances can store the packets or forward them on to a FortiAnalyzer unit or even to the FortiGuard Analysis and Management Service.

Application control at the endpoint

Application control lists can also be applied simultaneously to endpoint security profiles. In addition, application use at endpoints can be controlled with a personal firewall. Fortinet endpoint application control is easily enabled and configured through the FortiGate management interface as shown below in Fig. 4.

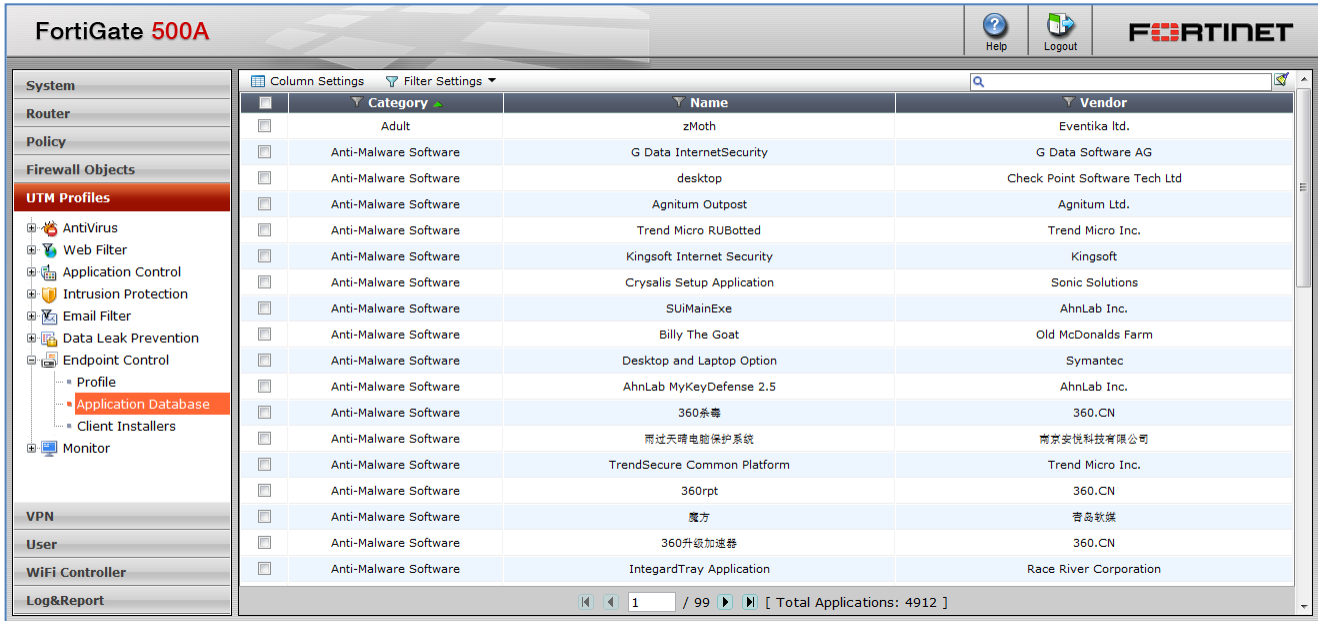


Figure 4: FortiGate Application Control at the Endpoint

Integrated Intrusion Prevention System (IPS)

Deploying updates and patches in large, complex next-generation networks is a complex and time-consuming process. Following a patch release, it can take a large enterprise weeks or even months to deploy the fix to all affected systems. Fortinet IPS protects networks from both known and zero-day vulnerabilities, blocking attacks that take advantage of unpatched systems.

Fortinet IPS offers a wide range of features that can be used to monitor and block malicious network activity including; predefined and custom signatures, protocol decoders, out-of-band mode (or one-arm IPS mode), packet logging, and IPS sensors. IPS sensors provide a convenient, centralized location to configure and deploy an arsenal of IPS tools. You can install Fortinet intrusion prevention technology, available in all FortiGate and FortiWiFi™ platforms, at the edge of your network or within the network core to protect critical business applications from both external and internal attacks.

IPS sensors

IPS sensors may be configured to apply specific inspection signatures to selected traffic. Actions can be assigned to block, pass, or reset any suspicious traffic. IPS sensors may also be used to enable packet logging for each signature, or to pass traffic from certain IP addresses without further inspection. On the flip side, IPS sensors can prevent attacks from spreading by quarantining all traffic originating from an attack source, sent to an attack destination, or received by the FortiGate device.

IPS sensors are populated with filters and custom signature entries. Attributes can be set to classify traffic by severity, target (client/server), OS, protocol, application, and tags. Specifying more or fewer attributes widens or narrows the focus of the sensor. Custom signature entries can be created to include or exclude signatures on an individual basis. Custom signatures can also specify actions such as logging, packet logging and filtering, attacker quarantine, and exempt IP address settings. Custom FortiASIC Security Processor (SP) chips, built into certain FortiGate appliances and modules, accelerate IPS functions by offloading intensive tasks such as IPS signature scanning. Fortinet IPS sensors can be accessed through the FortiGate management interface as shown below in Fig. 5.

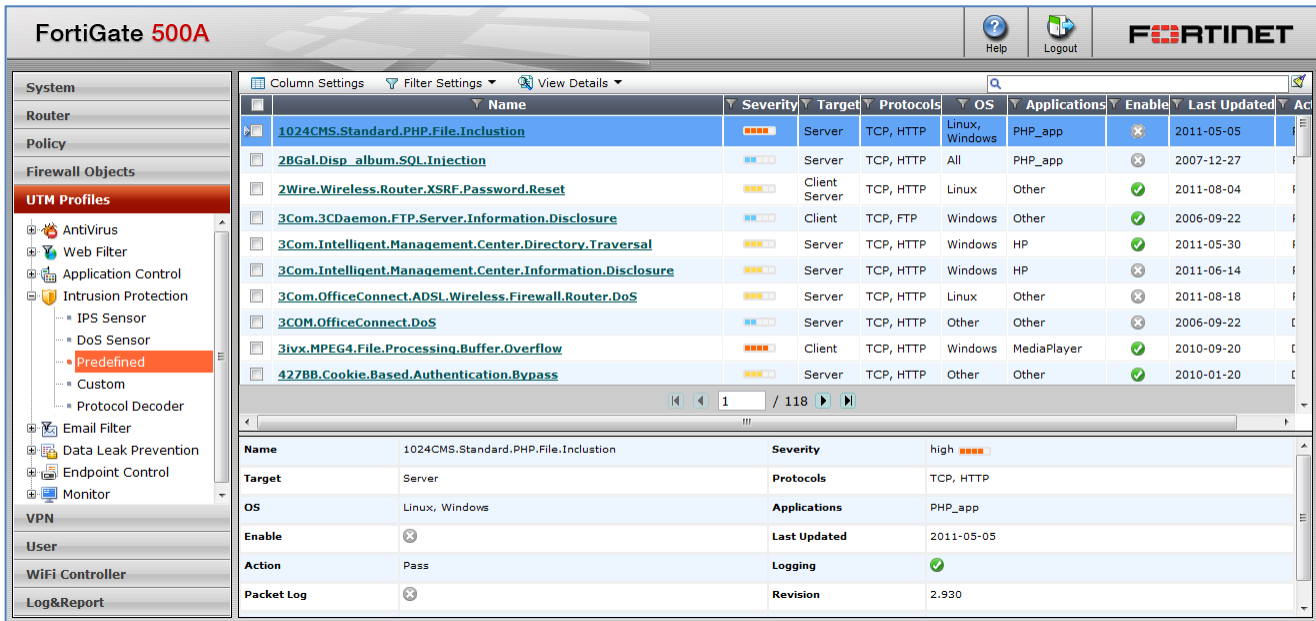


Figure 5: FortGate IPS Sensor Configuration

Predefined IPS signatures

Predefined IPS signatures are provided through the global FortiGuard Distribution Network, and can be used by FortiGate systems to detect more than 4,000 different attack signatures – from attacks against unpatched operating system vulnerabilities to invalid checksums contained in UDP packets.

Custom IPS signatures

Organizations can also create custom IPS signatures to extend protection beyond predefined signatures. For example, custom IPS signatures can be used to protect unusual or specialized applications, or even custom platforms from known and unknown attacks. In addition, custom IPS signatures can be used for specialized network traffic analysis and pattern matching. For example, if a network is experiencing unusual or unwanted traffic, a system administrator can create a custom IPS signature to monitor and understand traffic patterns.

Protocol decoders

Protocol decoders identify abnormal traffic patterns, such as those that do not meet established protocol requirements and standards. For example, the HTTP decoder monitors network traffic to identify any HTTP packets that do not meet the HTTP protocol standard. Many Fortinet protocol decoders are able to recognize traffic by type, rather than port, eliminating the need to specify individual ports.

Packet logging and attacker quarantine

IPS packet logging can be enabled to save packets matched by one or more IPS signatures. The packets are saved as log messages and the packet contents can be viewed and analyzed using log message analysis tools. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.

IPS also provides a way to quarantine attackers and display them on a 'banned user list'. Attackers can be quarantined according to their IP address, their IP address plus the victim's IP address, or by incoming interface used. Attackers can be banned from accessing the network for hours, days, or forever.

IPS out-of-band mode

Fortinet IPS can also be deployed in out-of-band mode. This allows Fortinet IPS to operate as an intrusion detection system (IDS), detecting and reporting attacks, but not taking any actions. Out-of-band sniffer mode is useful for network diagnostics.

FortiGuard Services

Backed by automatic, real-time updates delivered by FortiGuard Services, FortiGate IPS technology leverages a database of thousands of unique attack signatures to stop attacks that might evade conventional firewall defenses, plus anomaly-based detection that enables the system to recognize threats for which no signature has yet been developed. The combination of known and unknown threat prevention, plus tight integration with other Fortinet security technologies, enables FortiGate systems to stop attacks regardless of whether your network is wired or wireless, a partner extranet, or connected to a branch office.

Data Loss Prevention (DLP)

Trusted employees frequently send sensitive data into untrusted zones, either intentionally or by accident. Fortinet DLP uses sophisticated pattern matching techniques and user identity to detect and prevent unauthorized communication of sensitive information and files through the network perimeter. DLP features include fingerprinting of document files and document file sources, multiple inspection modes (proxy and flow-based), enhanced pattern matching, and data archiving.

Numerous communication protocols - including HTTP, HTTPS, FTP, FTPS, email (POP3, POP3S, IMAP, IMAPS, SMTP, and SMTPS), NNTP and instant messaging (AIM, ICQ, MSN, and Yahoo!) – can be monitored for sensitive data. Fortinet DLP can search content based on text strings as well as enhanced pattern matching that includes wild cards and Perl regular expressions. For example, pattern matching can be used to scan network traffic for sensitive personal information such as social security and credit cards numbers.

When a match is found, sensitive content can be blocked, passed or archived, with potential leak notifications generated. DLP can be used to block sensitive information coming into the network or going out. For example, by blocking content often found in spam email messages, DLP can enhance incoming data protection measures.

DLP sensors

FortiGate DLP sensors provide a central location to configure and store desired DLP features, and can be used to specify parameters such as document file fingerprints, document file sources, inspection modes, enhanced pattern matching, and archiving preferences. DLP sensors can contain multiple DLP filters, and each of these filters can point to a configured DLP feature, such as fingerprinting. Fortinet DLP sensors are easily configured through the FortiGate management interface as shown below in Fig. 6.

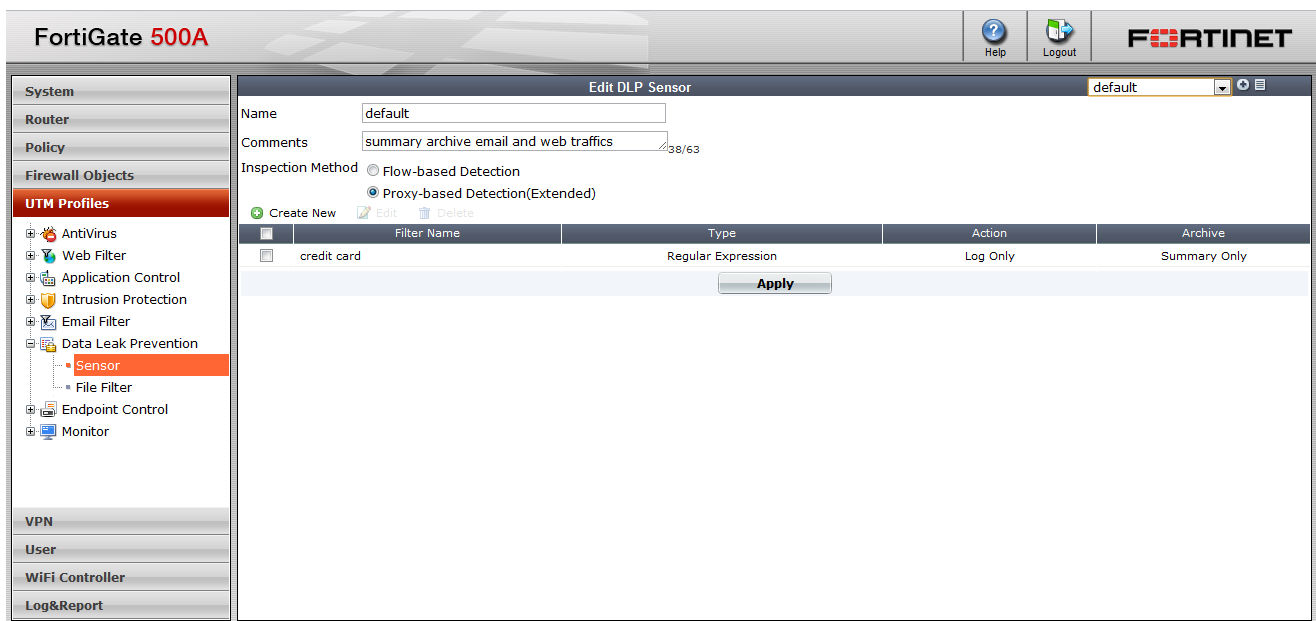


Figure 6: FortiGate DLP Sensor Configuration

Document fingerprinting

Document fingerprinting allows Fortinet DLP to create a checksum fingerprint and store it, enabling it to identify and block transfer of, for example, specific sensitive documents or files stored on a server or database. It can even find documents that are stored inside archive files.

Proxy-based vs. flow-based DLP inspection

Fortinet DLP can operate in either proxy-based or flow-based inspection mode. Both modes have their pros and cons. Proxy-based provides the highest level of analysis by examining content in detail. However, it can also place a high demand on system resources. Flow-based inspection is faster and uses less system resources because it inspects the session in chunks, however results may not be as accurate or reliable as proxy-based inspection.

DLP content archiving

Fortinet DLP content archiving can be enabled to store a record all content, or selected content that passes through a FortiGate unit. DLP sensors can be created to archive sensitive content or content delivered using certain protocols, and content can be archived to a FortiGate or FortiAnalyzer appliance. Archiving DLP content is useful when auditing is required by law, or for simply keeping track of network usage. Full DLP content archiving also saves web pages, email messages, and files in their entirety.

Web Content Filtering

The Fortinet web content filtering solution begins with traditional URL blocking lists, but goes further by expanding these methods and allowing their use in combination with other Fortinet security functions resident on all FortiGate consolidated security appliances. Fortinet's web content filtering technology enables a wide variety of actions to inspect, rate, and control perimeter web traffic at a granular level. Using Fortinet web content filtering technology, FortiGate appliances can classify and filter web traffic using multiple pre-defined and custom categories.

To accelerate web traffic and content inspection, all FortiGate devices support Web Cache Communication Protocol (WCCP) which allows the FortiGate to operate as a router or cache engine. Acting as a router, the FortiGate intercepts web browsing requests from client web browsers and forwards them to the cache engine. The cache engine then returns web content to the client as required. When operating as a WCCP cache server, the FortiGate can communicate with other WCCP routers to cache web content, returning requested content to client web browsers as needed. Fortinet web content filtering is easily accessible through the FortiGate management interface as shown below in Fig. 7.

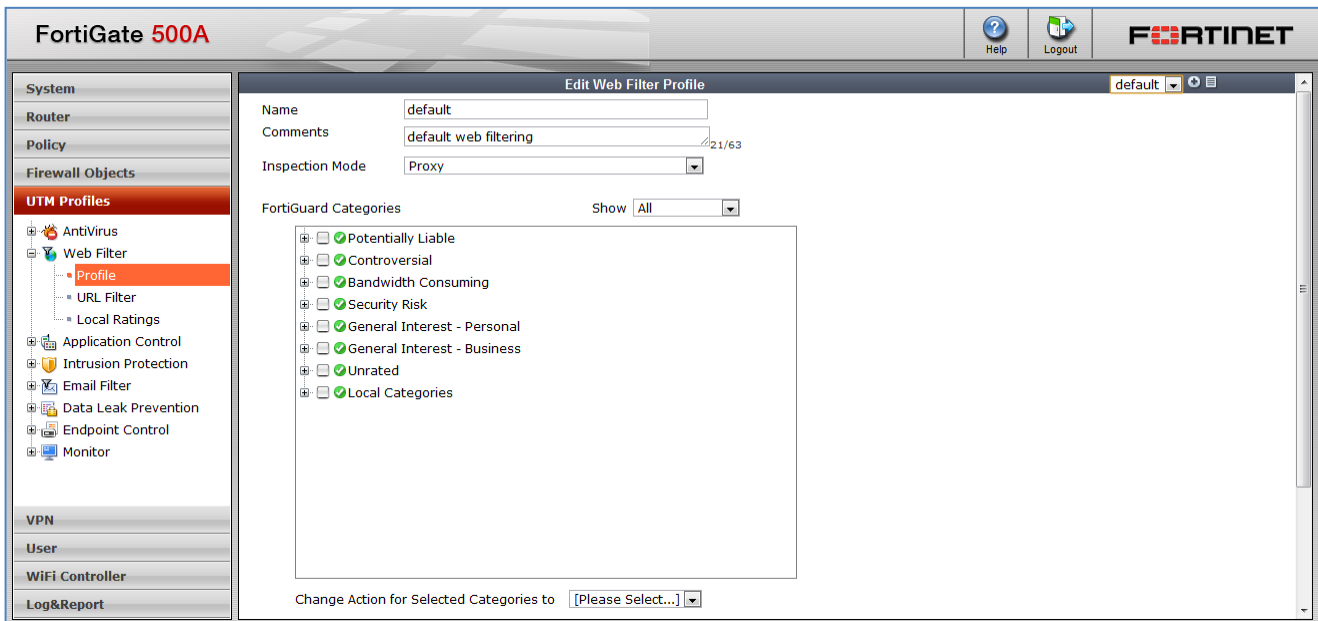


Figure 7: FortiGate Web Content Filtering Interface

Dual-stack IPv4 and IPv6 Support

With the recent exhaustion of the IPv4 address space, many organizations are migrating towards IPv6, the next generation Internet communication protocol. IPv6 drastically changes the supply of IP addresses from 4 billion IPv4 addresses to 340 trillion-trillion-trillion IPv6 addresses (2¹²⁸ addresses). IPv6 also promises enhancements over IPv4 including better security, improved addressing, routing efficiency, and quality of service. The architecture of IPv6 includes a number of features and benefits that will address the future needs for global end-to-end communication.

As more content and service providers begin to transition to IPv6, it's essential that organizations deploy network security devices that can deliver the same level of protection for IPv6 content as IPv4. There are mechanisms in place to enable communication between IPv6-only devices and networks with IPv4-only devices and networks. The two most common are dual-stack and tunnelling. Dual-stack is preferable because it allows the security device to process each packet in either IPv4 or IPv6. Tunnelling, on the other hand, wraps an IPv6 packet in an IPv4 header, allowing a device to forward a packet but not inspect it. This limited IPv6 support means that it will not be able to inspect the contents for malicious code or unwanted content, allowing unwanted traffic to traverse the network.

FortiGate consolidated security appliances support a dual stack architecture that recognizes and separately routes both IPv4 and IPv6 traffic, providing the same core network security technologies simultaneously for both Internet protocols. Vital network and content protection security features, including routing, are fully supported. Fortinet adopted early support of IPv6, receiving IPv6-Ready and JITC certifications in 2008, both important to global telecommunications carriers. Fortinet also earned the USGv6 certification in 2011, important to the US government and the businesses serving them.

Integrated Wireless Controller

All FortiGate appliances include an integrated wireless controller, consolidating security policies and management of all wired and wireless network traffic into a single pane of glass. The integrated wireless controller provides unmatched visibility and control of both thick FortiWiFi and thin FortiAP™ wireless access points. The same comprehensive threat protection provided for wired networks, including firewall, VPN, intrusion prevention, application control, web filtering, traffic shaping and many other security capabilities, are extended to wireless networks.

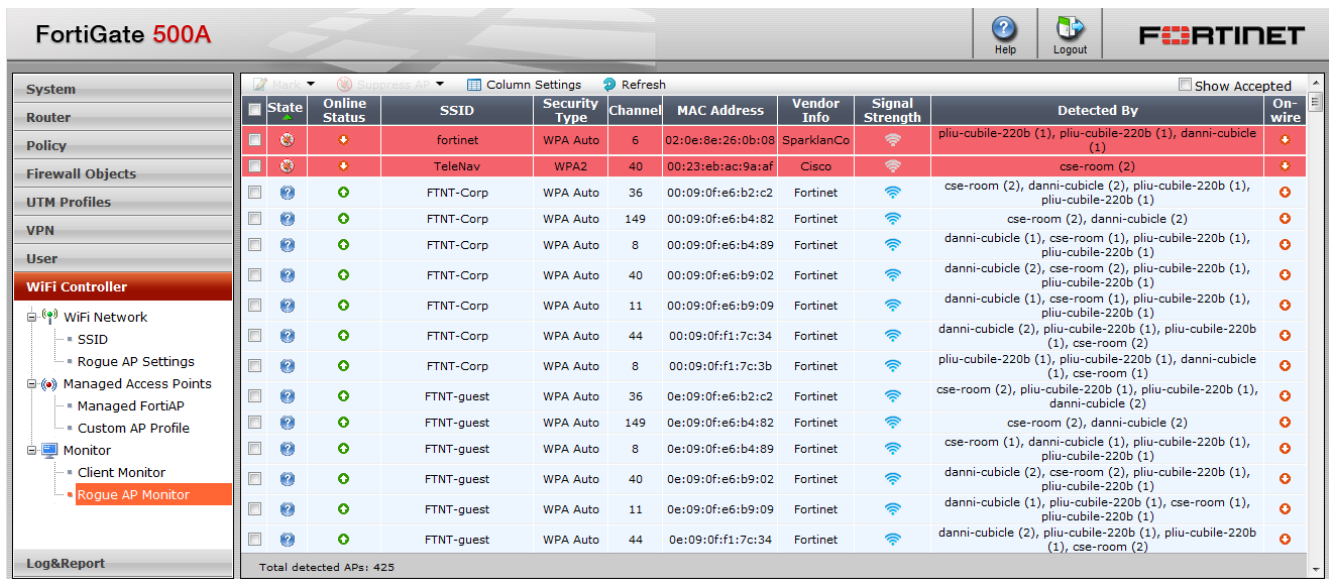


Figure 8: FortiGate Wireless Controller provides Single Pane of Glass Management for both Wired and Wireless Traffic

Centralized Management

For large installations, FortiManager™ appliances provide centralized policy-based provisioning, configuration, and update management for FortiGate, FortiWiFi, and FortiMail™ appliances as well as FortiClient™ endpoint security agents. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize web filtering rating request response times and maximize network protection. FortiManager provides a single pane of glass interface to manage and configure all Fortinet appliances as shown below in Fig. 8.

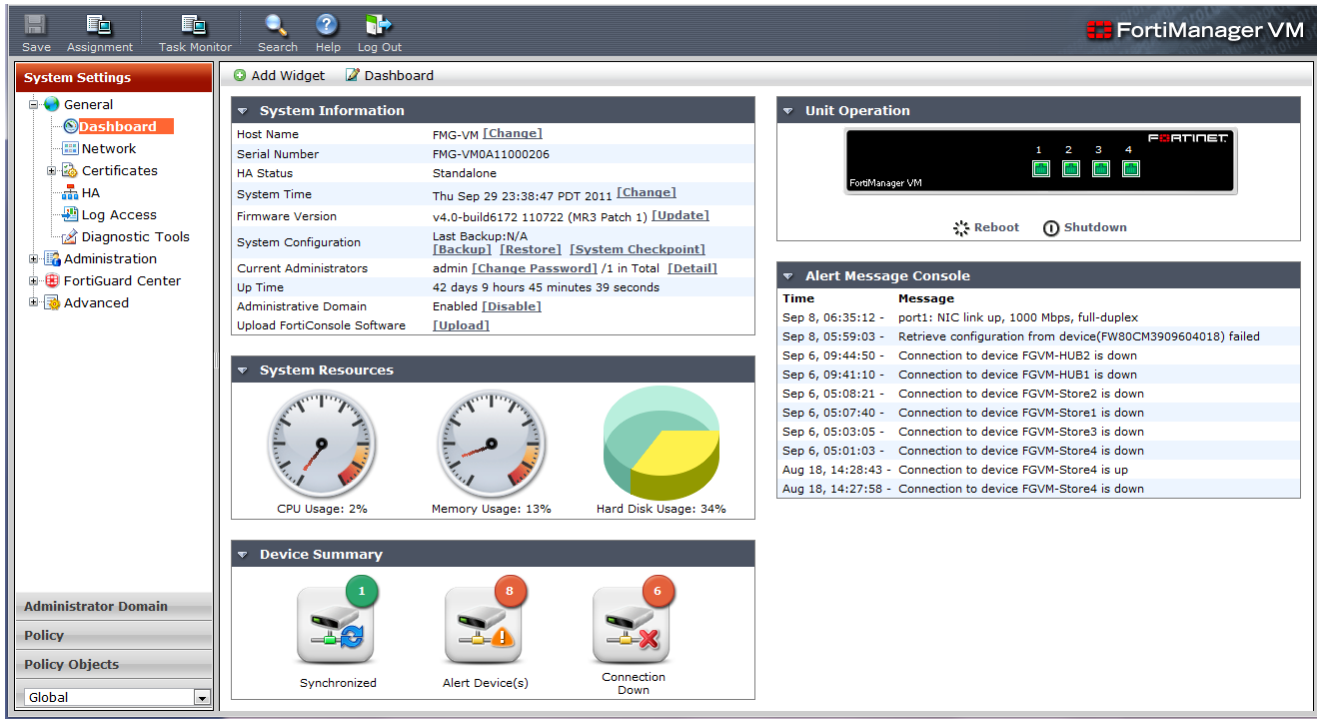


Figure 9: FortiManager Central Management Interface

For additional analysis and reporting capabilities, FortiAnalyzer appliances securely aggregate log data from Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customized reports, users can filter and review log records for traffic, event, virus, attack, web content and email data. Information can be mined to determine a user’s security stance and assure regulatory compliance. FortiAnalyzer also provides advanced security management functions such as quarantined file archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, web access, instant messaging and file transfer content.

Core Security Technologies

Firewall - Stateful Traffic Inspection and Packet Filtering

One of the most fundamental protections for enterprise and service provider networks of any size is a stateful firewall with packet filtering capabilities, which can selectively allow or block outsiders from accessing private data resources. A firewall, working closely with other networking infrastructure, examines each network packet to determine whether or not to forward it toward its destination according to policy.

Fortinet firewall technology combines FortiASIC™-accelerated stateful inspection with an arsenal of integrated application security engines to quickly identify and block complex threats. Fortinet Firewall technology, implemented in FortiGate consolidated security appliances, fully integrates with other Fortinet security technologies to enable extensive protection

profiles for in-depth defense. Built-in virtual security domains and security zones enable network segmentation by customer, business unit, or any other physical or logical division for increased policy granularity and multi-layered security.

FortiGate platforms support multiple operational modes, including transparent, static NAT, and dynamic NAT, to support existing infrastructure for deployment flexibility. In addition, FortiClient end-point security agents integrate with Fortinet firewall technologies, extending protection to remote desktop computers, mobile laptops, and Smartphones operating outside of the network perimeter.

Virtual Private Network (VPN)

With the number of threats accelerating, secure communications between enterprise networks, businesses and partners, and corporations and mobile workers is now more important than ever. Data breaches, information leaks, and infected networks and systems are costing corporations and government agencies billions of dollars every year.

Fortinet VPN technology allows organizations to establish secure communications and data privacy between multiple networks and hosts using IPsec and secure sockets layer (SSL) VPN protocols. Both VPN services leverage custom FortiASIC™ Network Processors to accelerate encryption and decryption of network traffic. Once the traffic has been decrypted, multiple threat inspections - including antivirus, intrusion prevention, application control, email filtering and web filtering - can be applied and enforced for all content traversing the VPN tunnel.

IPsec VPN tunnelling is typically performed at Layer 3, or lower, of the OSI network model. To enable remote access, the FortiGate establishes encrypted network connectivity between a remote node and the internal network. SSL VPN configurations are easier to setup and deploy as they communicate at the highest levels in the OSI model, independent of the underlying network architecture. Fig. 9 below shows the FortiGate SSL VPN configuration interface with simple setup options. Since the SSL protocol is already built into most web browsers as HTTPS, no additional endpoint configuration is typically required. Conveniently, both SSL and IPsec VPN tunnels may operate simultaneously on the same FortiGate device.

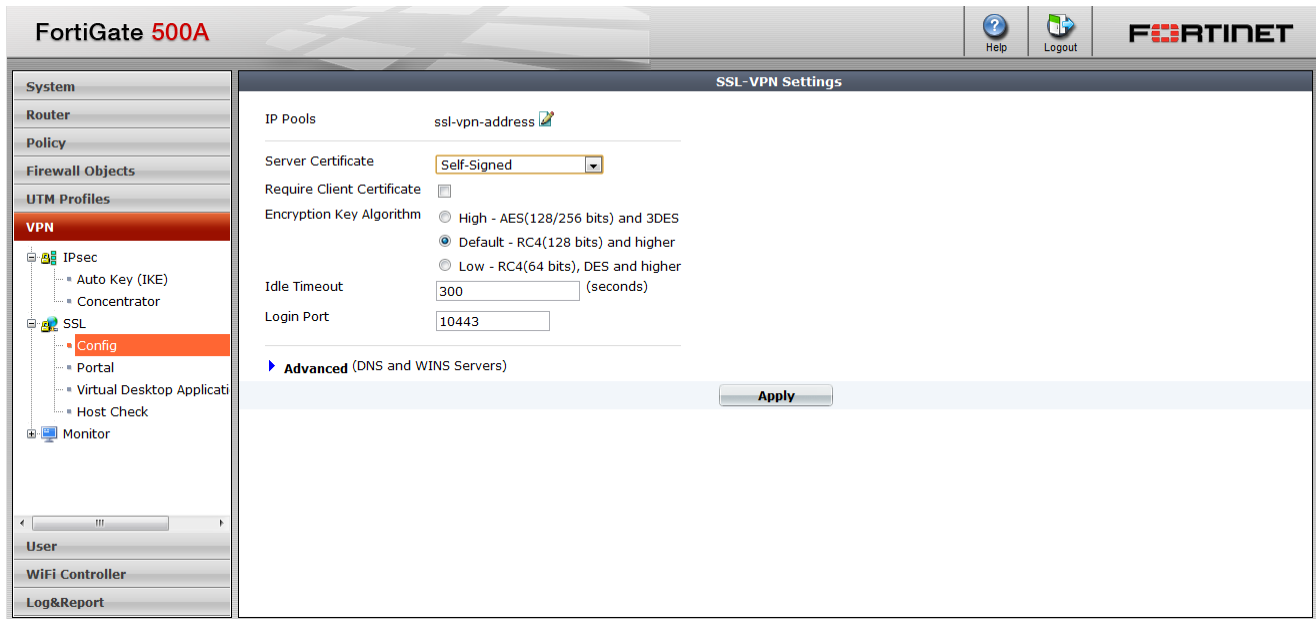


Figure 10: FortiGate SSL VPN Configuration

Fortinet IPsec and SSL VPN technologies in FortiGate platforms are tightly integrated with other security features such as firewall, antivirus, web filtering, and intrusion prevention, providing more comprehensive protection than VPN-only security appliances. FortiGate VPN solutions scale to meet the performance requirements of organizations of any size, from SOHO/ROBO and small businesses to large enterprises and service providers. FortiManager centralized management

appliances provide the ability to manage complex VPN deployments involving thousands of FortiGate systems from a single console.

URL Filtering

URL filtering is typically deployed to prevent users from visiting dangerous or inappropriate web sites. Fortinet URL filtering also gives administrators the option to explicitly allow web sites, or to pass web traffic uninspected both to and from known-good web sites in order to accelerate traffic flows. Real-time updates can be received from FortiGuard Services to determine the category and rating of a specific URL. Web sites or URLs can be easily added to the local URL filtering list using both text and regular expressions. URL filtering lists can be modified through the FortiGate management interface as shown in Fig. 10. One of the four following actions can then be assigned as needed to each URL pattern in the URL filtering list.

- **Block**
Prevents users from accessing potentially dangerous or inappropriate web sites and delivers a warning message to the user when access is denied.
- **Allow**
Specifically allows users to access a certain web site. Web site traffic is passed on to additional Fortinet security functions for inspection as needed.
- **Pass**
Specifically allows users to access a certain web site. Web site traffic is allowed to bypass additional Fortinet security functions. This option should be used only for web sites that are fully trusted.
- **Exempt**
Specifically allows users to access a certain web site. Web site traffic is allowed to bypass additional Fortinet security functions. However, the connection inherits the exemption, meaning that all subsequent reuse of the existing connection will also bypass additional Fortinet security functions. The exemption is cancelled when the connection times out.

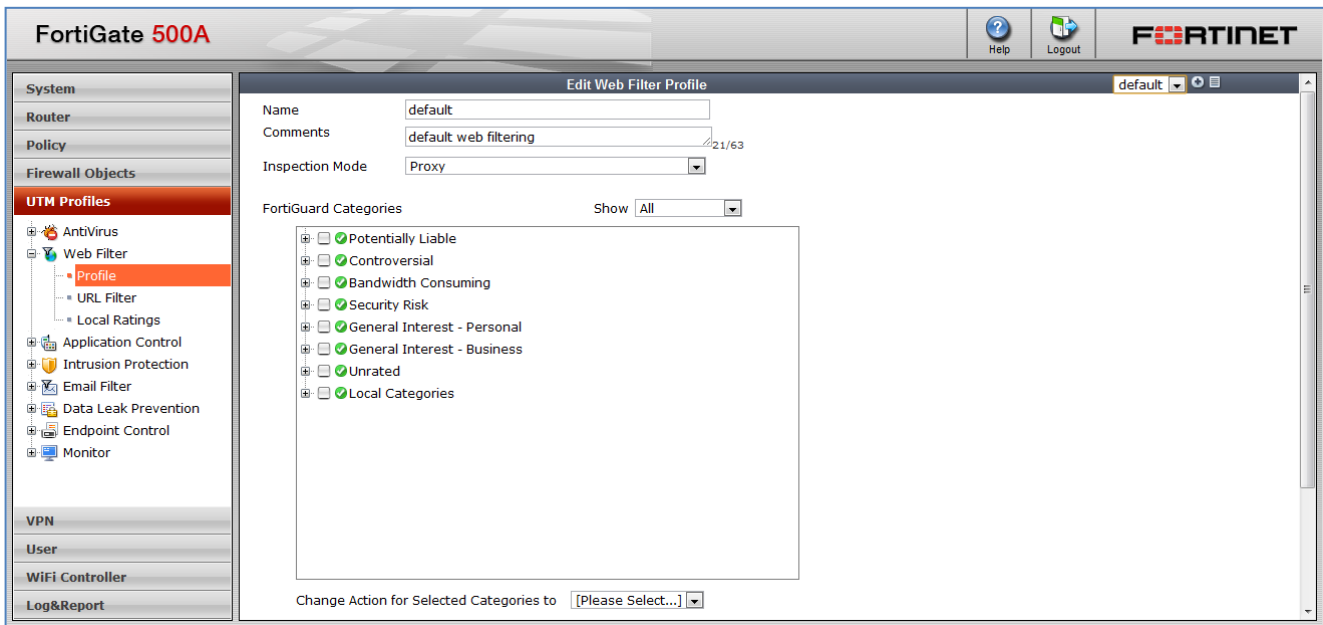


Figure 11: FortiGate URL Filtering Interface

Antivirus/ Antispyware

Malware infections in networks, servers and endpoint devices cost enterprises, service providers and government agencies billions of dollars every year. Fortinet antivirus technology combines advanced signature and heuristic detection engines to provide multi-layered, real-time protection against both new and evolving virus, spyware, and other types of malware attacks in web, email, and file transfer traffic. FortiASIC Content Processors, integrated into FortiGate and FortiWifi products, accelerate both signature scanning and heuristics/anomaly detection for protection against viruses, while delivering performance that scales from entry-level appliances to multi-gigabit core network or data center platforms.

In addition to three proxy-based antivirus databases, FortiGate appliances include a high-performance flow-based antivirus option. The flow-based option allows you to scan files of any size while maintaining the highest levels of performance. In addition, flow-based inspection enables scanning of files within compressed files to detect hidden threats. By providing you the flexibility to choose your antivirus engine, you can balance your performance and security requirements for your environment.

Encryption/decryption capabilities for all common tunnelling protocols including PPTP, L2TP, IPsec, SSL and on-demand host integrity checking enable inspection of encrypted content, such as traffic sent over VPN connections. In addition, Fortinet antivirus supports content inspection within SMTP, POP3, IMAP, FTP, HTTP, IM and P2P protocols, and all major compressed file formats as shown below in Fig. 11. For scanning of endpoint devices, FortiClient end-point security agents extend antivirus protection to remote desktop computers, mobile laptops, and Smartphones that may operate outside of the network perimeter.

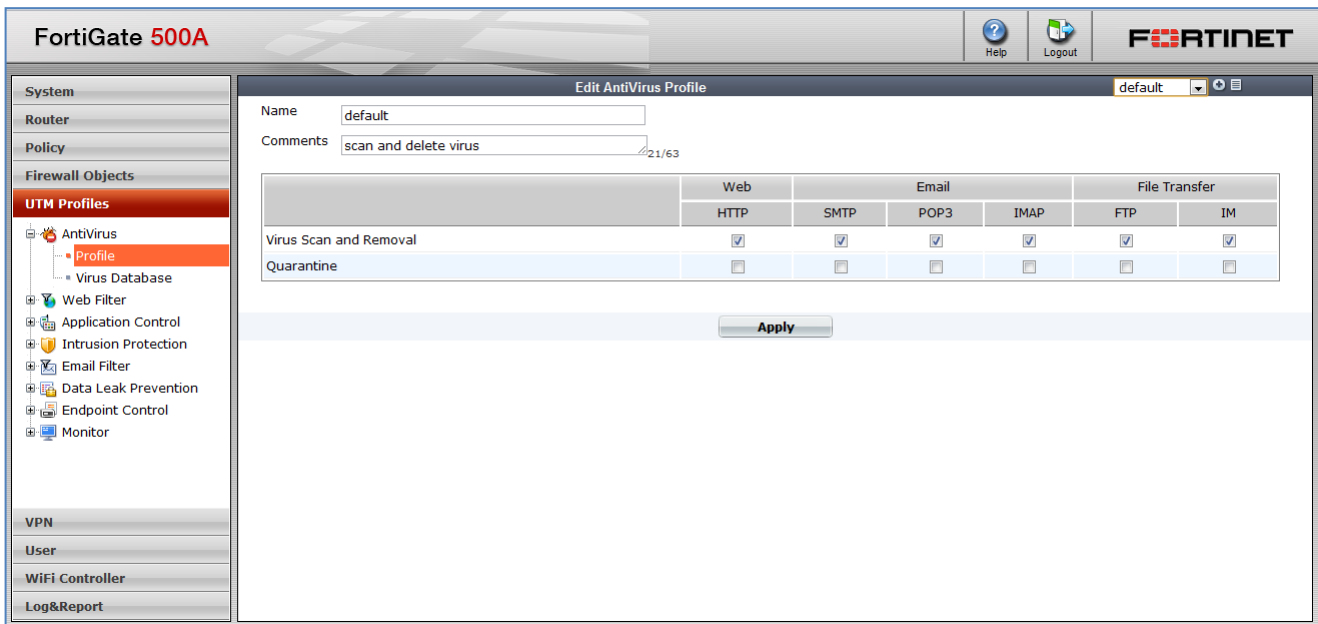


Figure 12: FortiGate Antivirus Configuration

Fortinet antivirus also gets regular updates from FortiGuard Subscription Services. The FortiGuard Labs threat research team and global distributed network provides industry-leading antivirus signature updates for comprehensive protection against all types of content-level threats.

Antispam

Unsolicited email in the form of spam costs corporations and government agencies billions of dollars every year. Employees spend time sorting and deleting spam from their regular email while servers and networks have to contend with the extra traffic generated. In addition, spam emails are the most common means with which bots propagate, and often contain malware and links to inappropriate sites.

Fortinet applies a comprehensive, multi-layered approach to guard against spam. Global spam filtering is provided through the FortiGuard Antispam service which has access to the Fortinet Global Threat Intelligence database. The FortiGuard team collects and analyzes a constant flow of sender IP reputation and spam signatures from the large installed base of FortiGate, FortiClient and FortiMail platforms. This global database is constantly updated, enabling FortiGate, FortiClient and FortiMail appliances to detect and filter most prevailing spam. In addition, customized spam filters can be created to filter email for banned words, blocked and allowed email sender addresses, heuristic rules, and highly sophisticated techniques such as Bayesian training in FortiMail.

A large amount of spam is sent everyday by improperly configured or virus-infected host email servers. FortiGuard Antispam Service maintains a global IP reputation database where the reputation of each IP address is updated based on information gathered from multiple sources. IP address reputation properties can include 'whois' information, geographical location, service provider, host server information, and more. In addition, by comparing each sender's historical email volume with their current email volume, FortiGuard Antispam Service updates the reputation of each IP address in real-time, providing a highly effective sender IP address filter.

Conclusion

Costs and lost business associated with data breaches and lawsuits continue to increase every year. This is proof that as long as valuable information exists, criminals will attempt to steal it using a wealth of traditional, as well as ever more sophisticated attacks. To stay ahead of new threats, enterprises need a security platform that can provide protection against both known and new threats, while scaling to accommodate business growth and new services. A field-proven, scalable platform including both core security technologies and next-generation security capabilities is required.

FortiGate consolidated security appliances from Fortinet are field-proven, purpose-built security platforms that includes rock-solid traditional security technologies, as well as protections against next-generation threats and malware. Since Fortinet develops all security technologies in-house, instead of licensing crucial security features from third-parties, all FortiGate platforms include finely tuned, hardware-accelerated protections that are able to quickly integrate new security technologies and scale effortlessly with any size of fast-growing business and any network environment. Fortinet also provides in-depth monitoring and reporting capabilities to alert administrators and users to threats, and to allow further analysis for fine tuning. When combined with FortiGuard Services, FortiGate consolidated security appliances protect your next-generation network and your business against threats now and into the future.

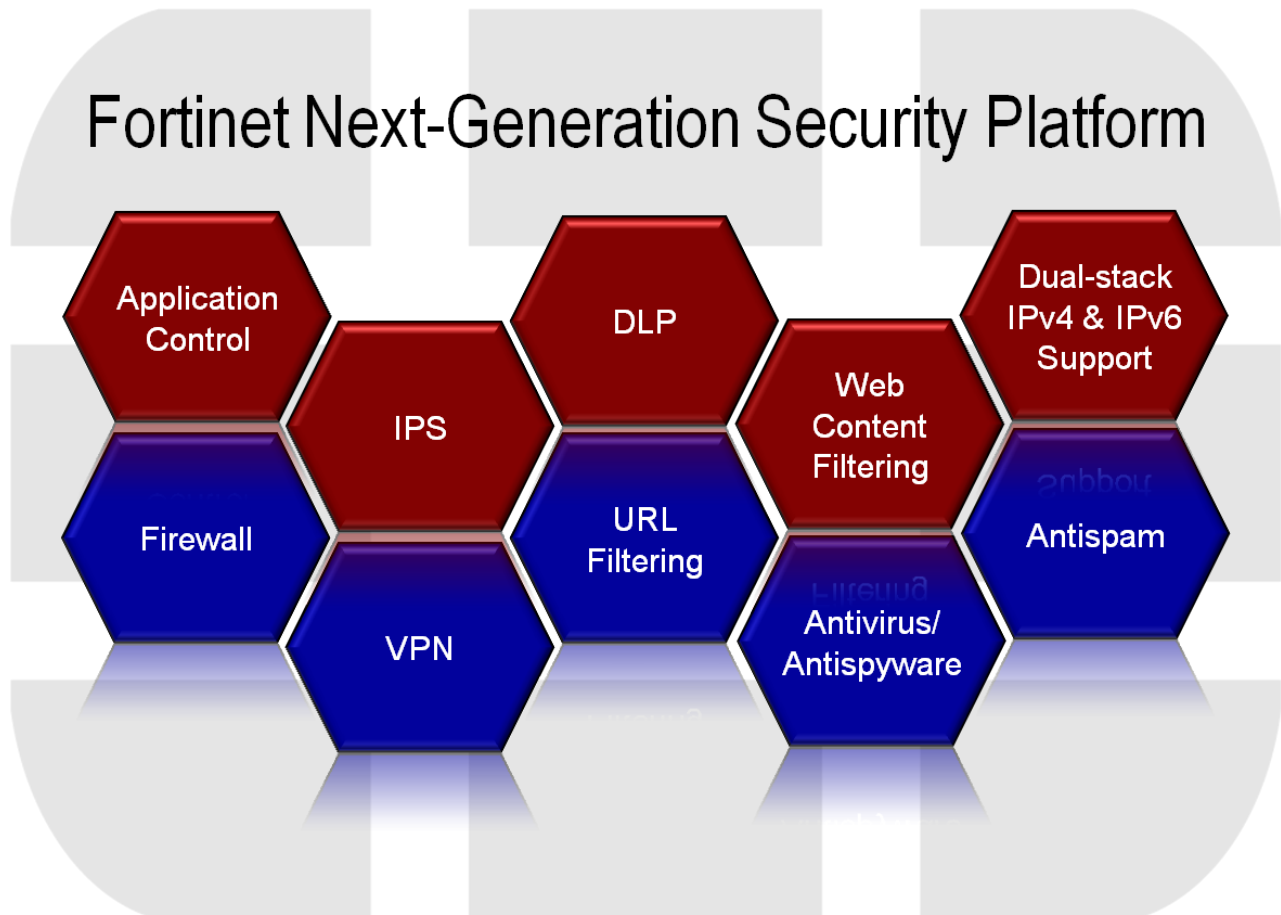


Figure 13: Fortinet Next-Generation Security Platform with Single Pane of Glass Management

About Fortinet

Fortinet delivers unified threat management and specialized security solutions that block today's sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership.

About FortiOS

FortiOS™ is a security-hardened, purpose-built operating system that is the software foundation of FortiGate® consolidated security platforms. FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC™ content and network processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with expert threat intelligence delivered via FortiGuard® Security Subscription Services.

FortiOS 4.0 software redefines network security by extending the scope of integrated security and networking capabilities within the FortiGate consolidated security platform. Regardless of the size of your organization, you can benefit from the most comprehensive suite of security and networking services within a single device on the market today.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with return and replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 90-day limited software warranty.

FORTINET

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015



Copyright © 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.