Web Filtering: An Essential Part of a Consolidated Security System
Summary

After almost two decades of popular adoption, organizations and users of the world-wide web are still being victimized by web-based threats. In spite of the billions of dollars invested in security, web-borne threats are still on the rise. They are more sophisticated and targeted, and with the rise of mobility in the workplace, even more difficult to control. The web’s standards-based interface and incredible number of applications have made it the medium of choice for hackers and thieves looking for new ways to disrupt services, steal information and perform malicious activities for financial gain. Here enterprises face a dilemma; employees need web access in order to do their jobs effectively, while management seeks to minimize risk to the corporation. In order to achieve an acceptable balance, management must decide who needs web access, when, how much, and from where. And most importantly, to stay ahead of new threats, enterprises need a security system that can enforce granular web access policies on all devices used to access the web from inside and outside the network perimeter. Since web-based attacks are frequently launched as a blend of several threat technologies, an effective security solution must provide a layered defense employing multiple security technologies. In-depth monitoring and reporting capabilities must be available to alert administrators and users to dangerous web sites and use patterns, and to allow further analysis for fine tuning. This solution must also be easy to configure, deploy and manage.

Introduction ............................................................................................................................................................................... 4
Web-Based Threats Cause Real Damage ................................................................................................................................ 4
  Prevalent Web-based Threats .................................................................................................................................................. 5
    Viruses and worms ................................................................................................................................................................. 5
    Spyware ................................................................................................................................................................................... 5
    Phishing .................................................................................................................................................................................. 5
    Pharming ............................................................................................................................................................................... 6
    Trojans horses and botnets .................................................................................................................................................... 7
Methods Used to Spread Web-based Threats .......................................................................................................................... 7
  Email ....................................................................................................................................................................................... 7
  Instant messaging ................................................................................................................................................................... 7
  Peer-to-peer networks .............................................................................................................................................................. 7
  Drive-by downloads ................................................................................................................................................................. 7
  Social networking .................................................................................................................................................................... 7
Methods for Controlling Web Access ........................................................................................................................................ 8
  Steps for Implementing Web Access Control .................................................................................................................... 8
Common Web Filtering Technologies ......................................................................................................................................... 8
  Banned word lists .................................................................................................................................................................. 8
  URL blocking lists ................................................................................................................................................................. 9
  Category blocking lists .......................................................................................................................................................... 9
Fortinet’s Web Filtering Solution ............................................................................................................................................. 9
  Web Content Filtering .......................................................................................................................................................... 9
URL Filtering ........................................................................................................................................................................... 10
  Block ................................................................................................................................................................................... 10
  Allow ................................................................................................................................................................................ 10
Pass.................................................................................................................................................................................... 10
Exempt................................................................................................................................................................................ 10
FortiGuard® Services .......................................................................................................................................................... 11
Unparalleled protection against zero-day web threats ................................................................................................. 11
FortiGuard Web Filtering Service ........................................................................................................................................ 11
How FortiGuard Web Filtering Service works .................................................................................................................... 12
Multi-layered Protection against Web-Based Threats ........................................................................................................... 13
Centralized Deployment and Management ......................................................................................................................... 14
Monitoring, Logging and Reporting ..................................................................................................................................... 14
Conclusion .............................................................................................................................................................................. 16
About Fortinet ......................................................................................................................................................................... 17
About FortiOS ......................................................................................................................................................................... 17
Introduction

Surfing the web is undoubtedly the most common use of the Internet. Consumers can access nearly any type of information and purchase goods and services from the comfort of their own homes. For workers and the businesses that employ them, the web has boosted productivity and efficiency by enabling instant communication and information sharing in multiple rich formats. However, when workers access the web from devices that are connected (or will soon be connected) to their employer’s internal network, they can expose the network to malicious activity including viruses, malware, phishing attacks and criminals seeking information to sell on the black market. In addition to web-based threats, non-business related web activity can reduce worker productivity and further expose businesses to liability through accidental sharing of information and access of inappropriate content.

These conflicting needs present enterprises with a dilemma. Employees need web access in order to do their jobs effectively, while management must minimize risk to the corporation. In order to achieve an acceptable balance, management must decide who needs web access, when, how much, and from where. Crafting a web access policy can be a contentious process requiring input from multiple conflicting interests, with resulting web access permissions granted to employees on a departmental or even an individual basis. When a comprehensive web access policy has finally been approved and presented to employees and the IT department, many companies consider the task accomplished. In reality, a security policy is only as effective as the security system and personnel used to implement and enforce it. Companies need a security system that has the flexibility to deploy and enforce granular web access policies on all devices used to access the web from inside and outside of the network perimeter, while remaining easy to configure, deploy and manage.

Web-Based Threats Cause Real Damage

The Internet has become a new breeding ground for malicious activity targeting both consumers and businesses. Its 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 disrupt services, steal information and perform 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.

Ever more sophisticated attacks use 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 event.

In addition to financial loss and legal liability, uncontrolled web access can result in:

- Lost productivity when workers access the web for non-business reasons
- Network congestion and business slowdown when valuable bandwidth is diverted from critical applications
- Increasing costs when additional Internet bandwidth must be purchased
- Lost business due to negative publicity following data breaches

---

1. 2010 Annual Study: Global Cost of a Data Breach, Ponemon Institute, LLC
Prevalent Web-based Threats

Viruses and worms
Viruses and worms usually leverage known system vulnerabilities and spread quickly through email, web sites and Trojan applications. They can carry out many malicious activities that range from disrupting network services to installing a stealthy backdoor application to provide unauthorized access to servers. Recent examples of sophisticated viruses and worms include SpyEye, ZeuS and Stuxnet. Some of these virus variants are now being used to attack mobile devices.

Spyware
Spyware encompasses a wide range of applications that are installed on a user’s computer to track and/or report certain information back to some external source. Unsuspecting users usually install these applications as shareware, freeware, or file sharing services, by opening infected emails, clicking on pop-up advertisements, or visiting frivolous or fraudulent web sites. Some of the most common types of spyware include; adware, keystroke loggers, toolbar editors, browser plug-ins, remote administration tools and games.

Phishing and Spear Phishing
Phishing attacks are usually launched using emails, instant messages or social network postings that appear to be from legitimate friends, auction sites, online payment processors or IT administrators. The messages usually redirect unsuspecting users to a fake website with a look and feel that is almost identical to the legitimate one. Users are then instructed to disclose personal information (social security numbers, account ID, passwords, credit card information, etc.) in order to resolve a problem or prevent disruption of critical services.

Spear phishing takes the next logical step, using stolen information to identify and launch direct attacks on high-value targets, such as senior executives and other high profile professionals with access to sensitive business information. Web-based social networking applications such as Facebook and Twitter are often used to launch spear phishing attacks, with attackers using stolen information to masquerade as a trusted associate or friend of the victim.
Figure 2: Phishing email and related fraudulent banking site

Uptimes of the phishing sites used to launch and control phishing attacks are a vital measure of how damaging phishing attacks can be, and can also be used to measure the success of mitigation efforts. Recently, phishing site uptimes are on the rise. This is a dangerous trend, as the first two days of a phishing attack are believed to be the most lucrative for the phisher\(^2\), and further demonstrates that efforts to shut down phishing sites are related zero day attacks are failing. The longer a phishing site remains active, the more money and personal information the victims and target institutions will potentially lose. Proxy avoidance or “anonymity networks” such as Tor can help phishing sites hide communications and evade detection.

![Phishing Email and Related Fraudulent Banking Site](image)

Figure 3: Recent trends in phishing site uptimes (HH:MM:SS)\(^2\)

Pharming

Identified as a next generation threat, pharming is even more dangerous than phishing because it requires no action from the end user. Unlike phishing attacks that require the user to click on a fraudulent URL, pharming victims may go about their normal web surfing activities, unaware that they are being attacked. Users are silently redirected from legitimate web sites to similar fraudulent web sites that have been designed to detect and extract personal and financial information.

---

\(^2\) Global Phishing Survey: Trends and Domain Name Use in 2H2010, APWG, April 2011
**Trojans horses**
Trojan horses are destructive programs that masquerade as useful applications. One of the most insidious types of Trojan horse is a program that claims to rid a computer of malware, but instead installs spyware or other malware onto an unsuspecting user's computer.

**Bots and botnets**
Originally developed to act as virtual individuals that could perform tasks in the background or while a computer user was busy, “bots” are now widely used for malicious purposes such as stealing passwords and silently gathering information. Bot “herders” control and gather information from globally distributed bots to form a larger “botnet”, which can be used to initiate denial-of-service attacks against remote targets or to distribute spam email. Bot herders managing large botnets often rent out their “services” to questionable third parties. The bigger the botnet, the more a bot herder can charge for services and botnet time.

**Methods Used to Spread Web-based Threats**

**Email**
Web-based email can be used to spread viruses, malware and phishing scams. Email viruses can access a user's entire contact database in order to send copies of itself, phishing emails and spam to additional victims. This mode of operation significantly extends the reach and life of the threat. URLs or images embedded in emails can be used to direct victims to dangerous web sites or install malware.

**Instant messaging**
Instant messaging can affect a company's ability to control sensitive information. It can be used to infect computers with spyware and viruses, conduct phishing attacks, and can also be used by Trojans to “phone home” to a remote computer. Sensitive information may be transmitted in the clear over the Internet and stored on servers that are not controlled and secured in accordance with the company’s computer security policies. In addition, instant messaging can reduce productivity when employees spend time “chatting” with friends and family members during work hours.

**Peer-to-peer networks**
Peer-to-peer networks are typically used for file sharing. They can expose endpoints to viruses, take up valuable network resources, lower employee productivity, and invite lawsuits should employees download copyrighted or sensitive material. Streaming media is a method of delivering multimedia, usually in the form of audio or video to Internet users. Viewing streaming media impacts legitimate business by using valuable bandwidth.

**Drive-by downloads**
Drive-by downloads can occur when a user visits a legitimate web site that has been infected with malware or scripts which redirect the user to actual malware sites. These malware sites may install viruses or information gathering software on the computer.

**Social networking**
Social networking web sites and applications, first popular with consumers but increasingly used from internal networks for business purposes, are becoming a real headache for enterprise security managers. Koobface is a computer worm that targets users of social networking applications including Facebook, Twitter and Friendster. When an unsuspecting user clicks on a link to download a video or other media, they are in fact installing the Koobface “bot” or botnet client. The Koobface bot uploads personal information and passwords to Koobface command and control servers.

---

3 Koobface Worm Doubles C&C Servers in 48 Hours
users to other malicious sites where additional malware can be downloaded. Experiments show a success rate of over 70% for phishing attacks on social networks.

**Mobile devices**
With all of the attention focused on security for networks and endpoint computers, mobile devices such as smart phones and touch pads which can access the Internet represent a "green field" opportunity for web criminals. Since most corporate IT departments have no control over the mobile devices used by their workers, they have no way to install protection such as antivirus, and no way to enforce security policies. Needless to say, as new smart phones incorporate more business-friendly features and applications, they are being used increasingly by mobile workers to store and communicate sensitive information, and to access the web. Successful computer viruses are now being repurposed to attack mobile devices and their more vulnerable operating systems.

**Methods for Controlling Web Access**
Businesses are realizing that traditional security solutions such as firewalls, intrusion detection systems and host-based antivirus are no longer adequate to protect against external web-based 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.

**Steps for Implementing Web Access Control**
Methods for monitoring and controlling web access range from manual and educational methods to fully automated systems designed to scan, inspect, rate and control each user's web activity. Clearly, web access is a worker efficiency issue as well as a security issue, and each company will need to decide which employees require web access and to what degree. Then they will need to choose and deploy the web access control mechanisms necessary to enforce their new web access policies. Some steps that companies should consider when implementing web access control include:

1. Establish a well written web usage policy for all departments and individuals as necessary, considering business needs as well as security concerns
2. Communicate the usage policy to every person in the organization
3. Educate all users on proper Internet, email, and computer conduct
4. Deploy monitoring tools that record and report on Internet usage
5. Install policy-based tools to capture, rate, and block undesirable and known-bad Internet URLs and web sites
6. Implement remediation steps to take appropriate action when users violate policies, register complaints, etc.

**Common Web Filtering Technologies**
Several different technologies are commonly used to monitor, log and filter access to web sites and related applications. Many solutions are software-based and run on servers attached to the network through a "mirrored" network port. Other solutions include dedicated appliances that are installed in-line with network traffic flows, enabling visibility of all Internet traffic and fast responsive action against policy violations and malicious content. Some common web content filtering technologies are described below.

**Banned word lists**
This web filtering method uses a "black List" dictionary containing banned or undesirable words or phrases. URLs and web content are compared against the black list to block unauthorized web sites. This technology was originally a manual process which used vendor-provided black lists as a starting point. This method has improved over the years and vendor-provided black lists have grown to include millions of keywords and phrases. Updates are usually performed manually and
filtering accuracy may be impacted for specific categories. For example, medical research sites may be blocked if they are mistaken for offensive material.

URL blocking lists
URL blocking is also typically performed using a black list, however this black list contains known-bad or unauthorized website URLs. Entire URLs can be blocked and exemptions can usually be made to allow access to useful portions of a website. Many vendors provide URL black lists with their products in order to simplify the technology, giving the user the ability to add new sites and perform URL pattern matching. Depending on the frequency of the updates, both banned word lists and URL black lists may fall out of compliance with corporate policies between updates.

Category blocking lists
Category blocking lists are used to control access to web content. They greatly simplify management by leveraging an external service that maintains and distributes the latest web URL ratings. There are no manual lists to install or maintain. Web traffic is compared to rating databases installed on category servers and the results can be cached locally to increase web filtering performance. This up-to-date web URL and category information eliminates manual management of local black lists, and can be used to ensure accuracy and real-time compliance with corporate Internet usage policies.

Fortinet’s Web Filtering Solution
Many threats leverage a combination of web-based attack technologies and methods to penetrate or circumvent perimeter security defenses. Examples of these so-called “blended” threats include spyware and phishing attacks which combine spam email with posts to social networking sites such as Facebook and Twitter. Users are tricked into visiting dangerous web sites which install malware on the host computer. The malware is used to collect account passwords, eavesdrop on conversations, or copy personal address books. Now the attacker can masquerade as a friend of the victim in order to abuse the trust of additional victims. In this way an attack can snowball indefinitely.

With this in mind, it should come as no surprise that multiple protections are frequently required to stop web-based threats at the network perimeter. This philosophy forms the basis of Fortinet's approach to designing threat protection solutions. By integrating multiple threat detection technologies and methods into a single platform, FortiGate consolidated security appliances significantly increase detection and blocking rates of both blended and non-blended web-based threats.

Web Content Filtering
The Fortinet web filtering solution begins with traditional 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 filter web traffic based on:

- Application use (full or partial blocking)
- Content as defined in data loss prevention (DLP) policies
- Wildcard pattern matching
- Multi-language pattern matching
- Web pattern lists
FortiGate web filtering services can also be combined with FortiGate Antivirus, Intrusion Prevention, Anti-Spam and Flow-based Inspection functions to further improve threat detection and mitigation. FortiGate also supports HTTPS web filtering to prevent hackers from hiding their attacks with encryption.

**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. URL filtering relies on FortiGuard Web Filtering Services to determine the category and rating of a specific URL. FortiGuard Web Filtering Services will be covered in more detail later on in this whitepaper. Web sites or URLs can be easily added to the local URL filtering list using both text and regular expressions. 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.
Web Caching
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.

FortiGuard® Services
In addition to web filtering, FortiGuard Services also provide comprehensive updates for antivirus, antispyware, intrusion prevention, antispam, application control, database loss prevention and vulnerability management functions on FortiGate consolidated security appliances. FortiGuard Services were designed from the ground up to optimize performance and maximize protection afforded by Fortinet security platforms. For the purposes of this document, we will limit the discussion to the web filtering capabilities and updates provided by FortiGuard Services.

Unparalleled protection against zero-day web threats
FortiGuard Services are continuously updated by FortiGuard Labs. More than 125 security threat researchers, engineers, and forensic specialists comprise the FortiGuard Labs team. Operating in Canada, China, France, Japan, Malaysia and the United States, this team provides around the clock and around the globe coverage to assure some of the fastest response times in the industry to new viruses, vulnerabilities, attacks and malicious threats. The FortiGuard team collaborates with the world’s leading threat monitoring organizations to advise and learn of new and emerging threats. Additionally, the team contributes to the overall security industry by identifying and responsibly reporting vulnerabilities directly to vendors of hardware, operating systems and applications.

FortiGuard Web Filtering Service
The FortiGuard Web Filtering Service enables FortiGate appliances and FortiClient endpoint security agents to block access to dangerous or inappropriate websites which may contain malware or objectionable content. Based on intensive global research and analysis, web filtering updates enable the application of granular and accurate web filtering policies that protect enterprise networks and computers against web-based threats and data loss. Real-time updates are delivered continuously via the FortiGuard global distribution network.

The FortiGuard Web Filtering Service provides information on 77 web content categories, more than 30 million rated websites, and more than 2 billion individual web pages making it a leader in ratings accuracy and the breadth of content
categories covered. With regular updates, FortiGate appliances and FortiClient endpoint security agents can accurately scan, rate, and filter web traffic based on categories and groups such as:

- Potentially liable - drug abuse, folklore, hacking, illegal or unethical, drugs, occult, phishing, plagiarism, proxy avoidance, racism and hate, violence, web translation
- Controversial - abortion, adult materials, advocacy groups/organizations, alcohol, extremist groups, gambling, lingerie and swimwear, nudity, pornography, sex education, sport hunting and war games, tasteless, tobacco, weapons
- Potentially non-productive - advertising, brokerage and trading, digital postcards, freeware, downloads, games, instant messaging, newsgroups and message boards, web chat, web-based email
- Potentially bandwidth consuming - internet radio and television, internet telephony, multimedia download, peer-to-peer file sharing, personal storage
- Potential security risks - malware, spyware
- General interest - arts and entertainment, child education, culture, education, finance and banking, general organizations, health and wellness, job search, medicine, news and media, personal relationships, personal vehicles, personal websites, political organizations, real estate, reference, religion, restaurants and dining, search engines, shopping and auction, society and lifestyles, sports, travel
- Business oriented - armed forces, business, government and legal organizations, information technology, information/computer security
- Other - content servers, dynamic content, miscellaneous, secure websites, web hosting

*How FortiGuard Web Filtering Service works*

The FortiGuard Web Filtering Service is a hosted solution designed to provide web URL filtering capabilities and updates for Fortinet customers such as enterprises, service providers, schools, libraries and government agencies. The FortiGuard Web Filtering Service is implemented using FortiGuard Rating Servers and FortiGate consolidated security appliances as shown below. If FortiClient agents are installed on endpoint devices, they will receive updates from FortiGate appliances.
The FortiGuard Web Filtering Service filters web content requests in real-time using the following sequence of events:

1. Customer or end user requests a website URL (a).
2. If the rating for the URL is already cached in the FortiGate unit, it is immediately compared with the policy for the user (b). If the site is allowed, the page is requested from the web server (c) and the response is retrieved (d).
3. If the URL rating is not in the FortiGate cache, the page is requested (c) and a rating request is made simultaneously to the FortiGuard Rating Server (e).
4. The response from the Web site (d) is stored by the FortiGate unit until the rating is received. The rating response is returned to the FortiGate unit (f) and is compared with the requestor’s policy (b).
5. If the policy allows the user to view the page, the web site response (d) is passed on to the requestor (g). Otherwise, a user-definable “blocked” message is sent to the requestor and the event is logged in the content filtering log.

**FortiGuard feedback channel**
The FortiGuard Web Filtering Service also provides a feedback channel for website categorization. Administrators can submit an unrated website or look up an existing website using the FortiGuard Web Filtering web site: [http://www.fortiguard.com/webfiltering/webfiltering.html](http://www.fortiguard.com/webfiltering/webfiltering.html). Administrators can also override FortiGuard service ratings by using a local rating on their FortiGate device, providing full control of web access.

**Multi-layered Protection against Web-Based Threats**
Owing to Fortinet’s philosophy of combining multiple threat detection technologies and methods on a single platform, web filtering can also be combined with other Fortinet security functions to provide superior threat detection and protection against the latest known and unknown web-based attacks.

For example, web content filtering technologies can be combined with antivirus, antispyware, intrusion prevention, antispam, application control, database loss prevention and vulnerability management functions into a single protection policy. By
sharing information between security functions, threats can be quickly identified and blocked at the perimeter - before they enter the network or cause damage to endpoint computers and devices.

Centralized Deployment and Management

Web filtering is enabled on each firewall policy and is fully configurable through an intuitive web-based interface. For large installations, FortiManager appliances provide centralized policy-based provisioning, configuration, and update management for FortiGate appliances and 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.

Figure 7: Centralized policy management

Monitoring, Logging and Reporting

FortiGate security platforms allow a wide array of internal and external logging and reporting features to track accountability and provide detailed reporting on all security functions. With authentication enabled, users must authenticate successfully to the FortiGate unit (e.g. through a local user database, Active Directory, LDAP, or RADIUS) before gaining access to the Internet. All logged Internet activity is tagged with a user’s authentication information, providing detailed logging and reporting of employee web surfing activity.
Figure 8: FortiGate UTM Weekly Activity Report – Top Clients

Figure 9: FortiGate UTM Weekly Activity Report - Top Allowed Sites by Requests
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 users 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.

**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 ever more sophisticated web-based attacks. To stay ahead of new threats, enterprises need a security system that can enforce granular web access policies on all devices used to access the web from inside and outside of the network perimeter. Since web-based attacks are frequently launched as a blend of several threat technologies, an effective security solution must provide a layered defense employing multiple security technologies. In-depth monitoring and reporting capabilities must be available to alert administrators and users to dangerous web sites and usage patterns, and to allow further analysis for fine tuning. This solution must also be easy to configure, deploy and manage.

When combined with FortiGuard Services and the many security functions available on FortiGate consolidated security appliances, Fortinet Web Filtering provides enterprises with the most comprehensive protection against web-based threats available today. Fortinet security solutions are built from the ground up by Fortinet, with all security technologies developed in-house for tight integration. Deployed on a single FortiGate platform, Fortinet security solutions are easy to configure and manage. Custom FortiASIC™ network and security processors offload demanding and repetitive tasks to accelerate inspection and traffic throughput, while many FortiGate systems allow effortless scalability with the addition of custom security modules. As the leading global provider of unified threat management (UTM) systems, Fortinet is well positioned to protect your company against the latest network and web-based threats now and into the future.
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.