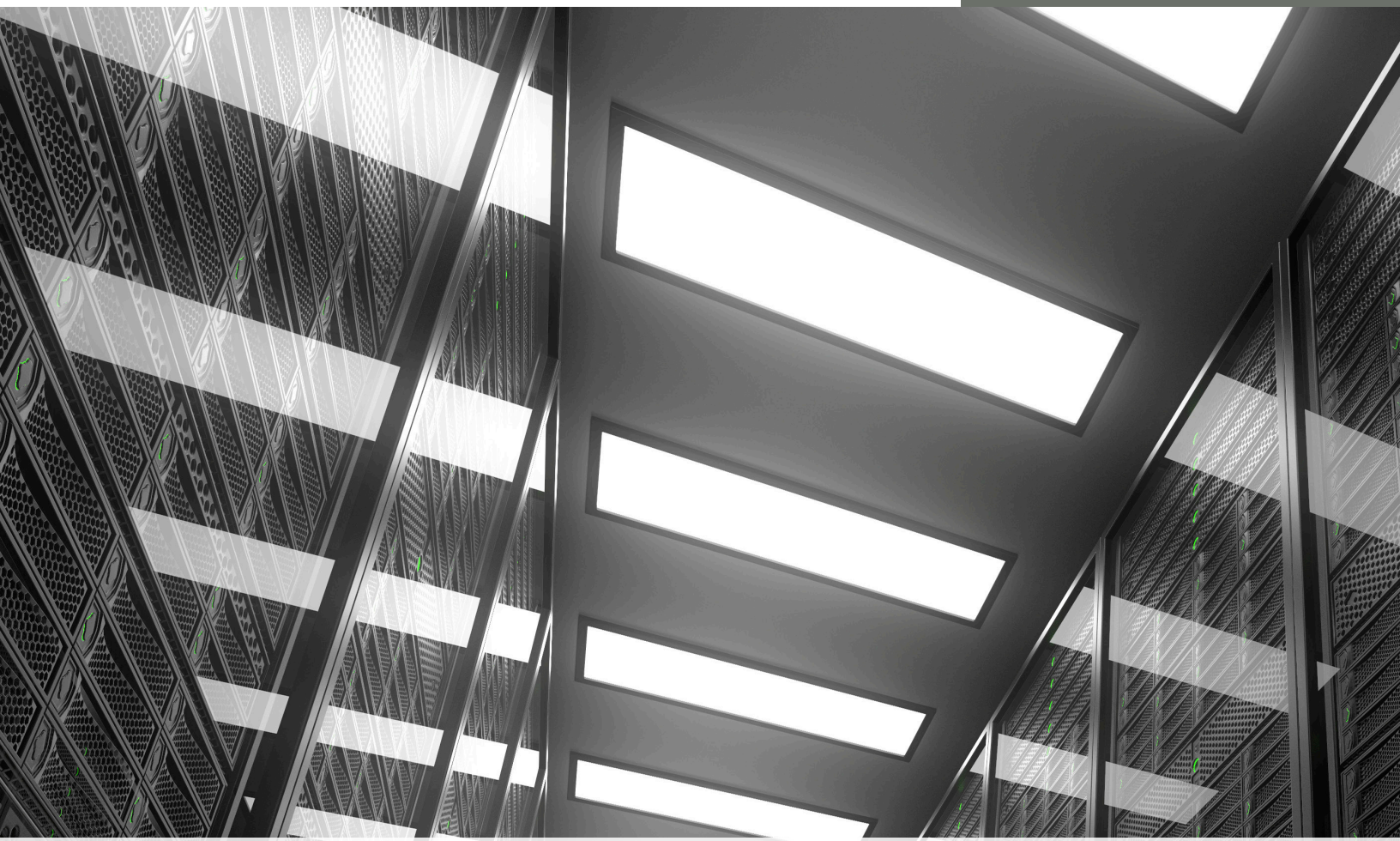
FORTINET

SOLUTION GUIDE



Application Security for the Data Center

Securing Applications from Threats Requires a Complete, Integrated Solution that Enhances Enterprise Firewall and Intrusion Prevention Technologies

Introduction

Most organizations focus their limited resources on locking down access and controlling their networks to protect their data centers from external threats. The latest generation of enterprise firewalls and intrusion prevention systems (IPS) primarily focus on securing the network and controlling access to it. These are great technologies, however there are limits to what they can offer to provide complete protection against threats that target applications, application services, and users.

As soon as an application is opened to the Internet, it is a target. All that stands between an attacker and an organization's sensitive data is an unassuming login screen. No matter how many layers of network security are in place, this entry point could expose customer data, proprietary information, or sensitive financial information if the application hasn't been hardened or protected by some other means.

In this solution guide we'll explore the top challenges organizations face when it comes to securing applications and the data they host, including web application vulnerabilities, application layer DDoS attacks, advanced persistent threats (APTs), scaling application encryption, and protecting users from email-borne threats.

Applications are Easy Targets

There is no question that a firewall is your first line of defense for network security. Today's latest firewall technologies are almost bulletproof, at least at the layer 2 and 3 levels. Attackers and cyber criminals know this and have had to adapt their techniques. Not that they won't try to look for firewall vulnerabilities, rather they know that high-value targets like financial institutions, retailers, and government agencies have tightened their security policies and the days of easy data breaches at the firewall are over.

The fastest growing categories of attacks and data breaches are those that target applications, application layer services, and inexperienced users. These represent most of the remaining weak spots and there are countless possibilities to exploit code vulnerabilities, application modules, and trusting users who think that the email they just received was a legitimate request to reset their account credentials.

Web Application Attacks

Verizon's 2015 Data Breach Investigations Report revealed that over 38 percent of all data breaches were caused by web application vulnerabilities. The Open Web Application Security Project (OWASP) has consistently reported since 2010 that almost every web-based application has one or more vulnerabilities listed in their Top 10 list of application security risks. They have also reported that 95 percent of all websites are attacked annually using cross-site scripting and injection techniques. Gartner stated in its 2015 Web Application Firewall Magic Quadrant that they expect more than 80 percent of all enterprises will have a web application firewall (WAF) in place by 2018 to protect against web application attacks.

Application Layer DDoS Attacks

Distributed denial of service (DDoS) attacks are one of the oldest security threat types, however they have evolved over the past decade to target application-level services. Large scale bulk volumetric attacks still grab the large headlines, however the fastest growing category of these attack types are layer 7 events that only take a few megabits of packets to do as much harm as an attack in the hundreds of gigabits. DDoS attacks are still ranked as the top threat by data center managers compared to other events like infrastructure outages and bandwidth saturation.

Email: The Backdoor to Your Security Fortress

Network security professionals spend the better part of their careers designing, implementing, and maintaining the latest and best defenses for their organizations. Even with the most advanced firewall security systems in place, all it takes is one click by a user on a link in a malicious email to bypass your carefully crafted network protections. Cyber criminals are getting much more sophisticated in their tactics. Many spam and phishing emails they send can fool even the most cautious of users with communications that appear to come from reliable sources or even your own IT department.

Email is also one of the key attack vectors for social engineering. Clever attackers can now easily access connections on Facebook, LinkedIn, and other social media sites to easily obtain contact information. Then they craft emails that look like they're being sent by legitimate friends and colleagues in an attempt to trick users into downloading malicious attachments or direct them to websites where malware can be installed.

Protecting Applications from APTs

APTs are custom-developed, targeted attacks. They can evade straightforward detection, using previously unseen (or "zero-day") malware, exploit vulnerabilities (unpatched security holes), and come from brand-new or seemingly innocent hosting URLs and IPs. Their goal is to compromise their target system with advanced code techniques that attempt to circumvent security barriers and stay under the radar as long as possible.

Applications and email are two top vectors in APTs. Many web applications allow the uploading of files and many emails contain attached files that could be risks. Antivirus scans can check for previously identified risks, however APTs generally are tailored to circumvent traditional AV detection and many slip past this first line of defense.

Secure Application Traffic Growth

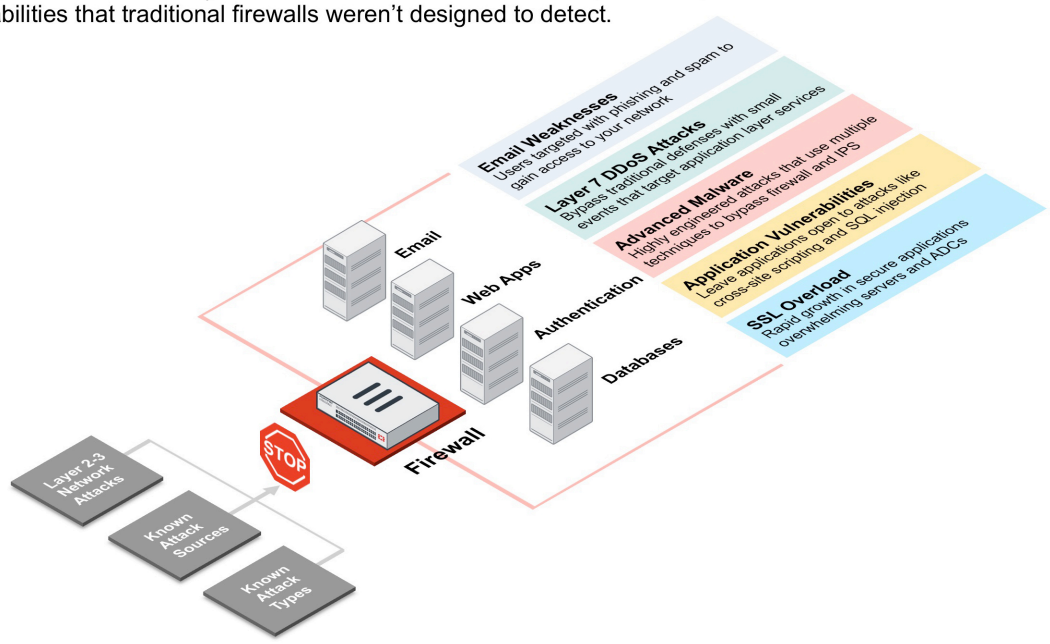
Although not a threat, many enterprises are aggressively expanding SSL to all their web-facing applications. Even seemingly benign applications are getting the "secure" treatment in order to patch known or unknown vulnerabilities to other more important systems. Sandvine's Encrypted Traffic Report 2015 saw encrypted traffic volume increase to 30 percent in 2015 and expects 50 percent growth in 2016. Combined with this explosive expansion in traffic, the complexity of moving to more advanced encryption keys as the technology expands from 1,024 keys to 2,048 and now 4,096, is doubling and even quadrupling secure packet sizes. Servers and load balancers are struggling to keep up with this demand using today's current crop of secure application delivery solutions.

Complete Application Security Extends Past the Firewall

Each of the areas presented in the previous section provide unique challenges that need more than a firewall or an IPS to completely address. Most firewall and IPS systems today, including our FortiGate product line, have features that can solve many of these new problems. However, in general they are limited to signature detection and need additional solutions to provide complete protection for unknown and zero-day attacks. FortiGate has many services that can be enabled such as deep packet inspection and data loss prevention (DLP), but even with those, there are still loopholes and there are performance impacts that need to be considered in enterprise deployments.

Backdoors to Your Firewall and IPS

Even advanced firewalls and IPS systems can't completely protect your network and applications from today's latest threats. Attackers have adapted to exploit vulnerabilities that traditional firewalls weren't designed to detect.



The most used application-level protection features of FortiGate and other firewalls are IP reputation and signature detection. Usually subscription-based services, IP reputation and attack signatures are very effective measures that block attacks before any processing is applied by the firewall. If an attack is from a known source or it matches a predefined signature, it is blocked automatically without the firewall having to perform any further inspection. FortiGate offers these services through our award-winning FortiGuard Labs.

Although signature services are very effective to block attacks from known sources and previous attack patterns, zero-day and APTs bypass these detection systems. In some cases APTs are so customized, that malicious code is developed specifically at a single target with no forewarning until the malware is deployed. Signatures and IP reputation also can't fully protect web applications from attacks as many code-based vulnerabilities have almost unlimited ways to bypass any predefined signatures.

In the face of these threats, Fortinet has risen to the occasion with purpose-built solutions to supplement the protections in firewalls and IPS platforms. These include web application firewalls for application security, DDoS attack mitigation appliances for DDoS protection, advanced application delivery controllers (ADCs) to meet the demands of secure application traffic, sandboxing to isolate malicious code for inspection, and email security gateways that can detect and prevent email-borne threats from getting to your users.

In a perfect world all of these security measures would be in a single appliance. However, even with the best hardware available today, the performance impacts of these services put an all-inclusive "super firewall" out of reach for enterprises. FortiGate offers many advanced services that come close, but still, no one product can do everything. We discussed deep packet inspection earlier. Most enterprise data center managers do not turn this service on as it can be very processor-intensive and can impact overall firewall throughput. In these cases, the FortiGate is streamlined to basic capabilities for maximum performance, where other devices manage the additional layers of security needed. Small to mid-size organizations enable many of the advanced FortiGate NGFW features for Unified Threat Management (UTM), where a single box can handle the throughputs and make things easier to manage to help when IT resources are limited.

So, as a data center manager you're most likely going to need to look beyond the capabilities of your firewall to provide the complete network and application protection to meet the challenges your organization faces.

For large organizations, one of the most difficult decision points is whether or not to consolidate to one vendor or opt for "best-of-breed" point solutions. There are many arguments on both sides of this debate ranging from "single vendors are easier to deal with" all the way to "point solutions will offer the best in security and features." When you sit down and weigh the options, you should look at what is critical to your organization such as features, interoperability, integration, management, and support to select a vendor that can meet as many of those to provide a complete end-to-end solution for your data center.

The remainder of this document discusses the major challenges and provides you information on how Fortinet can help you solve these problems as a complete single vendor for your advanced network and application security needs.

PCI Compliance, Firewalls, and WAFs

We've done our best to highlight the case that you're going to need more than a firewall to completely protect your applications and data. If you're in one of the many industries that deal in e-commerce and banking, you need to consider PCI compliance for your network and application security.

Although PCI DSS standards are not mandated by law, many laws, especially at the state and local level, specifically mention PCI compliance to meet legal requirements. A firewall alone is not going to be enough. To pass PCI DSS 6 compliance, you're going to need a web application firewall to meet all the OWASP Top 10 Application Threats that are referred to in that section. Below is a list of the OWASP Top 10 and how a WAF stacks up against a firewall.

Application Threats: The OWASP Top 10

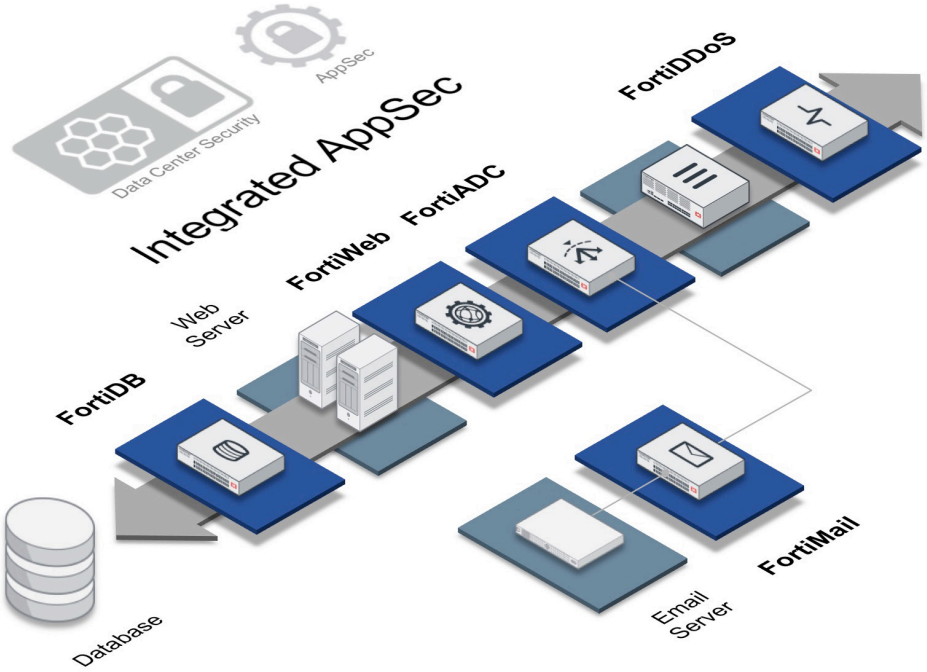
	Threat	Firewall	WAF
1	Injection (SQL, OS, and LDAP)	No	Yes
2	Broken Authentication and Session Management	No	Yes
3	Cross-Site Scripting	No	Yes
4	Insecure Direct Object References	No	Yes
5	Security Misconfiguration	No	Yes
6	Sensitive Data Exposure	Yes	Yes
7	Missing Function Level Access Control	No	Yes
8	Cross-site Request Forgery (CSRF)	No	Yes
9	Using Components with Known Vulnerabilities	No	Yes
10	Unvalidated Redirects and Forwards	No	Yes

Application Security Solutions

Fortinet is much more than our enterprise-class FortiGate firewalls. We offer many solutions that provide complete network and application security for a data center. The following section covers many of the advanced threats and challenges that data centers face today along with the solutions offered by Fortinet. For more details on the products presented, white papers, case studies and other useful information, please visit Fortinet.com.

Fortinet's Integrated Application Security Solution

Fortinet 's application security solution delivers a complete end-to-end high-performance solution that protects an organization's valuable information throughout the data center by using a combination of Fortinet products. These include web application firewalls, email security gateways, application delivery controllers, DDoS mitigation, and database security.



Web Application Security

Web applications are attractive targets to hackers as they are public-facing applications that require being open to the Internet. As many provide major e-commerce and business-driving tools, they can contain cardholder, company, and other sensitive data.

Perimeter security technologies such as IPS and firewalls have focused on network and transport layer attacks. Many vendors, including Fortinet have added application layer enhancements, usually referred to as “Deep Packet Inspection” (DPI) to extend signature detection to the application layer. Although DPI is useful in protecting against attacks on the web server infrastructure (IIS, Apache, etc.), it cannot protect against attacks on custom web application code such as HTML and SQL.

Web Application Firewalls (WAFs)

Securing web applications requires a completely different approach than signature detection alone. Only a web application firewall can provide complete application protection by understanding application logic and what elements exist on the web application such as URLs, parameters, and what cookies it uses. Using behavioral monitoring of application usage, the WAF can deeply inspect every application in your data center to build a baseline of normal behaviors and trigger actions to protect your applications when anomalies arise from attacks.

FortiWeb Web Application Firewalls

FortiWeb Web Application Firewalls provide specialized, layered web application threat protection for medium/large enterprises, application service providers, and SaaS providers. FortiWeb Web Application Firewalls protect web-based applications and Internet-facing data from attacks and breaches. Using advanced techniques it provides bidirectional protection against malicious sources, DoS attacks, and sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, file inclusion, cookie poisoning, and numerous other attack types.

- WAF throughputs ranging from 25 Mbps to 20 Gbps
- Multiple, correlated threat detection methods include protocol validation, behavioral identification, FortiGate quarantined IP polling, and subscription-based FortiGuard IP reputation, antivirus and web attack signatures
- Included vulnerability scanner and support for virtual patching with third-party scanner integration
- Layer 7 content-based server load balancing and hardware-based SSL acceleration
- Simplified deployment with automatic setup tools and integration with FortiGate
- Centralized Management and administrative domains (ADOMs)

Web Application Security Threats

- Public facing applications are attractive targets
- Sensitive customer and proprietary data exposed
- Almost every web application has vulnerabilities
- Firewalls can only detect known threats
- 95 percent of all websites have experienced cross-site scripting and SQL injection attacks

Fortinet Virtual and Hardware Appliances

Fortinet offers many of its products in both hardware and virtual appliance versions. Most products fully support the major virtualization platforms including VMware, Microsoft Hyper-V, Citrix XenServer, Amazon Web Services, and Microsoft Azure. See the chart below for virtual versions and platforms supported for products mentioned in this document.

Virtual Product	VMware	Hyper-V	XenServer	AWS	Azure
FortiGate VM	Yes	Yes	Yes	Yes	Yes
FortiWeb VM	Yes	Yes	Yes	Yes	Yes
FortiADC	Yes	Yes	Yes	No	No
FortiMail VM	Yes	Yes	Yes	No	No
FortiSandbox VM	Yes	No	No	No	No

DDoS Protection

DDoS attacks were one of the first data center threats and as they've evolved, they continue to be the top threat that data center managers face today. New DDoS attacks target layer 7 application services and can do as much damage as high-volume multi-gigabit bulk-volumetric attacks. Rather than simply flooding a network with traffic or sessions, these attack types target specific applications and services to slowly exhaust resources at the application level.

Application layer attacks can be very effective using small traffic volumes, and may appear to be completely normal to most traditional DDoS detection methods. This makes application layer attacks much harder to detect than other basic DDoS attack types. Most ISPs use basic methods to protect you from large-scale attacks, however they don't have the sophisticated detection tools to intercept these smaller application-level threats and normally pass them through to your network.

Advanced DDoS Threats

- Oldest but fastest evolving threat type
- Remains #1 threat to data centers
- Layer 7 threats fastest growing category
- Firewalls can only detect known DDoS threats
- Small layer 7 attacks under 50 Mbps can do as much damage as attacks in the hundreds of gigabits

DDoS Attack Mitigation Solutions

There are many options available for DDoS attack mitigation ranging from simple DIY server configurations to advanced data center-based hardware solutions. Most ISPs offer layer 3 and 4 DDoS protection to keep your links from becoming flooded during bulk volumetric events, however they don't have the capability to detect the much smaller layer 7-based attacks. Data centers cannot rely on their ISPs alone to provide a complete DDoS solution that includes application layer protection.

DDoS attack mitigation appliances are dedicated in-line devices that block layer 3, 4 and layer 7 attacks that come in carrier- and enterprise-grade options. Most organizations that want to protect their private data centers usually look at the enterprise models to provide cost-effective DDoS detection and mitigation. Today's offerings provide capacities that can handle large-scale volumetric attacks for 100 percent layer 3, 4, and 7 protection or can be used to supplement basic ISP-based bulk DDoS protection with advanced layer 7 detection and mitigation.

FortiDDoS DDoS Attack Mitigation Appliances

The FortiDDoS family of purpose-built appliances provides real-time network visibility in addition to detection and prevention of DDoS attacks. FortiDDoS helps protect Internet-facing infrastructure from threats and service disruptions by surgically removing network and application-layer DDoS attacks. It defends critical on-premises and cloud infrastructure from attacks while relying on sophisticated filtering technologies to allow legitimate traffic to continue to flow. These scalable, high-performance appliances deliver proven DDoS defenses, and are completely interoperable with existing security technologies and network infrastructure.

- Up to 48 Gbps of total bi-directional throughput
- Inline, transparent mitigation for layer 3, 4, and 7 DDoS attack types
- 100 percent behavioral-based DDoS detection and mitigation using ASIC technology
- FortiASIC TP2 processor delivers less than 5-second attack response and mitigation times
- IP reputation scoring system and continuous attack re-evaluation reduce risks of false positive detections
- Centralized alerts, bandwidth management, role-based management, and self-service portals for MSSP environments

Email Protection

Email is a critical business service that no organization can survive without, but it is one of the greatest vulnerabilities when it comes to security. It has become the primary target that criminals use to take advantage of poor security policies and unsophisticated users.

Email threats come in two primary forms, inbound and outbound. Inbound are the traditional threats like spam and phishing attacks that attempt to lure users into providing sensitive information such as login credentials or credit card information. Outbound threats aren't really attacks, rather they are risks to your organization's sensitive information. Employees, contractors, and consultants have the ability to send proprietary information to anyone, anywhere. Sometimes it's by mistake; other times it's not.

Secure Mail Gateway

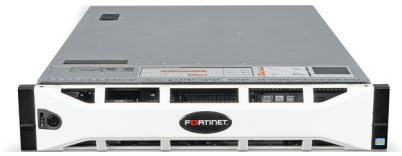
Secure mail gateways are dedicated hardware or virtual devices that provide protection from email spam and malware, and also provide outbound email content inspection and encryption. Through the use of reputation filtering, most email is filtered out and using advanced spam and phishing detection emails are scanned that pass through the network to determine if they are threats. Suspicious emails can be blocked or quarantined for later review depending on how the gateway is configured.

Data center managers can set detailed business rules to scan all outgoing email for sensitive data. If any sensitive data is discovered, it can be blocked or automatically encrypted depending on how the policies are configured.

Email Remains a Top Target

- Even sophisticated users are falling prey to advanced phishing schemes
- Data loss of sensitive materials is a major risk to organizations
- Emails with links to websites easily open security threats to your network
- Firewalls can't stop users from making mistakes
- Need a solution that can scan for spam, phishing, and suspicious links to prevent users from attacks

FortiMail



FortiMail is a complete secure email gateway offering suitable for any size organization. It provides a single solution to protect against inbound attacks, including advanced malware, as well as outbound threats and data loss with a wide range of top-rated security capabilities. These capabilities cover: antispam, antiphishing, anti-malware, sandboxing, data loss prevention (DLP), identity based encryption (IBE), and message archiving.

FortiMail's inbound filtering engines block spam and malware before they can clog your network or compromise your systems. Its outbound inspection technology (including 3G mobile traffic) reduces the loss of sensitive information, maintains compliance, and prevents your organization and users from being blacklisted. When integrated with Fortinet's NSS Labs Recommended FortiSandbox, FortiMail helps stop the most advanced threats before they reach end users.

- Highly effective email security: 37 consecutive VBSpam Platinum awards, 40 VB100 awards including high marks in their Reactive and Proactive (RAP) testing, AV Comparatives Advanced+ designation for Antiphishing, and NSS Labs Recommendation for Breach Detection (integrated FortiSandbox).
- Protection for sensitive information and compliance: Integrated DLP and email encryption, including predefined yet customizable dictionaries and Identity Based Encryption (IBE), plus email archiving.
- Part of Fortinet's Advanced Threat Protection Framework: Secured by FortiGuard Security Services. Integrating with FortiSandbox, FortiMail is an integral part of a cohesive approach to close off a critical, early-stage element of the targeted attack kill chain.
- Highest performance: The unique architecture of FortiMail has been proven to meet the requirements many of the world's largest carriers and is the highest-performing messaging security solution in the industry, delivering message protection for over 28 million messages per hour in a single appliance.
- Unparalleled deployment flexibility: Gateway, inline and server modes, plus physical, virtual, and cloud form factors ensure a seamless fit for all environments.

Secure Application Delivery

Users have come to expect applications to be there when they need them and to respond immediately. It is a given now that they also expect that you are protecting their and your organization's sensitive data. In order to provide the security that almost every application needs, data center managers are deploying SSL on almost every application, however this comes at a cost in user capacities, speed, and latency.

As mentioned previously, the trend in secure traffic growth will strain even the best-architected data centers to keep up with this demand. Coupled with this is that SSL encryption keys are getting more complicated as they expand from the older 1,024-bit keys to 2,048, and now 4,096.

ADCs with SSL offloading

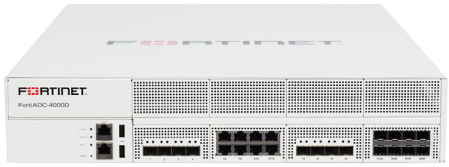
Application Delivery Controllers (ADCs) offer the feature to offload SSL traffic from servers to the ADC itself. Most manufacturers can do this using software encryption and decryption, however only hardware-accelerated appliances have the dedicated ASIC processors to handle the speeds of a modern data center. Most software-based devices can handle a few hundred to a few thousand transactions per second vs. hardware-based appliances that can manage tens-of-thousands of secure transactions per second.

By offloading this processor-intensive traffic from the servers to the ADC, secure applications can scale up to 100 times while at the same time reducing response rates for end users.

Secure Application Traffic Growth

- Most organizations rapidly deploying SSL to protect all applications
- Secure traffic growing at rapid rate
- Application delivery infrastructure strained to keep up
- Firewalls usually have limited application delivery functionality
- Expansion of complex encryption keys (2,048 and 4,096) put increased demands on data center resources

FortiADC



FortiADC hardware and virtual ADCs provide unmatched server load balancing performance whether scaling an application across a few servers in a single data center or serving multiple applications to millions of users around the globe. With included SSL offloading, HTTP compression, global server load balancing, firewall, and link load Balancing, they offer the performance, features, and security needed at a single all-inclusive price.

- L4 throughput from 2.7 Gbps to 50 Gbps.
- Complete layer 4 to 7 server load balancing solution with intelligent policy-based routing
- Web application firewall and IP reputation (subscriptions required)
- Scripting for custom load balancing and content rewriting rules
- Authentication offloading speeds user authentication for secure applications
- SSL forward proxy for increased secure traffic inspection with FortiGate firewalls
- Qualified for Microsoft Exchange 2010 and 2013

Advanced Threat Protection for Applications

Malware can come in any form and can be one of the most difficult threats to detect. Some forms of it can be simple to detect as they may route a user to a website to download malicious code. Newer methods are much more obfuscated and rely on many different vectors to infect users or data center infrastructure elements.

This complexity, combined with the almost limitless options for zero-day malware attacks can make it almost impossible for firewalls and IPS systems to detect all these threats. Additionally, many of them may be buried in seemingly harmless code that in some cases may take years to be fully exposed.

Sandboxing

Even with the best threat detection defenses, sometimes it's just best to let the code "explode" to see what it's going to do. This is where a sandbox comes in and acts like a bomb squad. The suspicious code is isolated in a virtual bomb detonation chamber and allowed to do what it was intended to do. Since the sandbox is completely isolated from your network and applications, if the code is malware, it's not going to do any harm to your real environment.

Once the code is extracted and installed in the sandbox, it's easy to examine the changes it makes to do the damage it was intended to do. If it is assessed to be a threat, the malware is quarantined and blocked from entering your network.

FortiSandbox – Advanced Threat Detection

FortiSandbox is a key part of Fortinet's integrated and automated Advanced Threat Protection solution. Recommended by NSS Labs, FortiSandbox is designed to detect and analyze advanced attacks designed to bypass traditional security defenses. In independent NSS Labs testing, FortiSandbox demonstrated 97.3 percent breach detection effectiveness and due to Fortinet's unique multi-layered sandbox analysis approach, detected the majority of threats within one minute.

FortiSandbox, secured by FortiGuard, offers inspection of all protocols and functions in one appliance. It can integrate with your existing Fortinet infrastructure including FortiGate, FortiMail, and FortiClient, fueling a security ecosystem that automatically protects, learns, and improves your overall threat protection. It delivers highly effective protection against advanced persistent threats that is affordable as well as simple and flexible to deploy and manage. Complement your established defenses with this cutting-edge sandbox capability; analyzing files in a contained environment to identify previously unknown threats and uncovering the full attack lifecycle.

- Protects against advanced threats: Scans files on the network, in emails, in URLs, in network file share locations, and on-demand. Protects against advanced email threats, Windows threats, Office threats, zip threats, pdf threats, mobile threats, and more.
- Inspects across all Operating Environments: Code emulation examines and runs instruction sets to assess intended activity independent of operating environment for broader security coverage.

- Examines activity, rather than attributes: Executes objects within a secure virtual runtime environment ("sandbox") to analyze activity--system changes, exploit efforts, site visits, subsequent downloads, botnet communications, and more–to expose sophisticated threats.
- Pre-filters to deliver fast results: Leverages Fortinet's proactive anti-malware (consistently top-rated in VB100 RAP tests) and extended database as well as additional patented advanced threat intelligence techniques to detect a large percentage of advanced threats without the time and effort of full "sandboxing."
- Provides rich threat intelligence: Uncovers information related to the full threat lifecycle, not just initial code, to speed remediation. Trigger automated and manual response in other Fortinet products to mitigate incidents. Dynamically generate custom threat intelligence and distribute to supporting Fortinet products.
- Delivers Officially Licensed Microsoft Components: Product comes with Microsoft Windows, Internet Explorer, and Office embedded licenses, confirmed approved for use in virtual environments unlike other sandbox solutions.

Cooperative Network Security Across the Extended Enterprise

The Fortinet Security Fabric enables Fortinet Application Security products and those of third-party vendors to work together to boost security across core networks, remote devices and the cloud.

Fortinet Application Security products—including web application firewalls, secure email gateways, DDoS mitigation, and high-performance secure application acceleration—are all deeply integrated into the Fortinet Security Fabric for direct communications. This provides data center managers with an architecture that is secure, aware, actionable, scalable and open.

Secure: Fortinet Application Security products employ various combinations of FortiGuard Labs threat intelligence services to provide the latest protection from viruses, malicious sources, spam, web application attacks and Advanced Persistent Threats. The Fortinet Security Fabric distributes threat intelligence across the network of security devices.

Aware: Fortinet Application Security products are integrated via the Fabric with other Fortinet solutions to seamlessly share information between each other. The devices are deeply integrated with FortiGate appliances and, where applicable, also with FortiSandbox. Most Appliances offer centralized management and are tied to FortiAnalyzer for consolidated reporting and analytics. Additionally, most products offer user authentication support that can be tied into FortiGate or other authentication methods.

Actionable: This is the Fabric category that focuses on making sense out of it all to take action quickly, especially when any part of the network is under attack. All devices can be configured to alert IT staff of suspicious activity, or can take action by themselves to block threats. Centralized management and reporting via the single pane of glass helps security managers cut through the clutter to act on events in near real time. Automated tools and behavioral detection can augment human response times with granular policies to take actions immediately to minimize damages.

Scalable: Scalability is defined as both speed and expansion. Application Security offers some of Fortinet's highest performance devices including FortiWeb and FortiMail, with the fastest WAF and email security in the industry. We also offer high-performance ASIC-enhanced solutions for DDoS and ADCs with FortiDDoS and FortiADC. Each Fortinet product line provides models that span the needs of mid-market organizations all the way to large carriers and MSPs. In addition, FortiADC can be employed to expand capacities for other Fortinet products such as FortiMail, FortiCache and FortiGate.

Open: Finally, as mentioned above, Application Security is an open platform that integrates many third-party solutions, via their native APIs, including those from industry leaders such as IBM, HP and Verisign.

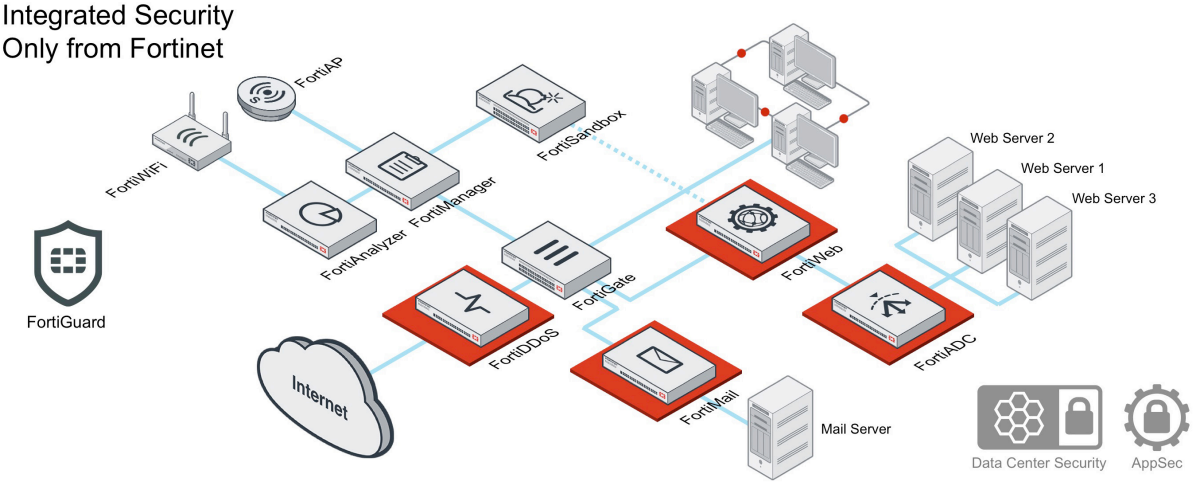
End-to-End, Integrated Application Security

Only Fortinet can offer the security, performance, and integration for a total network and application security platform that can meet the needs of your data center. Starting with the award-winning FortiGate NGFW as a foundation along with the Fortinet Security Fabric for network-wide communications, Fortinet offers the additional products and services you need to provide complete protection that goes beyond firewalls to protect your applications, users, and sensitive data.

No matter how complex your needs are, a comprehensive Fortinet security solution that includes WAF, DDoS, application delivery, email security, and sandbox integration is easy to setup and manage. We provide you the tools you need to centrally manage your Fortinet solutions and tools for consolidated threat analysis and reporting.

Fortinet Application Security

- One vendor
- Integrated Security
- Only from Fortinet



Fortinet products are designed to leverage and interoperate with other Fortinet devices and services via the Fortinet Security Fabric. We optimize and test our products to minimize bottlenecks to increase overall performance between platforms when used together in an enterprise data center environment.

Only Fortinet offers deep integration between our FortiGate, FortiWeb, FortiMail, and FortiSandbox platforms. Whether it's simplifying the setup of traffic routing to advanced ATP scanning with FortiSandbox, Fortinet makes it easy to deploy advanced application security in your network and closes the gaps common in point solutions.

Most of Fortinet's products support "single pane of glass" management and reporting through our FortiManager and FortiAnalyzer products. Unified under a single screen, operators get a complete picture of their Fortinet products for simplified management and complete visibility of incidents that span one or more Fortinet devices.

Finally, expertise matters. We are leaders in enterprise security technologies. Our trained pre-sales engineers can provide assistance in reviewing your advanced threat requirements and design solutions to meet the unique challenges of your organization. As a customer you have options for 24/7 support, on-site consulting, and other enterprise-class services offered by our award-winning FortiCare global customer support.

Summary

A firewall is your first line of network defense in your data center, however many new trends that target applications and end users require additional protections that a firewall or an IPS can't provide. Signature-based detection, IP reputation, and deep packet inspection can stop some of these advanced threats, but they are limited in what they can offer. Additional products like web application firewalls, DDoS attack mitigation appliances, sandboxing, email security gateways, and application delivery controllers are needed to address these new threats to your data center and users.

Fortinet offers a wide range of products to data center managers that not only complement our class-leading FortiGate firewalls, they also are designed to work together seamlessly in a complete network and application security protection framework. For more information on the products presented in this white paper, please visit Fortinet.com.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

May 16, 2016