

## *Fortinet's technology provides leading edge security in support of the Comprehensive National Cyber-security Initiative (CNCI)*

### **CNCI, TIC, and Networx Background:**

After numerous cyber attacks on several federal agency computer systems in the time period following 9/11, The White House determined that the government needed a more comprehensive strategy to defend government networks and sensitive information from hackers and nation states. On January 8, 2008, President Bush launched the Comprehensive National Cybersecurity Initiative (CNCI), by issuing National Security Presidential Directive 54.

The CNCI is the most thorough and far-reaching effort which the government has ever undertaken to improve the management and security of its IT infrastructure. As one of the 12 components of the CNCI, the Trusted Internet Connection (TIC) initiative was formalized in November 2007 with the goal of decreasing the number of connections that agencies had to external computer networks to 100 or less. Officials believe that the fewer connections agencies have to the Internet, the easier it will be for them to monitor and detect security incidents.

Under the TIC initiative, EVERY agency must either work with an approved MTIPS (Managed Trusted Internet Protocol Service) provider (AT&T, Sprint, Verizon, Qwest have been approved by GSA thus far) or be approved by The Department of Homeland Security to provide their own consolidated service by passing 51 requirements known as a TICAP (Trusted Internet Connection Access Provider). Currently, there are 96 agencies 'seeking service' through MTIPS providers and 20 agencies who have registered to become TICAPs.

The program contract vehicle for government agencies to pursue the TIC initiative is called Networx. Networx is the largest telecommunications program in the history of the federal government. It is the replacement for the previous contract vehicle known as FTS2001. It is divided into Networx Universal, with a ceiling of \$48.1 billion, and Networx Enterprise, with a \$20 billion cap. Both contracts are indefinite-delivery indefinite-quantity (IDIQ) with four-year base periods and two three-year options.

### **The Consolidation Imperative:**

The most fundamental aspect of the TIC initiative is consolidation. Driven by space, power, budget, security, and other constraints, consolidation has become both a tactical and strategic imperative for government IT and network defense professionals at all levels. The benefits of consolidation, whether physical or virtual, are well known: lower equipment and operations costs, less power consumption, improved manageability, and a better environmental footprint among them.

Most of the buzz about consolidation concentrates on its application to the data center as a whole, or to application servers in particular. But this focus overlooks an area where consolidation offers even more dramatic advantages: network security. The primary focus of consolidation with the TIC initiative is to increase security. Consider, in the case of application server consolidation, most of the benefits are in some sense peripheral to the fundamental task at hand: the delivery of application services. By contrast, consolidating network security with a unified platform delivers profound improvements in its ability to accomplish its fundamental task: managing the diverse range of threats that confront government networks.

Historically, there has been something of a rivalry of importance between antivirus and vulnerability researchers. Yet, as attacks become more complex and multi-modular, they demand a hybrid approach to threat research that combines these multiple disciplines. Just as enabling the various countermeasure modules in a consolidated solution to share knowledge makes its response to threats more effective, so too an integrated program of research and development across all threat types delivers more accurate countermeasures.

Consolidating network security also delivers notable cost benefits, another primary goal of the Networx program vehicle. According to Gartner, in 2008, the most important way information security organizations could save money would be to leverage the convergence of established security

functions into network- or host-based security platforms that provide multiple layers of security in a single product to protect against an evolving multitude of network and content threats.

## The Benefits of Virtualized Networking:

In order to effectively manage multiple agencies within a core backbone effectively and efficiently, the use of virtual networking will be a cornerstone of both MTIPS and TICAPs. Providing a separate physical infrastructure for every agency being provided service is simply not achievable. Virtual networking provides a method to consolidate multiple devices, such as those typically found in a data center or in a deployed tactical environment, in order to simplify and reduce physical hardware requirements. Implementing virtual networking technologies allows a single network device to transparently host multiple agency networks on a common infrastructure. Implementing Virtual Local Area Networks (VLANs) allow network links to be shared by virtualized servers to help improve network performance, reduce management complexity and enable more granular usage policies.

It is important to understand two aspects of virtual technology: virtual domains (VDMs) and virtual LANs (VLANs). VDMs enable a single infrastructure that provides routing and network protection for several agencies. This is useful for MTIPS/TICAP networks where each organization requires its own network interfaces (physical or virtual), routing requirements, and network protection rules. VLANs allow a single physical network link (or trunk) to support up to 4,096 virtual networks. Using virtual networks allow a trunk to support multiple agencies and applications while providing a method to manage traffic and network performance. Routing between VLANs and between VDMs adds more flexibility and scalability.

## Challenges and Requirements in Virtual Network Security:

The primary reasons for implementing VDMs and VLANs are to improve network manageability, scalability and security. Security solutions for virtual networks must allow management on a per-customer or per-application basis while ensuring availability of the control itself and the systems it protects. Also required is a high-performance security platform that is capable of scaling to support thousands of virtual networks with management, logging and reporting customized for each customer or application.

In a traditional virtualized model where software appliances are loaded as guest machines in a virtual infrastructure ensuring availability can be problematic. Ensuring that high volume attacks do not monopolize resources on one machine while starving others often becomes an issue. This can be managed through complex rules that cross functional boundaries between security and systems administration, but this confusion of ownership and custodial care serves to weaken, not enhance, security programs leveraging traditional virtual infrastructures. Complexity is the enemy of security, and with the dedicated nature of the Fortinet FortiGate® platform, such problems do not exist while maintaining robust virtualization specific to IA and seamlessly integrated in to traditional virtual infrastructures with greater security and decreased operational risk.

Three key requirements for virtual network security exist: manageability, scalability, and modular security. The solution must support the ability to manage multiple domains and multiple networks from a single device with domain specific administrative profiles for log data, reports, alerts, options and menus. Scalability is a key requirement as the performance to support thousands of VDMs and VLANs without impacting overall network throughput, specific users or applications. Lastly, modular security is imperative as not all security settings are appropriate for every agency/echelon being serviced. This requires a complete security suite where specific solutions can be applied on a per agency/domain/echelon or per application basis while providing a low cost of ownership.

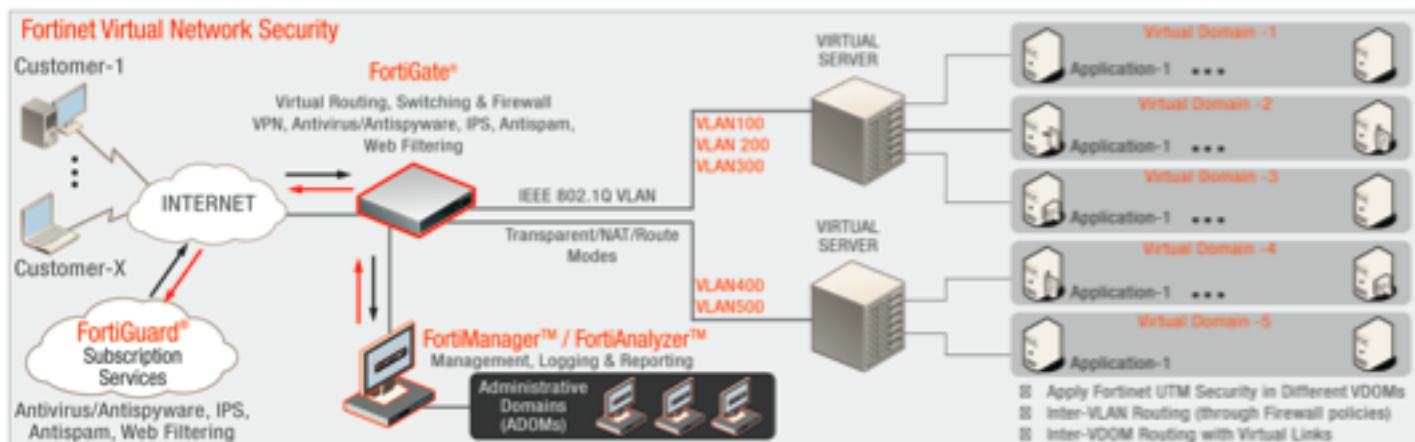


Figure 1 - Fortinet Virtual Network Security

## Fortinet's Next Generation Gateway Security Solution:

Fortinet is a leading provider of network security appliances and the leader of the unified threat management (UTM) market worldwide. Fortinet's award-winning portfolio of security gateways, subscription services, and complementary products delivers the highest level of network, content, and application security for enterprises of all sizes, managed service providers, government organizations and telecommunications carriers, while reducing total cost of ownership and providing a flexible, scalable path for expansion. Fortinet's flagship FortiGate security platforms offer a powerful

blend of ASIC-accelerated performance, integrated multi-threat response, and constantly-updated, in-depth threat intelligence. Employing innovative technologies for networking, security and content analysis, Fortinet systems integrate the industry's broadest suite of security technologies, including firewall, VPN, antivirus, intrusion detection/prevention (IDS/IPS), Web filtering, anti-spam, and traffic shaping; all of which can be deployed individually to complement legacy solutions or combined for a comprehensive threat management solution.

## Why Fortinet Provides ROI:

A key differentiator, Fortinet's custom-built FortiASIC™ content and network processors enable FortiGate systems to detect and eliminate even complex, blended threats in real time without degrading network performance. Fortinet provides an extensive set of complementary management, analysis, database and endpoint protection solutions which also increases deployment flexibility, assists in compliance with industry and government regulations, and reduces the operational costs of security management. Due to the accelerated performance of ASIC technology, typical layered defense techniques can be consolidated into one high-performance solution, allowing customers of all sizes to deploy less hardware than traditional solutions, saving money on both capital and operational expenditures.

## Proven IPv6 Technology:

The transition to IPv6 networks is not only being driven by the rapid consumption of the IPv4 address space but also the demand of new mobile IP devices/networks and emerging applications such as IPTV, voice-over-IP (VoIP), intelligent appliances, RFID-enabled services, and gaming. IPv6 is a viable solution for the required billions of new addresses. Corporations, governments and universities are responding to and beginning the transition to IPv6, however this will take many years to realize. Security will be critical during this transition and even more complex in pure IPv6 networks given the new addressing/routing capabilities, devices and applications. A solution is required today that secures IPv4 networks, enables secure IPv4 to IPv6 transition networks and is fully ready and easily evolves to support pure IPv6 networks.

The United States Government had set a mandate for all federal agencies to implement IPv6 networks by 2008. Obviously, this has not happened in total, as migrating from an IPv4 to IPv6 network can be complex. Ensuring consistent security is paramount to a successful migration to IPv6. Fortinet's family of FortiGate security platforms are IPv6 ready today and have proven interoperability via the JITC IPv6 certification. Fortinet's FortiOS™ security operating system and FortiASIC hardware acceleration processors are fully IPv6 compatible and support both "dual-stack" and "IPv4 tunneling" implementations with routing between physical and virtual interfaces. The FortiGate systems' industry-leading protection and performance secures the transition to IPv6.

## Common, Secure Operating System—FortiOS:

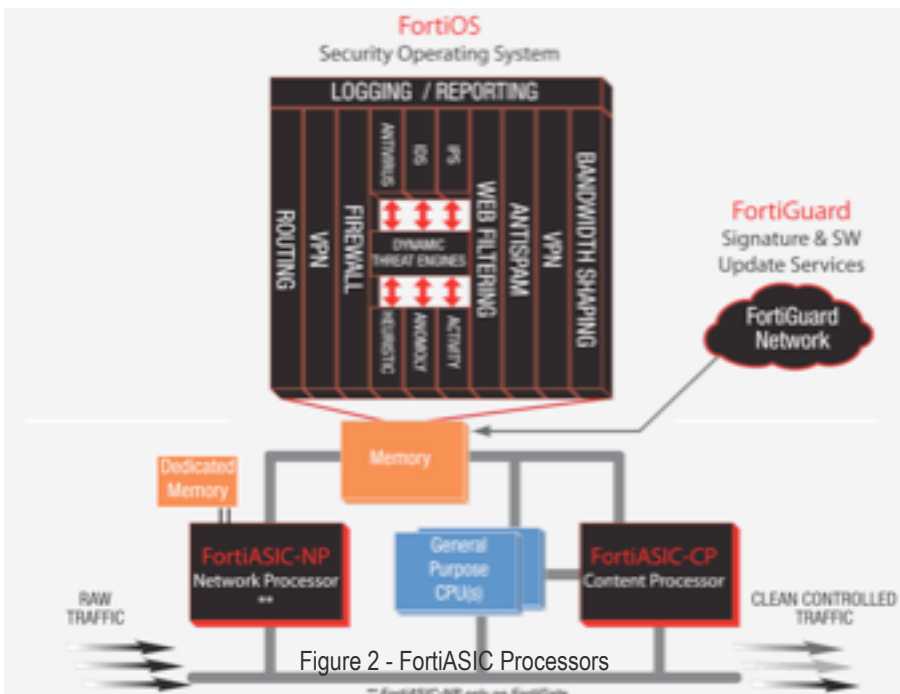
FortiOS is a security-hardened, purpose-built operating system that is the foundation of the FortiGate multi-threat network security platforms. Leveraging the hardware acceleration provided by the FortiASIC content and network processors, FortiOS enables real-time content inspection, as well as signature and heuristic packet scanning for advanced threat protection. Ongoing updates from the FortiGuard® Network ensure that security subscription services and the FortiOS operating system are always up to date and providing a complete Unified Threat Management solution.

Federal government organizations can now benefit from an integrated solution that offers a comprehensive suite of security services – content inspection firewall, VPN, IPS, antivirus, Web filtering, Antispam, IM/P2P, and integrated bandwidth shaping. FortiOS employs an integrated policy engine that enforces granular security policies including web filtering and full content scanning for instant messaging, support for P2P rate limiting and SSL-VPN.

The security of FortiGate appliances themselves is critical. FortiOS is pre-hardened and does not include any third-party applications. FortiOS has been built from the ground up to deliver security services at the highest levels of performance and is certified for Common Criteria EAL 4+, FIPS 140-2 Level 2, and has been submitted for NIAP's Common Criteria Medium Robustness 3.0 program.

## Performance and Scalability:

FortiGate platforms are based on an integrated hardware and software architecture specifically designed for high-performance application-level content processing in perimeter, core and data center networks to provide real-time security functions at multi-Gbps data rates. The FortiASIC Content Processor (CP) is a key component in all FortiGate security platforms providing a hardware scanning



engine, hardware encryption, and real-time content analysis processing capabilities. The FortiASIC Network Processor (NP) series of processors provides acceleration for firewall, encryption / decryption, signature and heuristic packet scanning, and bandwidth shaping. FortiOS security services can be selectively enabled to provide a unique set of services or a full suite of UTM security services all within a single platform. The FortiGuard network dynamically updates system software and security services such as antivirus, antispam, Web filtering, antispayware, and intrusion prevention to ensure the maximum level of protection is being provided.

## **High Availability:**

FortiGate high availability (HA) provides a solution for two key requirements of critical enterprise networking components: enhanced reliability and increased performance. FortiGate HA is implemented by configuring two or more FortiGate units to operate as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewalling, VPN, IPS, virus scanning, web filtering, and spam filtering services.

FortiGate HA can be configured as either Active-Passive (failover protection) or Active-Active (load balancing and failover protection), depending on the needs of the organization.

## **Centralized Management:**

FortiOS is tightly integrated with the Fortinet FortiManager™ and FortiAnalyzer™ systems to provide centralized management, reporting and analysis of network traffic and threats.

The FortiManager family of appliances supply the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances and end-point security agents. The appliances provide centralized policy-based provisioning, configuration, and update management for FortiGate, FortiWiFi™, and FortiMail™ appliances, as well as FortiClient™ end point security agents. They also offer end-to-end network monitoring for added control. FortiManager delivers a lower TCO for Fortinet implementations by minimizing both initial deployment costs and ongoing operating expenses. Managers can control administrative access and simplify policy deployment using role-based administration to define user privileges for specific management domains and functions by aggregating collections of Fortinet appliances and agents into independent management domains. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize Web filtering rating request response time and maximize network protection.

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout a network. It provides organizations of any size with centralized security event analysis, forensic research, reporting, content archiving, data-mining, malicious file quarantining and vulnerability assessment. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet appliances and third-party devices deliver a simplified, consolidated view of your security posture. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns that can be used to fine tune the security policy, thwarting future attackers. In addition, FortiAnalyzer platforms provide detailed data capture that can be used for forensic purposes to comply with regulations and policies regarding privacy and disclosure of information security breaches.

## **Accelerated Content Analysis:**

Fortinet's gateway architecture takes advantage of a specialized hardware architecture to accurately and quickly detect malicious content without sacrificing the security or performance of the network. Using deep file analysis and proxy-based application engines, the FortiGate appliances subject files to multiple layers of content, protocol, and heuristic analysis allowing the system to detect even the most sophisticated polymorphic malware. To add further detection accuracy, the proxy approach allows FortiGate systems to counteract evasion techniques by unpacking and decrypting files prior to inspection. This is essential inasmuch as files are often "packed" and encrypted intentionally to evade stream-based detection methods.

For example, hackers, being aware of the operation of stream-based methods, deliberately "pack" their malware to evade detection from stream-based scanners. Packing files refers to a method that compresses or archives files in formats such as UPX, gzip, ZIP and RAR. Used legitimately by Web applications, Web servers commonly compress files for faster delivery of content across the Internet. Once the file is received by the browser it automatically decompresses the file for display or execution.

Most stream-based AV engines offer limited support of packers, as having to buffer and reassemble all packets that make up a file, and then having to unpack the files often negates the performance gains. In a recent report published from Microsoft more than half of new malware discovered in the wild are packed for evasion and obfuscation reasons. The fact that many stream-based engines have limited support for packing routines means that deploying a stream-based AV gateway potentially means greater than 50 percent of the most active malware could flow into a network undetected—creating a significant security gap in gateway defenses that puts users at a higher risk of becoming infected.

## **Secure Email:**

Email is one of the most predominant communication methods. Unfortunately, email has also become one of the most common vehicles for proliferating blended threats comprised of viruses, worms, spyware and spam. These blended attacks can negatively impact productivity, cause system downtime, lead to identity theft, and potential leakage of sensitive data like operational mission status. In response, organizations have leveraged point product security technologies, such as antispam, to patch against single threaded attacks. In addition, legislation has been introduced to ensure that organizations comply with security best practices for email archiving that enable forensic and legal audits. Email is a mission critical application for all users that must be secured.

For this reason, secure email is one of the services that can be requested from a service provider in an MTIPS deployment, and should certainly be a consideration for those agencies looking to provide TICAP services.

FortiMail is a specialized email security system that provides multi-layered protection against blended threats comprised of spam, viruses, worms and spyware. The FortiMail system relies on a customized operating system that cleans emails through corresponding FortiMail antispam, antivirus and antispymware engines. To ensure up to date email protection, FortiMail relies on Fortinet FortiGuard antivirus, antispymware and antispam security subscription services that are powered by a worldwide 24x7 Global Threat Research Team. FortiMail provides unparalleled deployment flexibility and powerful bi-directional email routing, Quality of Service (QoS), virtualization and archiving capabilities with a lower total cost of ownership.

## **FortiGuard:**

The Fortinet FortiGuard Security Subscription Service provides comprehensive antivirus, antispymware, antispam, intrusion prevention and Web content filtering capabilities to enable protection against blended threats. FortiGuard services are continuously updated by a 24x7 Global Threat Research Team possessing in-depth expertise in all security disciplines. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security knowledge and provide true zero-day protection from new and emerging threats. FortiGuard services updates are delivered via a global distribution network to FortiGate®, FortiMail, FortiClient PC and FortiClient Mobile products. This means administrators spend less time keeping defenses up-to-date with the latest knowledge base of viruses, spyware, worms, vulnerabilities, exploits, spam and dangerous web content sites.

This is very important in today's zero-day threat environment. By possessing a world-class threat research team and global distribution network, Fortinet's customers do not have to rely on third-party OEM integration before threat mitigation techniques are released. For US Federal customers, the FortiGate and FortiManager platforms can be easily configured to only pull updates from CONUS distribution servers.

## **The Benefits of using Fortinet for TIC deployments (MTIPS and TICAPS):**

Securing government networks is a prime objective of the TIC initiative. By consolidating the connections to the internet the government will be able to provide better oversight and correlation and ensure that all connections will be monitored for better a better security posture. Fortinet is the best positioned company in the industry when it comes to providing the comprehensive set of capabilities needed for the TIC initiative. By providing a high-performance, scalable, consolidated security solution Fortinet is uniquely capable to assist the US Federal government in realizing the goals of the TIC initiative in support of the Comprehensive National Cybersecurity Initiative.

## Why Fortinet Makes Sense for TIC/MTIPS/TICAPS

<b>ROI</b>	The performance capabilities of the FortiGate consolidated network security solution, powered by custom designed ASIC technology, enables organizations to deploy less hardware, cover more threats in an integrated fashion, and virtualize policies distinctly or similarly across domains. Furthermore, since Fortinet does not charge for subscription services on a per-user basis, all threat mitigation techniques are licensed per appliance, saving organizations substantially on operational expenditures.
<b>Proven IPv6 Technology</b>	Fortinet's FortiOS security operating system and FortiASIC hardware acceleration processors are fully IPv6 compatible and support both "dual-stack" and "IPv4 tunneling" implementations with routing between physical and virtual interfaces.
<b>FortiOS</b>	The Common, Secure Operating System—FortiOS is a security-hardened, purpose-built operating system that is the foundation of the FortiGate multi-threat network security platforms. FortiOS has been built from the ground up to deliver security services at the highest levels of performance and is certified for Common Criteria EAL 4+, FIPS 140-2 Level 2, and has been submitted for NIAP's Common Criteria Medium Robustness 3.0 program, the first vendor to do so.
<b>Performance and Scalability</b>	FortiGate platforms are based on an integrated hardware and software architecture, accelerated with custom designed ASIC technology, specifically designed for high-performance application-level content processing in perimeter, core and data center networks to provide real-time security functions at multi-Gbps data rates.
<b>Centralized Management</b>	FortiOS is tightly integrated with the Fortinet FortiManager and FortiAnalyzer systems to provide centralized management, reporting and analysis of network traffic and threats.
<b>Accelerated Content Analysis</b>	By using emulation routines, the FortiGate architecture requires just one signature to detect a polymorphic virus. As files are reassembled and analyzed, if the body is found to be encrypted, the FortiGate will emulate execution of the file to the point where the once encrypted code is decrypted and exposed for analysis. In this case, regardless of the file structure changes in the variants, only the signature of the exposed file needs to be checked, removing the need to write a signature for each variant.
<b>Email Security</b>	FortiMail is a specialized email security system that provides industry-leading multi-layered protection against blended threats comprised of spam, viruses, worms and spyware.
<b>FortiGuard Threat Management Services</b>	The Fortinet FortiGuard Security Subscription Service provides comprehensive antivirus, antispam, intrusion prevention and Web content filtering capabilities to enable protection against blended threats, licensed on a per-appliance basis.

### About Fortinet:

Fortinet is a US-based manufacturer of network security appliances and a leader in Unified Security Threat Management. Fortinet offers a broad breadth of security solutions for network cloud and enterprise based applications. The FortiGate and FortiMail solutions make up a large part of the Network MTIPS providers security architecture. The Fortinet Federal team is located in Herndon, VA.



### Contact:

Jeff Lake  
 Vice President, Federal Operations  
 Fortinet, Inc.  
 13221 Woodland Park Road  
 Suite 110  
 Herndon, VA 20171  
 Email: [jlake@fortinet.com](mailto:jlake@fortinet.com)  
 Phone: 703-709-5011  
[federalsales@fortinet.com](mailto:federalsales@fortinet.com)

Copyright© 2009 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.