Exploring IMS Network Security for Next Generation Network (NGN) Carriers

White Paper

High Performance Multi-threat Security Solutions

FORTINET™

The New Telecom Revolution

The telecom industry has entered a phase of revolutionary change as Internet technologies are enabling a new era of multimedia services that are dramatically changing business models.

New multimedia services are driving explosive new revenue growth while the use of open systems Internet-based technologies are dramatically reducing capital and operating costs.

These are exciting opportunities yet they also present daunting challenges for telecom carriers. Time-to-market, competitive differentiation, customer satisfaction and cost control become increasingly critical to subscriber retention, control of the value / revenue chain and ultimately business success.

The Technology Evolution

Internet, or Internet Protocol (IP), technology is the catalyst of change driving the telecom revolution in the following, fundamentally important, areas:

- Network Infrastructure
- Open System Platforms
- Broadband Multimedia Applications & Services

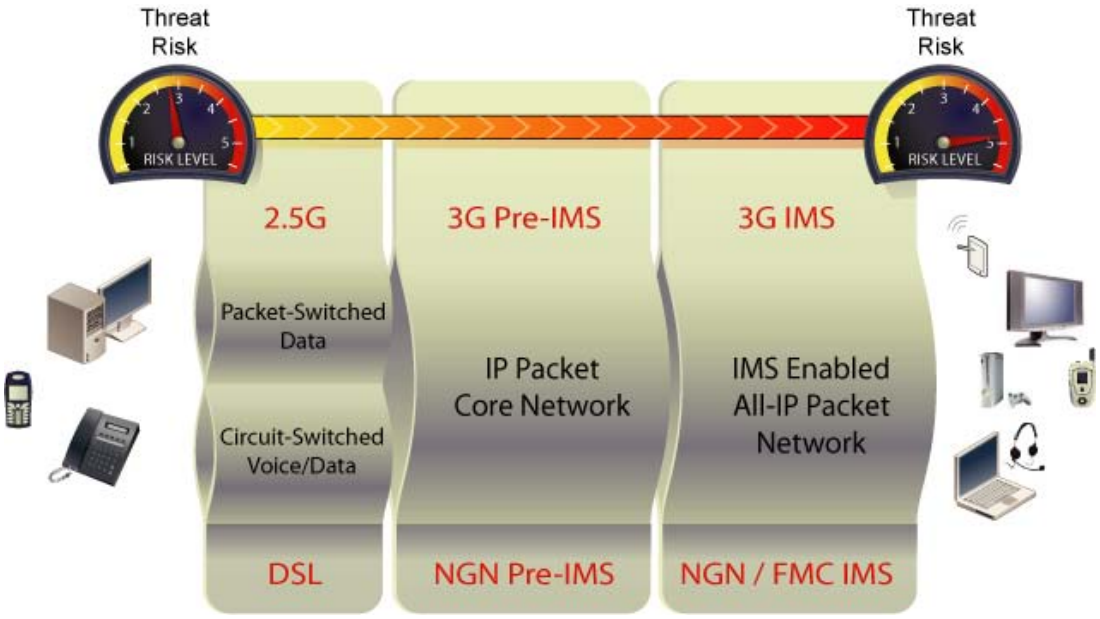
Carrier ***network infrastructure*** is undergoing a dramatic, yet evolutionary change, from a circuit-switched to a packet-switched architecture, utilizing IP technology for service delivery. The increased efficiencies of IP technology enable networks delivering much greater capacity and higher performance which thereby reduces capital costs.

The network infrastructure evolution to IP technology has in turn driven the deployment of ***open system platforms***. Carriers are able to leverage much greater economies of scale and negotiating power to reduce capital equipment costs (versus vendor proprietary systems) while accelerating time-to-market for new services development / deployment through the use of industry standard tools.

Now possible are ***broadband multimedia applications & services*** that allow carriers to offer new high-value services. Multimedia messaging, video, games, music and many new multimedia services are increasingly important competitive differentiators that are significantly increasing the ARPU (Average Revenue per User) beyond toady's voice services and boosting business profitability to new levels.

IMS, or IP Multimedia Subsystem, is the glue that binds the network infrastructure and open system platforms together allowing carriers to quickly and cost-effectively deliver new broadband multimedia applications and services.

Figure 1: Evolution to the IMS Enabled All-IP Network

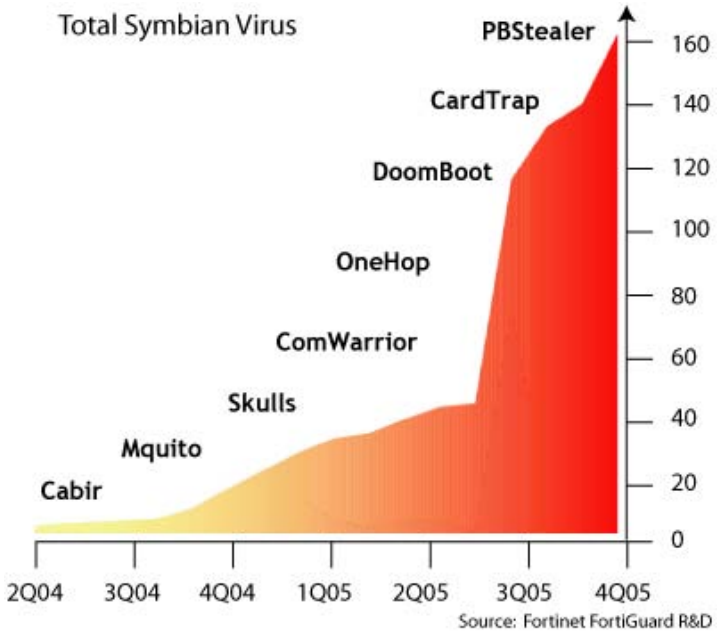


The Business Risk

However, new market opportunities aren't achieved without some degree of increased risk. As a result of the move to IP-based open systems architecture, telecom carriers face an array of new security threats and operational challenges that directly impact the business. Generally speaking however these challenges fall into two main categories:

- **Cyber-Risks** – which are technical threats to the open standards model taking place at the Application, Control and Transport layers of the infrastructure, and
- **Criminal Incentive** – attempts to defraud either subscribers and/or carriers in an effort to obtain monetary gain, notoriety, or credibility with their criminal peers.

Figure 2: Increase in Cyber Threats to Wireless Networks



One example as shown in Figure 2, illustrates the increasing prevalence of security threats and cyber crime in wireless networks as new multimedia subscriber terminals become available and cyber criminals and hackers learn about the technical vulnerabilities and exploit them. Due to these security risks and the business impact, securing the new IP-based network at all levels is now a key objective as carriers strive to maximize business success and profitability.

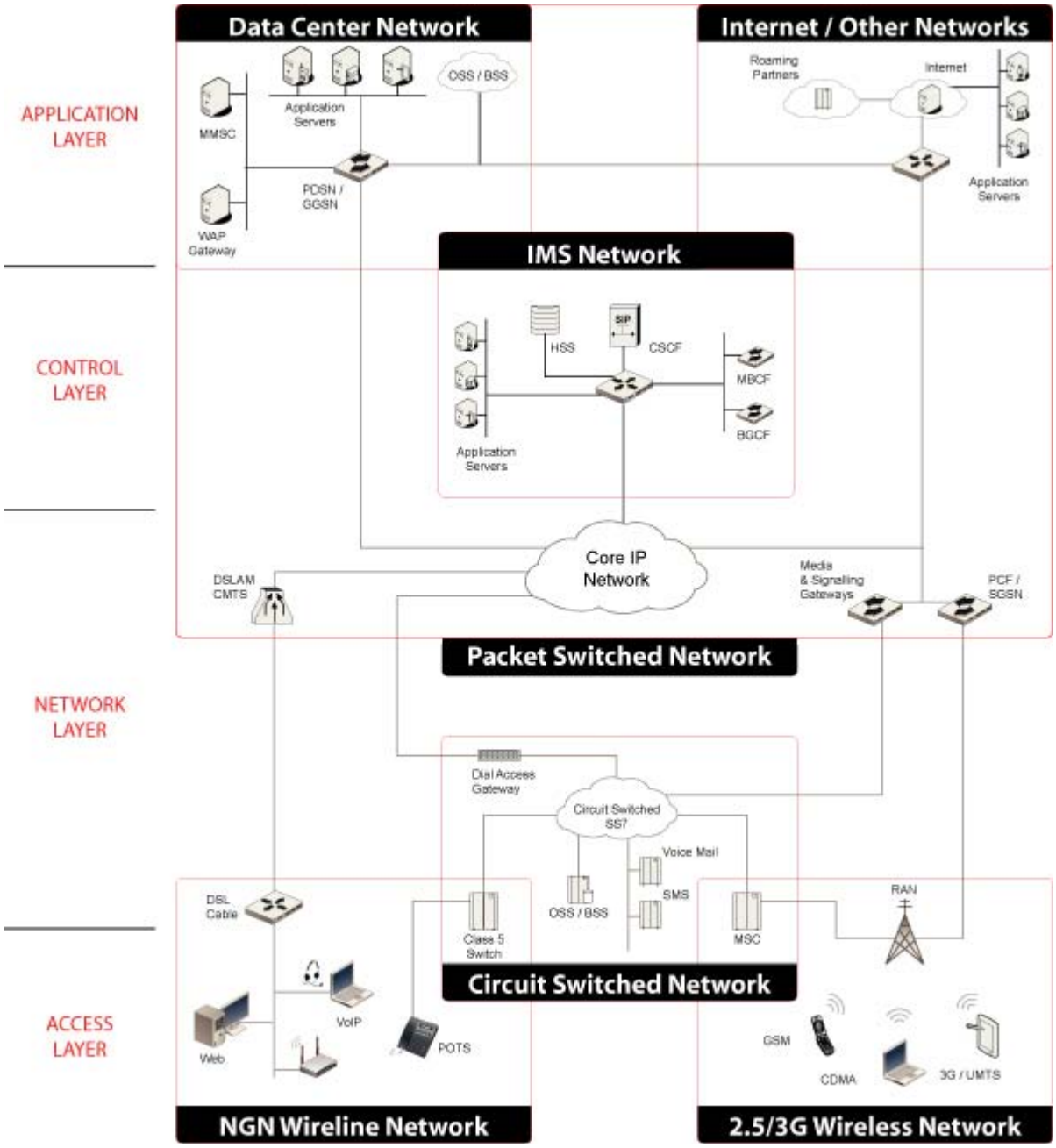
Understanding IMS Technology

At the heart of this strategy is IMS. IMS enables the convergence of voice, data, and multimedia services such as Voice over IP (VoIP), Video over IP, push-to-talk, presence or instant messaging services. While there are number of protocols used within an IMS network – such as HTTP and SMTP — the most important and prevalent one is called SIP, or Session Initiation Protocol. IMS uses SIP because it provides an easier and more open method to set up and control rich media applications over an IP network. SIP provides a pathway to build a single unified network, bridging the gap that previously existed between the once-separated Telecom and Internet worlds.

IMS is comprised of four separate layers that work together to enable rich media services (see Figure 3 below):

- **The Application Service Layer** – where IMS applications are hosted, such as Push-to-Talk, Instant Messaging, VoIP, Video on Demand, etc.
- **The Control Layer –** SIP / H.323 control functions for application access, user and service administration, billing and other functions.
- **The Transport Layer –** provides network / inter-network connectivity
- **The Access Layer –** subscriber access network for devices such as DSL modems or mobile 3G handsets

Figure 3: The Layers of the IMS Network Model



Understanding the Risks to IMS Networks

Due to the recent and ongoing development of IMS and inherent use of SIP, IMS networks have built-in operational challenges that make them very vulnerable to attacks. To some extent such vulnerabilities can be taken into consideration as networks are designed, however, a certain level of uncertainty remains on best practices for effectively securing an IMS infrastructure. Therefore it becomes increasingly important to understand that security must be enabled at every level of the network model, as well as at the end point, or subscriber device. The various types of threats that increase the risk for a security breach or attack and that can occur at each layer within the IMS Network Model include:

- **Risks to the Application Service Layer:** Since applications are typically hosted on networked servers running conventional operating systems, they are vulnerable to the same type of threats as enterprise businesses experience. For example, a "Push-to-Talk" application running on a Linux-based server, or an Instant Messaging or VoIP Call Management application on a Windows-based server are all vulnerable to the same threats as their enterprise counterparts experience on a daily basis, such as a Denial of Service (DoS) intrusions, viruses, or worms proliferation that ultimately can impact uptime and cost carriers service revenue.

  An inability to effectively address specific security issues in the Application Layer limits a carrier's ability to provide enhanced services to customers. By holding back services until the application can be fully secured, carriers are limiting revenue-generating opportunities, and providing competitors the opportunity to be the first to offer services, convert customers and build competitive advantage.

- **Risks to the Control Layer:** The SIP protocol is managed in the Control Layer where there are specific types of attacks that can be launched against SIP elements in the IMS network. Any device that uses IP to communicate with the IMS network can send traffic to this layer and launch an attack. Some examples of these types of attacks that can impact the Control Layer include:

  - *Message Floods* - which are caused by a device sending an unauthorized amount of specific SIP messages. An example of a message flood is an INVITE flood which is the SIP method that instructs a telephone on a VoIP network to ring. Each SIP invitation consumes a certain amount of network resources. Another misuse of this message would be sending a large number of SIP INVITE messages causing many phones on the network to constantly ring.

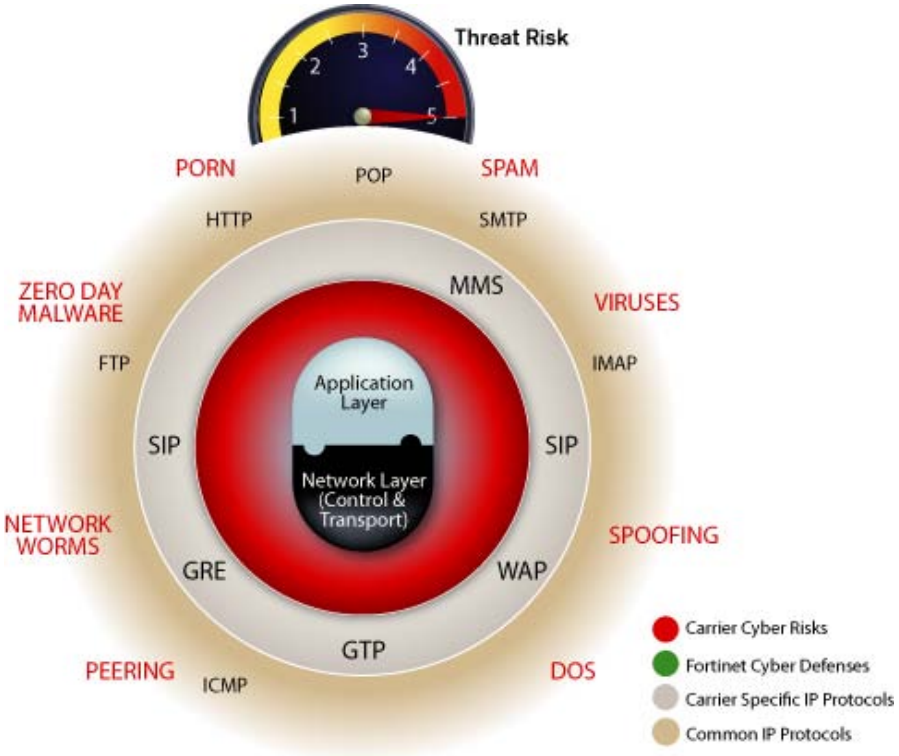
  - *Registration Floods* – that use the SIP registration method, which is a request for use on the network. The Control Layer must register and authenticate all end points on the network and also must limit the rate of incoming registrations. An unauthorized Registration Flood sends an unlimited number of requests to the server, consuming all of the server resources and causing the server to potentially crash and impacting service availability.

- **Risks to the Transport Layer:** One of the most common risks to the Transport Layer is from a flood of data packets that consume a network's entire bandwidth and cause it to perform poorly. This type of flood can occur using any of the available network protocols such as a TCP Flood (also known as a SYN Flood) or a UDP Flood, among several others. When one of these floods occurs at the Transport Layer, it prevents a resource from responding appropriately, resulting in a Denial of Service (DoS) which, in turn, brings down the network and impacts service availability.

  Another example of an attack to the Transport Layer is an Over Billing Attack in the case of a GPRS enabled network, where a hacker uses the GTP protocol to hijack another user's network session after they have disconnected, causing the victim to incur all of the charges caused by the hacker's misuse.

The wide variety and nature of security threats that are aimed at each layer of an IMS network demonstrates the magnitude of the problems associated with network security today. The chart in Figure 4 on the next page, illustrates the various security threats that target each network layer, and points out the importance of deploying a robust security solution to protect the entire IMS network infrastructure.

Figure 4: The Threats against Each IMS Network Layer



- **Risks to the Access Layer** – Personal computers and new "smartphone" mobile devices (such as Symbian OS™, Microsoft Windows Mobile™), are key network entry points for security threats which, once connected, allow a hacker to propagate infection to other endpoints on the IMS network .

  While the security risks to personal computers are well recognized the risk to wireless smartphones is not well understood, these devices are now the targets of similar threats as their desktop or notebook counterparts. This includes threats such as viruses, worms, Trojan horses, Adware, Spyware and spam. For example with a PDA that can receive e-mail messages, the same attachments that are the harbingers of an attack to a PC, can also cause a similar amount of damage on a smart cellular phone or PDA. In fact, there are already new threats to these devices, specifically viruses which attach themselves to messages sent via the MMS protocol.

  In particular for wireless carriers such threats become extremely damaging as subscribers have limited abilities to take the kind of action to rid their mobile device of the problem as they would on their desktop or notebook PC. Therefore, if there is an attack to a smartphone, it becomes the responsibility of the *wireless carrier* to fix the problem or, more importantly, to re-engineer both the device and the network to prevent attacks from occurring before they can cause extensive damage to the carrier subscriber population and have an adverse impact on the carriers business model.

IMS Operational Infrastructure Requirements

Besides securing the network from external threats, wireless and wireline carriers also have to consider the implications of putting more data on their networks internally. In the past, telecom carriers segmented their network infrastructure into several independent networks based on data type. The networks handling voice traffic were specifically designed and dedicated to that function, as were the networks handling data traffic. This allowed carrier administrators to effectively manage and make changes to each of the networks, taking into consideration each network's unique attributes.

With previously independent networks now converging onto a single, packet-based IMS network standard that is designed to handle a variety of data types, network throughput must be able to handle the increased traffic and demands that are associated with it. As a result, IMS networks call for a completely different traffic capacity plan than in the past. The issues that these new plans must address include provisions for higher throughput, increasing the number of sessions, and providing a larger number of connections per second.

Throughput and Scalability

When telecom carriers are building an IMS network, they need to deploy network and/or security components that can scale to a level that will meet the capacity demands of the network. In addition, scalability requirements must also meet the number of concurrent and/or simultaneous connections that will support the network's entire subscriber base.

Take text messaging for example, a feature that is common with most wireless carriers today. Networks that carry text messages process a large number of short-lived data transactions. With large carriers, it is not uncommon to find networks that are handling millions of simultaneous connections. The types of network requirements necessary to handle this kind of capacity are very different from those associated with merely surfing the Internet, such as those found with wireline DSL networks. Therefore, any device on an IMS network must be able to scale up in order to meet the requirements associated with higher network throughputs. Also imagine now processing voice calls (VOIP) on this same data network when it was previously on a separate voice only network.

In addition, wireless and wireline carriers need to have provisions for future growth to accommodate tomorrow's customer application needs. When new capabilities become available — such as real-time wireless video that allows a user to have a live video conference with another caller — the existing networks that were previously capable of handling standard web traffic by leveraging some type of packet based overlay network will not be able to scale to the levels necessary to handle these new forms of media at an equivalent performance level.

Therefore telecom carriers need to ensure that any changes they make to their networks not only satisfy today's needs, but provide an opportunity for growth to meet tomorrow's needs as well. This strategy isn't isolated to applications, but must be applied to security issues as well. For example, if the existing security components deployed across the network cannot analyze millions of text or video sessions per second, and also spot security threats as they occur, then that security solution will not meet the needs of a next-generation IMS network.

Quality, Availability and Redundancy

Customer satisfaction and retention are directly related to the quality, consistent uptime and consistent availability of new services. If, for example, the quality of a VoIP service results in frequently dropped calls or poor audio quality, customers will discontinue the service and the carrier will lose money. Therefore, it is critical that the quality of any new service be superior, or at least equal to if not better than the quality of services offered on older technologies.

To provide consistent availability, telecom carriers must build redundancy into their network plans so that there are several levels of backup available. Ensuring availability of service through redundancy is

essential in the event that an individual network component fails, or there is a security breach, or in the event of a natural disaster that results in disruption of service.

Telecom carriers need to be selective in choosing vendors that offer equipment specifically designed to accommodate high availability requirements. To ensure minimal disruption for users on the network, each device must be able to communicate with all other devices on the network so that traffic can automatically be re-routed through a backup device in the event of a problem.

Effective Management

Effective management is also essential under the new requirements associated with an IMS network. Good network management is all about adaptability and responsiveness in order to quickly, effectively and efficiently address changes in the network environment. For example, in the event there is a security threat to the network, management must have the tools that allow them to react quickly to eliminate the threat. Effective management also means being able to respond to changes from a central location as the changes occur, without having to deploy a slower, manual process such as initiating a team of system engineers to physically analyze or remedy the problem.

Flexibility

Another requirement necessary for designing an effective IMS network is flexibility. Networks with open standards also open up greater possibilities for security attacks such as viruses, network intrusions and worms. Enabling network administrators with the ability to create and adjust policies on the fly means providing a greater degree of flexibility to respond to attacks as they occur. For example, if a new virus or intrusion is detected, administrators must have the tools on hand that provide the flexibility and agility to deploy solutions at the moment they are needed in order to thwart a security breach or attack.

Standards Supported Hardware Design

The ability to attain and maintain an IMS network is also a function of choosing hardware components and technologies with a superior design. Advanced Telecom Computing Architecture (ATCA) is a modular platform standard that can be incorporated into carrier networks, and enables flexible, carrier-grade convergent systems.

With ATCA, IMS network administrators are able to mix diverse network hardware components for each layer of the IMS model — such as an application server blade, a transport-oriented GPRS (General Packet Radio Service) blade, and a control-oriented SIP signaling gateway —all within the same chassis. This degree of flexibility is something that was never attainable with older closed, circuit-switched proprietary hardware manufacturers.

This modular approach enables equipment manufacturers to employ the same chassis/backplane for multiple products, providing the flexibility that telecom carriers require to address the technical challenges of managing all the layers involved in an open standards-based IMS network.

The Fortinet Solution for IMS Networks

FortiGate™ 5000 ATCA Multiservices Security Gateway Solution

The *FortiGate* 5000 series ATCA-based platforms are carrier-grade network security solutions that are enabled by the modular *FortiGate OS*™ distributed software system. The FortiGate 5000 provides scalable, multi-gigabit capacities that meet the most stringent carrier requirements for security, performance, reliability and availability. Fully redundant configurations are available that eliminate any single-point of failure while providing automatic fail-over modes to ensure continuous service.

The FortiGate 5000 Series solutions fulfill the promise of effectively securing IMS networks in the following ways:

- **Providing a Robust Security Platform**
- **Supporting a ATCA Standards-based Hardware Chassis and Server Blade Design**
- **Ensuring Network Performance and Service Integrity**
- **Ensuring Effective Management and Analysis**
- **Providing Flexible IMS Security Deployment**

A Robust Security Platform:

All FortiGate solutions, including the 5000 series, provide a *single source* solution for telecom carriers seeking to secure their IMS network in the most effective way possible. Traditional network security solutions involve the procurement of a variety of hardware, software and security subscription services from several vendors for each layer of the network model, which in turn requires an additional expense for each layer of desired security.

FortiGate Security Platform solutions simplify this process by providing a cohesive and integrated strategy of hardware, software and subscription services that works together to form a highly secure solution protecting each layer within the IMS network. The first two components of this integrated solution are: *Targeted Security Modules, and Updated Security Subscription Services.*

Component #1: Targeted Security Modules

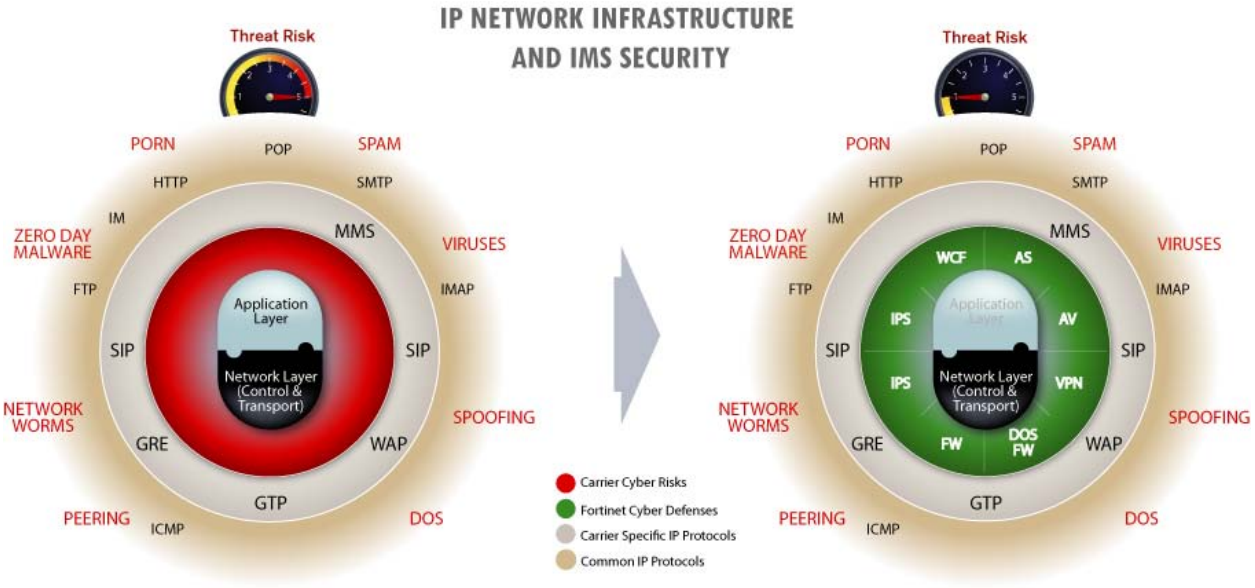
As part of the FortiGate 5000 solution, Fortinet offers an extensive array of security modules that are designed to defending the network against of the unique threats that target the individual layers of the IMS network. A list of these security modules and the type of threat that they provide protection for are listed in Figure 5 below:

Figure 5: FortiGate Security Modules Target Specific Network Layer Risks

Security Modules	IMS Risks
Application Layer	
Anti-Virus	Viruses, Spyware, Keyloggers, Trojan Horses and Malware/Greyware
Web Content Filtering	Inappropriate Web Content inclusive but not limited to porn, phishing and web sites that proliferate viruses
Anti-Spam	DHA (Directory Harvest Attacks), Spam
Application Protocols	Application protocols inclusive but not limited to HTTP, FTP, Telnet and other commonly used applications and services
Control Layer	
SIP IPS	SIP Specific Protocol Intrusions
Transport Layer	
Firewall	Topology Hiding/NAT, Network Policy Violations, Peering Enforcement
Virtual Private Network	Illegal IP Traffic Capture

With the deployment of targeted security modules, a protective shield is formed that diminished the security threats against the layers of the IMS network, leading to a fully protected network infrastructure, as illustrated in Figure 5 below.

Figure 5: Targeted Modules Provide IMS Network Layer Protection



Component #2: Updated Security Subscription Services

With the deployment of FortiGate Security Modules, the *FortiGuard™ Center* (the security subscription service for FortiGate products) provides a comprehensive source of information and software updates that are automatically pushed down to each of the security components that have been enabled by the

carrier administrator, ensuring that each module is running with the most updated security descriptions at any point in time. This provides automatic configuration on a real-time basis and assures network administrators that they will always be working with the most current security knowledge available to thwart any potential security risks to the network.

The FortiGuard Center updates are updated in real-time from the Fortinet global database to a locally hosted service provider database. This hierarchical architecture enables service providers to flexibly customize their protection configuration while maximizing performance, ensuring security, and sustaining highly effective service levels. With FortiGuard Center, carriers gain the following advantages:

- Automated Updates – Keeps defenses up-to-date with the latest viruses, Spyware, & heuristic engines.
- Industry Leading Threat Response Time – Fortinet beats the competition, offering signature updates to block the latest attacks.
- Proactive Threat Library – Protection from thousands of popular OS and application threats and vulnerabilities.
- 24x7 Worldwide Coverage – Over 50 distribution servers are deployed in 12 different countries around the globe.
- Per Device Subscription Services – Significantly lowers subscription costs versus traditional per user licensing models.

Fortinet's security subscription services are also created, updated and managed by a global team of Fortinet security professionals working around-the-clock, seven days-a-week to ensure that the latest threats are detected and blocked before they can harm your network. This team constantly mines the Internet for new and emerging threats and creates the security counter-measures that protect IMS networks against these threats.

With the combination of FortiGuard's Targeted Security Modules and Updated Security Subscription Services, Fortinet provides the fastest response times for providing new security updates in the industry. These software components work in conjunction with FortiGate ATCA-compatible server blade hardware, to form a complete integrated solution to ensure a robust IMS security platform.

ATCA Standards-based Hardware Chassis and Server Blades

Besides an effective software and update subscription strategy, telecom carriers must also ensure that each security device and module throughout the network adheres to a single and rigid hardware standard that supports one uniform platform. Today, that standard is ATCA, which has gained widespread acceptance due to the flexible functionality it provides to network administrators. By deploying ATCA-compliant hardware devices, administrators can mix and match different components with the assurance that each device will maintain a familiar degree of consistent functionality across the network wherever those devices are deployed.

Supporting each FortiGate ATCA hardware blade is the *FortiGate OS*™, which enables each FortiGate security software module, empowering telecom carriers with a choice of the exact security solution that best fits the individual needs of their network, whether at the Application, Control, or Transport Layer, or any combination thereof. The FortiGate security platform approach provides assurance that the entire network infrastructure will remain highly secure.

To date, Fortinet is the only IMS network security provider that supports the ATCA standard for all of its hardware devices, providing administrators with the flexibility and control they are seeking to support their existing network security strategies.

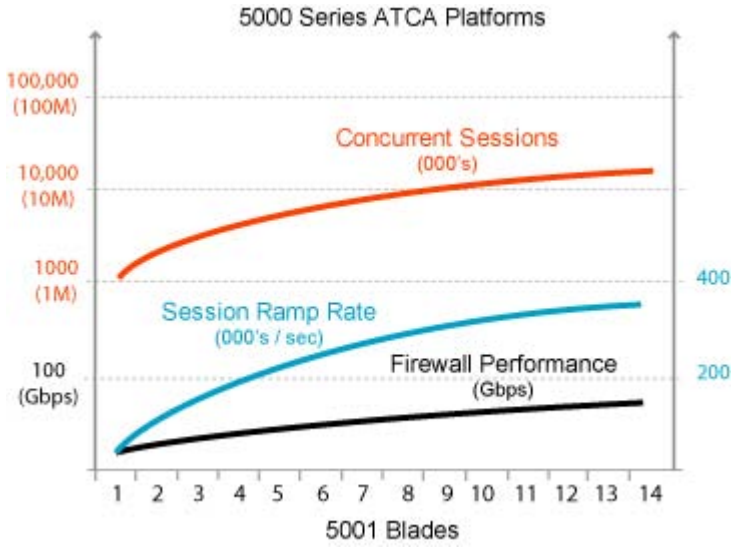
Ensures Network Performance and Service Integrity

To enable robust network performance, bandwidth and throughput must also be maximized. Traditional solutions that use standard computer configurations as the foundation of their network security solutions impose performance limitations to network bandwidth and throughput as part of their design. For example, network administrators operating a PC-based IPS security point product running over a 1-gigabit traffic can potentially see a reduction of their total network throughput reduced to a mere 200 megabits due to limitations imposed by the inherent designs of the architecture of the PC component that is running the security software.

The FortiGate 5000 Security Gateway solution employs a unique hardware architecture that is designed to maximize network bandwidth and throughput. FortiGate leverages the use of specially designed ASICs (Application Specific Integrated Circuits) that run specific portions of the security software, eliminating the bottlenecks that can otherwise restrict network performance. These ASICs are deployed within the FortiGate ATCA hardware blades and chassis, maximizing network performance at every level of the IMS architecture. So if Firewall, VPN, and IPS security are all turned on, the ASICs will ensure that the simultaneous use of all these modules will not affect the network bandwidth, throughput, and connections-per-second, nor impact overall network performance and service integrity.

The illustration in Figure 6 below illustrated how this ASIC design translates into robust network performance within the IMS network architecture while providing protection against the various security threats without degrading functionality or performance at each network layer.

Figure 6: How ASIC Design Translates into Enhanced Network Performance



With the FortiGate 5000's use of ASICs that are embedded in both the chassis and ATCA hardware blades, administrators can re-provision the blades from one network location to another without concern over degrading network performance in the new location. To accomplish this, all the administrator needs to do is re-license the FortiGate security software module for that new deployment scenario, and install the blade in the FortiGate ATCA chassis. Once accomplished, the ASICs will automatically detect the new location, register itself onto the FortiGuard Center, and download and install any new updates for that server. The ASICs will also ensure that the performance and service integrity of the server blade at the new location is equivalent to its performance at its previous location.

Effective Management and Analysis

Fortinet also offers a wealth of valuable management tools that provide detailed analysis of the status of each software, hardware, and service component within the FortiGate 5000 system. *FortiManager*™ and *FortiAnalyzer*™, for example, can collate data —such as information logs —from each of the server blades and use it to process detailed analytic reports that help network administrators and managers better understand what is taking place within each server blade, layer, and network.

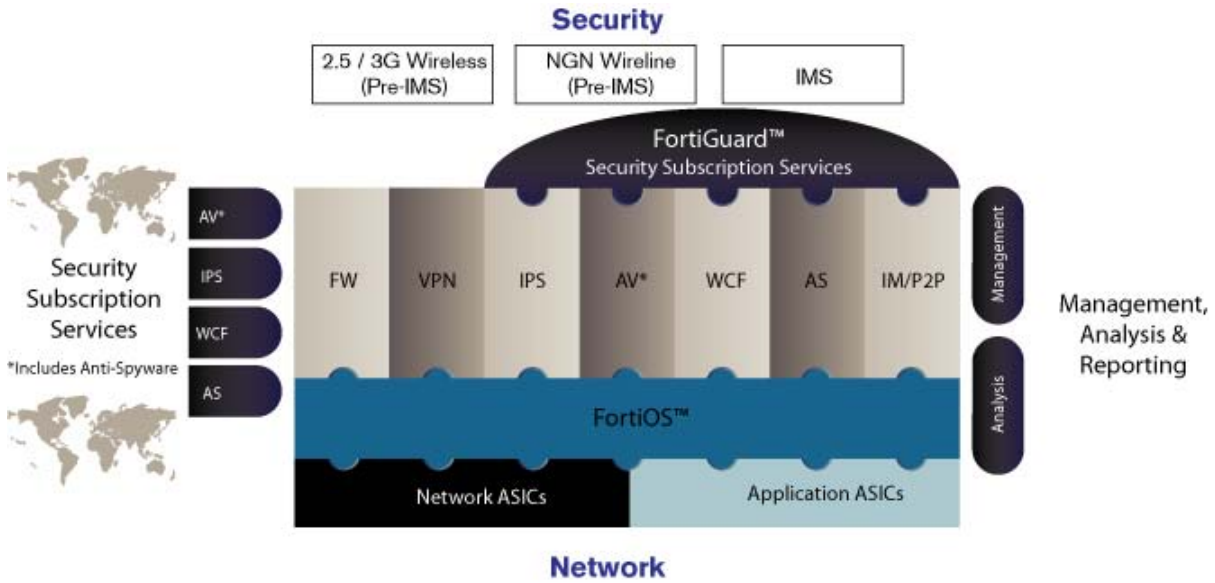
The *FortiAnalyzer*™ family of real-time network logging, analyzing, and reporting systems are a series of dedicated hardware solutions that securely aggregate and analyze log data from FortiGate security appliances. The systems provide network administrators with a comprehensive report of network usage and security information, and support the needs of enterprises and service providers responsible for discovering and addressing vulnerabilities dispersed across FortiGate systems. The FortiAnalyzer appliance minimizes the effort required to monitor and maintain acceptable user policies, identifies attack patterns, prosecutes attackers, and complies with governmental regulations regarding privacy and disclosure of security breaches. FortiAnalyzer also accepts and processes a full range of log records provided by FortiGate systems, including traffic, event, virus, attack, content filtering, and email filtering data. In addition, FortiAnalyzer provides advanced security management functions such as quarantine archiving, event correlation, vulnerability assessment, traffic analysis, and content archiving.

The *FortiManager*™ System is an integrated management and monitoring tool that enables enterprises and service providers to easily administer large numbers of FortiGate Antivirus Firewalls. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full range of network protection services provided by FortiGate devices, and supports the needs of enterprises and service providers responsible for establishing and maintaining security policies across multiple, dispersed FortiGate installations.

Telecom carriers that already have other fraud detection technologies can use these analytic reports to detect anomalous behavior or activity within an individual subscriber's account in order to prevent a security breach from impacting the rest of the IMS network.

The illustration in Figure 7 below shows the relationship between the four components of the FortiGate Security Modules, the FortiGate ATCA hardware blades, the FortiOS operating system, and the FortiGuard Security Subscription Services, and how they work together to ensure the most complete and robust security solution possible for today's IMS networks.

Figure 7: The Integrated FortiGate 5000 Network Security Solution for Telecom Carriers



Flexible IMS Security Deployment

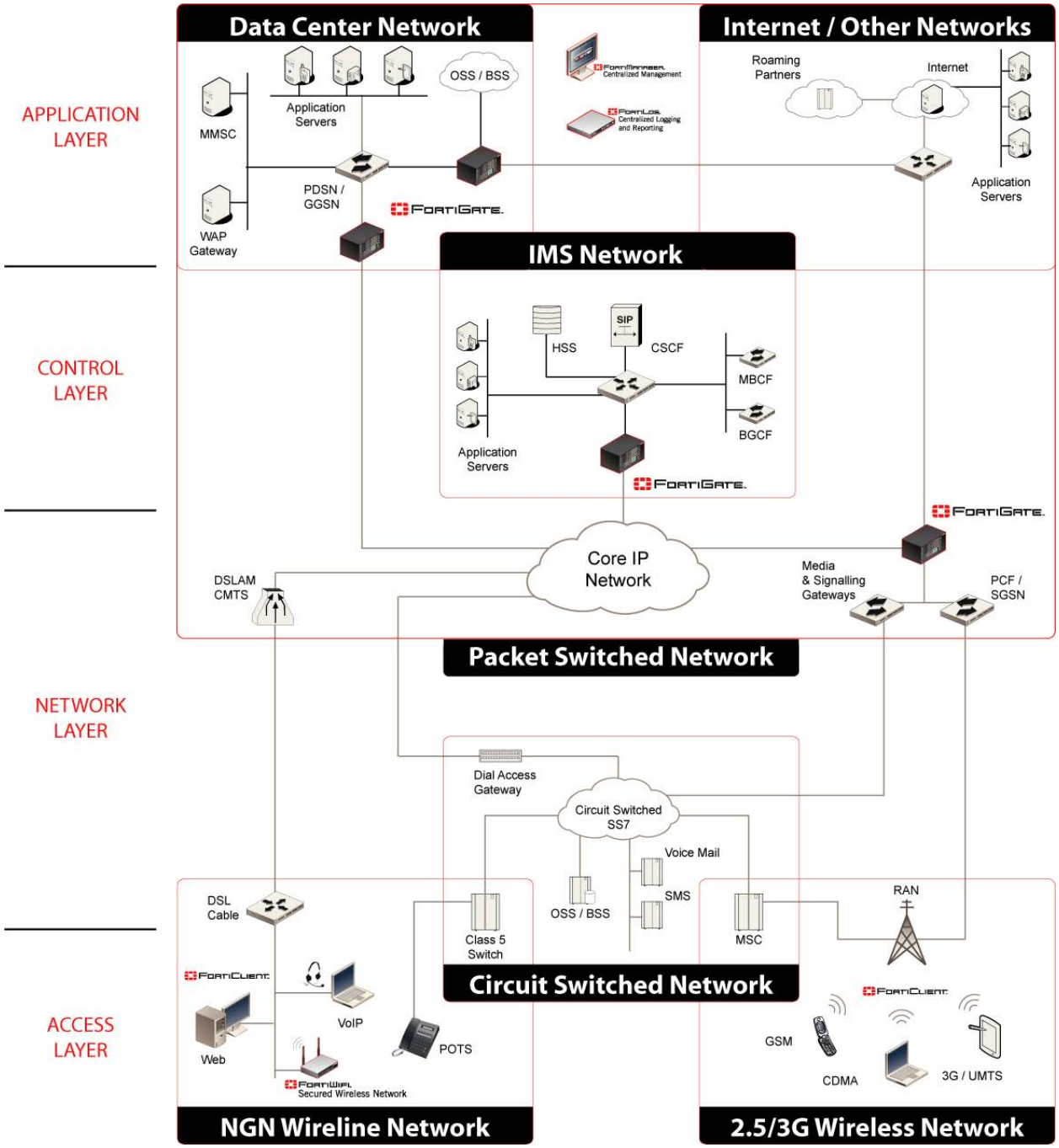
> Securing the Access Layer
>
> Access Layer security is addressed with the *FortiClient™ Mobile*, a software solution that resides on a Symbian or, Windows Mobile 5 Smart Phone or PDA.

The FortiGate 5000 series for Telecom Carriers, affords network administrators the highest degree of flexibility in how they deploy security across their IMS networks. This multi-layered approach allows them to deploy security at any layer that is appropriate, whether for the Application, Control, or Transport Layer of the IMS network.

With conventional network security solutions specifically designed for a particular network layer, administrators are often locked into dedicating that solution solely for one area. For example, a security server designed to address a threat at the Application Layer can only be used in that layer. In the event that a new security threat surfaces to attack the Control or Transport Layers, the administrator cannot re-deploy that solution to other layers without severely degrading overall network performance. With FortiGate 5000, solutions can be deployed across multiple layers while maintaining high levels of network performance. This provides the unusual combination of effective security, high performance AND cost effectiveness across the IMS network.

The flexible capabilities inherent with the FortiGate 5000 Security System design can be deployed across any layer of the IMS model as illustrated in Figure 8 below.

Figure 8: The FortiGate Flexible Security System Supports Each Network Layer



Summary

Telecom Carriers must embark on the new frontiers of rich media services that drive ARPU and reduce costs and have begun to embrace the IMS network standard and the technological benefits that are associated with its architecture in order to effectively deliver those services to their subscribers. Legacy network security strategies that were acceptable under closed circuit-based network architectures are completely revisited and redesigned to fully protect the network from a host of new security threats that jeopardize network uptime, service availability and carriers business model.

To successfully secure IMS and Next Generation services the security strategy must take into consideration the unique attributes of each layer of the IMS network model, namely the Application, Control, Transport and Access Layers, as well as each of the individual subscriber mobile devices. This requires deploying multi-layered security solutions at each of these layers to protect the network against all security threats both now and in the future.

Fortinet is the only single source partner that empowers telecom carriers with the capability of securing next generation IMS infrastructures and services. With Fortinet, carriers have the platform and solutions to enable a robust security strategy and provide management with the assurance that new application services can be securely deployed to their telecom subscribers. Fortinet enables carriers to seize new market opportunities as they arise and to grow revenues that will meet both today's and tomorrow's business goals.

For more information about Fortinet carrier security solution, please visit the Fortinet solution website at: http://www.fortinet.com/products/carrier.html

About the Authors

John Peterson - Vice President of Solutions Development

John Peterson, Vice President of Solutions Development and a member of Fortinet's Global Business Development organization, is responsible for the creation and communication of new solutions for Fortinet's strategic business partners. John joined Fortinet with over 15 years of experience in leadership, technology and innovation from leading technology innovators including US Robotics, 3Com, Cisco Systems and NetScreen. At NetScreen, he was the Director of Worldwide Systems Engineering, where he built and led a global technical sales organization. This included growing NetScreen's Systems Engineering organization from 5 to 90 members, which then led to a successful IPO in 2001 and ultimately the company's sale to Juniper Networks in 2004. John also served as a United States Marine and completed studies in Aviation Electronics.

Freddy Mangum - Vice President, Product Management, Emerging Technologies

As Vice President of Product Management, Emerging Technologies, Freddy Mangum is responsible for driving strategy and demand for Fortinet's products into emerging markets. Freddy brings to Fortinet more than 12 years of sales, marketing and business development experience with companies in the networking and security markets. Prior to his association with Fortinet, Freddy owned a marketing consulting company that provided product strategy and marketing services to companies such as IronPort Systems, Sarvega (acquired by Intel) and Permeo (acquired by Blue Coat). He was also previously employed with prominent security companies, including Internet Security Systems (ISS), where he directed marketing activities for product lines, generating more than $250 million in revenue. Freddy has also held numerous senior technical marketing and consulting engineer roles with companies such as Cisco Systems, WheelGroup and UUNET. He holds a B.S. in economics with honors from George Mason University and has completed additional studies at American University, Georgetown, University of Colorado, Stanford and Princeton.

Appendix: The IMS Security Checklist

Today, IMS security threats are multi-vector in nature, and require a comprehensive strategy that is designed to protect the carrier infrastructure at each layer of the IMS network model, taking into consideration the unique qualities and functionality of each IMS infrastructure layer.

The table below, (Figure 9) provides a checklist of the attributes that telecom carriers should look for in determining an effective security solution for their IMS network configuration and each layer within the network.

Figure 9: Checklist for an Effective IMS Security Strategy

Security Layer Requirement	Check Off √
Application Layer Requirements	
Spam protection for Messaging (IM, Email, etc.)	
Protection from proliferation of application borne viruses through messaging, video and picture sharing	
Intrusion Prevention System to protect real-time services such as VoIP	
Ability to restrict inappropriate web content access by underage subscribers	
Control Layer Requirements	
Service Protocol Inspection of all IP based protocols	
Protection from SIP Signaling Floods	
SIP IPS and Firewall Protection	
Protection from Invalid SIP Registration Floods	
Transport Layer Requirements	
Protection from Denial of Service Attacks	
Protection from Bandwidth Flooding (UDP, GDP, TCP, SYN Flooding)	
Protection from Over Billing Attacks	
Access Layer Requirements	
Security Support for Microsoft Windows Mobile & Symbian OS Devices	
Additional Requirements	
Ability to Scale to Meet Throughput Requirements for Rich Media Services	
Provisions for Future Growth to Accommodate Tomorrow's Service Needs	
Ability to Maintain High Availability	
Provision for Multiple Layers of Backup Redundancy	
Flexible Network Management and Administration Tools	
Ability to respond rapidly to changing Security Threats	

Security Layer Requirement	Check Off √
Security Subscription Services	
Online Reporting of Security Threats	
Built in ASICS to Accelerate Network and Application Security Performance	
Ability to Mix and Match Components to any Layer	
Integrated Security Subscription Service powered by trusted Global Threat R&D organization	
Automatic Software Update for each Hardware Device	
Support for the ATCA Hardware Standard	

Glossary

3G - Usually used in the context of cell phones, 3G is short for *third-generation* technology. The services associated with 3G provide the ability to transfer voice data, for example, from a telephone call, and non-voice data, for example from downloading information, exchanging email, and/or instant messaging. In marketing 3G services, video telephony has often been called the “killer application” for 3G.

3GPP - The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. It's a co-op project among ETSI (Europe), ARIB/TTC (Japan), CCSA (China), ATIS (North America) and TTA (South Korea). 3GPP specifications are based on evolved GSM specifications, now generally known as the UMTS system.

ASIC - An ASIC (Application-Specific Integrated Circuit) is an integrated circuit (IC) customized for a particular use, rather than intended for general-purpose use. For example, a chip designed solely to run a cell phone is an ASIC. In contrast, the 7400 series integrated circuits are logic building blocks that can be wired together to perform many different applications. Intermediate between ASICs and standard products are application specific standard products (ASSPs).

ATCA - Advanced Telecommunications Computing Architecture is the largest specification effort in the history of the PCI Industrial Computers Manufacturers Group (PICMG), with more than 100 companies participating. Known as AdvancedTCA™, the official specification designation is PICMG 3.x (see below). AdvancedTCA is targeted to requirements for the next generation of "carrier grade" communications equipment. This series of specifications incorporates the latest trends in high speed interconnect technologies, next generation processors, and improved Reliability, Availability and Serviceability (RAS).

Denial of Service / (DoS) - A denial-of-service attack, also, known as a DoS attack, is an attack on a computer system or network that results in loss of service to users — typically the loss of network connectivity and services — caused by the attacker consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

GPRS - General Packet Radio Service (GPRS) is a mobile data service available to users of GSM mobile phones. It is often referred to as "2.5G", that is, a technology between the second (2G) and third (3G) generation of mobile telephony. It provides moderate-speed data transfer by using unused TDMA channels in the GSM network. Originally there was some thought to extend GPRS to cover other standards, but instead those networks are being converted to use the GSM standard, which is the only kind of network where GPRS is in use.

GTP - GPRS Tunneling Protocol (or GTP) is an IP based protocol used within GSM and UMTS networks. The GTP protocol is layered on top of UDP. There are in fact three separate protocols, GTP-C, GTP-U and GTP'. GTP-C is used within the GPRS core network for signaling between GPRS Support Nodes (GGSNs and SGSNs). This allows the SGSN to activate a session on the users behalf (PDP context activation), to deactivate the same session, to adjust quality of service parameters or to update a session for a subscriber who has just arrived from another SGSN.

MMS - Multimedia Messaging Service (MMS) is a technology for transmitting not only text messages, but also various kinds of multimedia content *(e.g.* images, audio, and/or video clips) over wireless telecommunications networks using the Wireless Application Protocol (WAP). It is standardized by 3GPP and 3GPP2.

IMS - The IP Multimedia Subsystem (IMS) is a standardized Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. It uses a Voice-over-IP (VoIP) implementation based on a 3GPP standardized implementation of SIP, and runs over the standard Internet Protocol (IP). Existing phone systems (both packet-switched and circuit-switched) are supported. The aim of IMS is not only to provide new services but all the services, current and future, that the Internet provides. In addition, users want to be able to execute all their services when

roaming as well as from their home networks. To achieve these goals, IMS uses open standard IP protocols, defined by the Internet Engineering Task Force (IETF). A multimedia session between two IMS users, between an IMS user and a user on the Internet, and between two users on the Internet is all established using exactly the same protocol. Moreover, the interfaces for service developers are also based on IP protocols.

SIP - Session Initiation Protocol (SIP) is a protocol developed by the IETF MMUSIC Working Group and is the proposed standard for initiating, modifying, and terminating an interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality. In November 2000, SIP was accepted as a 3GPP signaling protocol and permanent element of the IMS architecture. Along with H.323, it is one of the leading signaling protocols for Voice over IP.

Symbian OS - Designed for mobile devices, Symbian OS is an operating system with associated libraries, user interface frameworks and reference implementations of common tools, produced by Symbian Ltd.. It is a descendant of Psion's EPOC. Symbian is currently owned by Ericsson, Panasonic, Siemens AG, Nokia, and Sony Ericsson.

SYN - SYN (synchronize) is a type of packet used by the Transmission Control Protocol (TCP) to synchronize the sequence numbers on two connecting computers when initiating a new connection.. The SYN is acknowledged by a SYN/ACK by the responding computer. A type of denial of service attack known as a *SYN Flood* involves sending large numbers of SYN packets and ignoring the return, thereby forcing the server to keep track of a large number of half-open connections.

Trojan horse - a Trojan horse is a malicious program that is disguised as legitimate software. The term is derived from the classical Greek myth of the Trojan horse. These programs may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed
There are two common types of Trojan horses. One is otherwise-useful software that has been corrupted by a hacker inserting malicious code that executes while the program is used. Examples include various implementations of weather alerting programs, computer clock setting software, and peer-to-peer file sharing utilities. The other type is a standalone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity needed to carry out the program's objectives. Trojan horse programs cannot operate autonomously, in contrast to some other types of malware, like viruses or worms. Just as the Greeks needed the Trojans to bring the horse inside for their plan to work, Trojan horse programs depend on actions by the intended victims. As such, if Trojans replicate and even distribute themselves, each new victim must run the program/trojan. Therefore their virulence depends on the successful implementation of social engineering concepts rather than flaws in a computer system's security design or configuration.

UDP - The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages known as datagrams to one another. UDP does not provide the reliability and ordering guarantees that TCP does; datagrams may arrive out of order or go missing without notice. However, UDP is faster and more efficient for many lightweight or time-sensitive purposes. Also its stateless nature is useful for servers that answer small queries from huge numbers of clients. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications, Voice over IP, Trivial File Transfer Protocol (TFTP), and online games.

VoIP - Voice over Internet Protocol (also called VoIP, IP Telephony, Internet telephony, and Broadband Phone) is the routing of voice conversations over the Internet or any other IP-based network. The voice data flows over a general-purpose packet-switched network, instead of on traditional, dedicated, circuit-switched telephony transmission lines. Protocols used to carry voice signals over the IP network are commonly referred to as Voice over IP or VoIP protocols. They may be viewed as commercial realizations of the experimental Network Voice Protocol (1973) invented for the ARPANET. Voice over IP traffic can be deployed on any IP network, including ones lacking a connection to the rest of the Internet, for instance on a private building-wide LAN.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, Web content filtering, VPN, spyware prevention and antispam--providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by the ICSA (firewall, antivirus, IPSec, SSL, IDS, client antivirus detection, cleaning and antispyware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700 Fax +1-408-235-7737
www.fortinet.com

WPR123-0506-R1