The Evolution of Data Center and Carrier Network Security

Featuring Gartner's note, Competitive Landscape: Carrier-Class Network Firewalls

Welcome

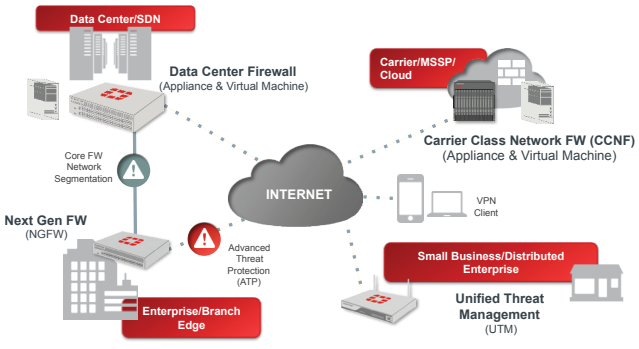
IT networks are undergoing significant change due to new infrastructure technologies and more sophisticated threats, and a one-size-fits-all approach to network security no longer applies. This report discusses the increasing specialization of network security technologies, and key trends and requirements for data center and carrier network firewalls.

Data Center and Carrier Networks Driven by Higher Performance

Firewalls are one of the earliest information security technologies developed, and still remain a fundamentally vital cornerstone to any IT security strategy. However, today's modern firewall bears little resemblance to the original ones from the 1980's. While still retaining a packet filtering engine at its core, firewalls are increasingly specialized for specific IT use cases and environments. Consider for example:

- Unified Threat Management (UTM) firewalls – consolidated security for small and medium enterprises, often integrated with network switching and wireless access and security

Increasing Specialization of the Network Firewall



Source: Fortinet

Featuring research from Gartner

- Edge (aka NGFW) firewalls – enterprise campus access firewalling, with next-generation application and user security and increasingly, consideration for advanced threats

- Data Center firewalls (DCFW) – core firewalling and segmentation for enterprise and carrier data centers that are being increasingly consolidated and transformed by virtualization, cloud and SDN

- Carrier Class Network Firewalls (CCNFW) – carrier and MSSP security that augments data center security with specific communication service provider use cases including multitenancy, carrier clouds, 4G/LTE, and SDN/NFV.

Key Requirements for Data Center and Carrier Firewalls

While the attached Gartner note discusses a multitude of projects impacting carriers and service providers, such as 4G/LTE and the Internet of Things, the one constant among all of these is increasing speeds and traffic. Hence one of the key distinctions of carrier-grade firewalls from enterprise campus NGFW is higher performance. Defined by Gartner, CCNFWs must be capable of at least 40 Gbps throughput, 10 million concurrent sessions, 100,000 connections per second and the ability to generate 100,000 logs per second while introducing no more than three milliseconds of latency, tied to the Third Generation Partnership Project (3GPP) maximum latency budget for LTE Advanced (LTE-A) of 10 milliseconds from end to end. Similarly NSS Labs, in defining for the first time evaluation testing criteria for Data Center Firewalls, also instituted a minimum of 40 Gpbs throughput.

But higher performance also manifests in other requirements and considerations as well:

- higher concurrent sessions and connection rates, driven by increasing numbers of mobile users and connected devices accessing network and data center services;

- greater small and mixed-packet performance from continuous, anytime, anywhere communications and access;

- native IPv6 and CGNAT performance to scale to larger numbers of devices;

- higher-speed interfaces, such as 40GbE/100GbE ports, to support next-generation switching fabric with increasingly converged and consolidated infrastructure

- higher port density for flatter scale-out architectures that can support elastic clouds and user-centric application frameworks

Source: Fortinet

From the Gartner Files:

Competitive Landscape: Carrier-Class Network Firewalls

This research provides essential competitive insights into carrier network firewall providers. It delivers relevant information to help firewall product and marketing managers address the carrier market.

Key Findings

- Projects related to LTE, LTE-A, VoLTE and the Internet of Things (IoT) are key challenges for communications service providers (CSPs) today, given the new protocols and interfaces. CSPs' goal is to increase service capabilities, which will in turn create the need for higher speeds and improve customer experience and quality of service.
- Multitenant capabilities to separate customer environments (virtual domains and virtual system instances) delivered in a single chassis are often preferred for carrier data center solutions.
- CSPs are moving toward SDN and NFV, where security will have longer test cycles but the speed at which deployments occur will be faster than that of other technology rollouts such as IP or IMS.
- Gartner believes CSPs will seek to deliver as cost-effectively as possible a combination of firewall and threat inspection capabilities, such as application awareness/control, URL filtering, anti-malware and intrusion detection/prevention, as virtual network functions, to extend their existing services.

Recommendations

- Initiate conversations with CSPs to discover emerging security concerns around protecting LTE and the IoT (that is, home automation, smart cities and others), and work with marketing managers to create aligned messaging around these areas of growth.
- Ensure market messaging aligns to CSP needs in terms of speeds, feeds and latency, and that product support for future technology environments such as SDN and NFV stands out.
- Emphasize how products assist CSPs in their plight for more secure communications networks, and in particular how they relate to 4G/LTE.
- Understand CSP security and threat inspection needs in terms of 4G/LTE and supporting protocols, which in turn could be an opportunity for greater firewall product differentiation.

Analysis

Definition

The carrier-class network firewall (CCNFW) marketplace considered in this Competitive Landscape research is composed primarily of purpose-built appliances and virtual appliances for securing or augmenting the security service delivery capabilities of carrier networks. These are highly scalable, reliable and manageable systems that offer a broad set of security controls designed to efficiently protect users, infrastructure and applications from current and future threats, without impairing performance or introducing excessive latency. In addition to port/protocol inspection, they are capable of decoding key protocols in use on modern networks, detection and mitigation of Internet Protocol (IP) or application layer threats, and policy enforcement through a variety of actions (block, throttle, redirect and others). They must provide robust native IPv6 as well as carrier-grade NAT (CGNAT) support to both address the pending global IPv4 exhaustion and support greater scalability to address increasing network performance demands. They support a variety of tunneling, encryption, proxy, load balancing/throttling and authentication capabilities. They are highly reliable platforms offering high availability and five-nines (99.999%) reliability within and across POPs (points of presence), and should be upgradable (hardware and software) with little to no downtime. They should be able to support active-active and active-passive load balancing capabilities.

Typical use cases for CCNFWs include:

- **Network protection** — To protect a carrier's own network. Examples include protecting existing infrastructure components such as

switches, routers, the evolved packet core (EPC) and subscriber data from malicious network attacks, and reducing potential network distributed denial of service (DDoS) risks.

- **Carrier managed security service providers (MSSPs) and carrier cloud deployments** — To provide security services to customer environments and enable carriers with new managed security service business opportunities (that is, data center protection either hosted in a colocation or in the cloud).
- **Clean pipe services** — To offer deep inspection of network traffic — for example, DDoS and intrusion prevention/detection systems (IPS/IDS) with application awareness for protection against Layer 7 attacks.

Key differentiators between CCNFWs and enterprise next-generation firewalls (NGFWs) are:

- **Speeds** — CCNFWs must be capable of at least 40 Gbps throughput, 10 million concurrent sessions, 100,000 connections per second and the ability to generate 100,000 logs per second while introducing no more than three milliseconds of latency, tied to the Third Generation Partnership Project (3GPP) maximum latency budget for LTE Advanced (LTE-A) of 10 milliseconds from end to end.
- **Standards and protocol support** — Common TCP/IP protocols, common routing protocols (such as BGP and OSPF), encryption protocols (IPsec/SSL), multicast protocols (UDP), authentication services (RADIUS/Diameter) and optional support for LTE protocols (such as GTP, SCTP, Diameter and SIP) and both IPs (IPv4 and IPv6).
- **Management** — They must support command line interface (CLI), Web graphical user interfaces (GUIs), fat/rich/thick client capabilities and (optional) API interfaces. They must have features such as multitenant logging and reporting, applying policy across multiple domains, strong role-based workflow management and integration with trouble ticketing systems.
- **Form factor** — They can run on either commercial off-the-shelf (COTS) servers, supporting x86 and virtual machines (VMs), or purpose-built hardware. They must support tight integration with the evolving software-defined networking (SDN) and network function virtualization (NFV) standards, so they can be managed as part of a larger orchestration ecosystem.
- **Other capabilities** — They may provide IPS/IDS, DDoS protection, botnet protection, Web application firewalling, public-key infrastructure (PKI) support, application awareness and strong application delivery controller functionality. NGFWs also provide these capabilities.

Competitive Situation and Trends

Current Trends

New services are emerging from the adoption trajectory of 4G/LTE, and the promise of 5G changes CSP speed requirements for CCNFWs.

CSPs, like most large enterprises, use a layered approach to security, and a firewall is an important part of the security ecosystem. The largest CCNFW vendors, Cisco and Juniper, often lead the market in the CSP landscape largely because they supply switches and routers to Tier 1 CSPs that are moving higher volumes of traffic (voice, data, multimedia). Consequently, the need for carrier-grade resilience (that is, five-nines reliability, NEBS compliance, etc.) is a top priority, as this is where the potential for network outages likely occurs.

CSPs deploying firewalls typically base necessary speeds on particular project guidelines. However, due to CSPs adopting 4G/LTE technologies and considering SDN/NFV as the overall architecture, 10 Gbps is no longer sufficient due to higher traffic volumes. Therefore, we see a transition occurring toward 40 to 100 Gbps throughput rates as buying criteria. While they continue to deploy lower speeds in many mobile networks, CSPs are moving toward these higher speeds in their core networks as voice, video and multimedia traffic increases. The IoT will also play a role in the need for higher speeds and capacity. Due to consumer perception, mobile network providers and traditional wireline ISPs are making the shift toward higher speeds because consumers and end users expect similar experiences with respect to 4G/LTE services. Looking forward, 5G promises to increase throughput even more, creating direct competition between the traditional fixed-line and wireless CSPs.

While CSPs often "prefer" CLIs, centralized management consoles such as Web/thick client GUIs and API interfaces have become more widely desired capabilities.

Tier 1 CSPs have long used CLIs as their preferred remote troubleshooting method and style of interaction with individual devices. CLIs can also be used for initial deployment configurations. Today, smaller Tier 2/3 CSPs tend to utilize Web GUIs or leverage firewall management consoles for centralized management and support of individual multitenant network firewalls. However, with networks evolving toward SDN and NFV, initial and post configuration has also evolved to incorporate automated deployment and provisioning capabilities. This has been largely due to the desire for maximum staff efficiency and to ensure policy consistency, as elements are moved within and around in the SDN environment. To support more complex integrated environments, APIs are a necessity. APIs are most often used in support of customized customer dashboards and centralized administration, provided via internal carrier, developed or third-party software capabilities for large-scale carrier networks.

Current management options include:

- Web GUIs that can be ideal for individual box configuration and troubleshooting a specific issue, such as interface problems or functions that are virtualized or on demand
- Centralized management through a console that smaller carriers would consider a "quicker" and "easier" configuration platform for more broad security configurations
- APIs, which can be ideal for setting parameters and monitoring or applying more application-specific security configurations
- Thick clients or non-Web browser-based applications

Emerging Trends

Full IPv6 inspection and mobile protocol inspection are helping carriers transition to delivering enhanced network security service capabilities.

One of the most challenging issues for CSPs today, particularly those rolling out 4G/LTE, is the newer set of protocols and interfaces that accompany the technology. In addition, the IoT has created the requirement for CSPs to carry more IP addresses. IPv6 promises to address this challenge. Going forward, support for mobile protocols such as the S1 link, GTP and Diameter, for example, can help to increase the security of the network and improve visibility for network inspection devices. The S1 link is the most important to protect subscriber data and improve customer privacy issues as well as introduce protection from the radio access network (RAN) to the EPC. By adding these inspection and participation capabilities, carrier network firewalls are able to extend the capability of the carrier network, allowing carriers to offer new security service offerings and present revenue opportunities to their clients.

The shifting of platforms from traditional security appliances to virtualized solutions orchestrated using SDN and NFV concepts will help CSPs lower costs and improve network performance.

SDN is not a new concept overall, but it is a newer concept for CSPs that typically rely on hardware-based solutions, as these provide for a more secure and reliable network. CSPs are now tasked with having to drive new services and reduce opex. As a result, today we are seeing more exploration from the CSPs of provider solutions that can help them achieve the elasticity of their networks to provide services, bandwidth, security and others on demand while reducing overall network operating costs. Many providers in the CCNFW space are moving their hardware-based platforms toward either x86 platforms or VMs. This is important as CSPs move toward SDN environments and begin virtualizing network functions.

SDN and NFV will enable software-defined security-as-a-service, whereby security functions historically within appliances, such as routers, session border controllers, firewalls and other gateways, are now hosted in servers and can be dynamically launched as needed. However, while dynamically launching security as needed is good, proactive and predictive security is also needed as well as reactive security that launches only after hacks occur. Since viruses, malware and patterns of attacks change often, the signatures within the security gateways need to be adapted on the fly and traffic dynamically redirected as needed. This is the underlying advantage SDN and NFV can offer over hardwired hardware appliances.

SDN will create new security challenges for how networks and subscriber data are protected, as it places network control and access in a more central position. Specific protocols and interfaces will need to be handled differently — for example, the S1 interface will need to be protected as it is a direct route to the EPC. The layered approach to security and the centralized points where the SDN

can be controlled also create an opportunity for more monitoring and security control to be added to the network. It can be easier to "roam" across a traditional network once access is gained through its large network edge. SDN will instead allow the setup and rollout of more security through the ability to centrally configure and provision security services, either for subscribers or for the network functions themselves.

The security challenge in particular will be key for successful SDN deployment; however, SDN can increase security as it will reduce the number of devices to be configured manually and can thus reduce the possibility of misconfiguration. SDN could also provide CSPs with new revenue streams from enabling services such as security as a service, when functions can be virtualized and the networks become more elastic. A more secure and robust network will bring better services to consumers and new consumption models may be obtained for enterprises. In addition, clean pipe service delivery will also drive the adoption of firewall capabilities in the carrier space. Services such as integrated intrusion prevention and URL filtering may be provisioned as virtualized network functions under SDN control, with new revenue streams and lower capex and opex.

CSPs are currently investigating and testing SDN and NFV, and the market is growing rapidly as SDN and NFV increasingly become integrated into mobile networks for LTE EPC and voice over LTE (VoLTE) solutions, along with cloud-based Wi-Fi controllers supporting seamless roaming. However, with respect to security, longer test cycles may occur as CSPs cannot risk any security event that will compromise the network. Additionally, network protocols such as Network Service Headers are being introduced in draft to the Internet Engineering Task Force in order to both provide service chaining where multi-inspection can be performed serially within a global CSP network and insert network functions dynamically (see the Evidence section). Product managers must ensure they thoughtfully integrate with SDN capabilities such as OpenFlow and Open vSwitch. One of the many challenges with SDN is to ensure the SDN fabric properly routes packets through the network firewall for inspection; it will be up to carrier network firewall providers to offer multiple integration options for inspection.

VoLTE and LTE-A will bring new security needs as CSPs begin migration plans to add voice over their LTE architectures.

While we are seeing security challenges emerge with the introduction of an all-IP infrastructure (an element of 4G/LTE), improved authentication and encryption capabilities have also been introduced. For instance, in Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network (E-UTRAN), all data sent over the radio interfaces is encrypted. Conversely, concurrent trends that are increasingly popular include the deployment of small cells. While small cells provide greater network accessibility, they can be easy to tamper with. Hackers can leverage or exploit these access points.

Wireless CSPs rolling out VoLTE and LTE-A will need to put in place components and configurations to ensure quality of service, prevent legitimate network failures and fend off malicious attacks. Technology providers that have strong capabilities geared toward mobile network operators migrating to add voice to their LTE networks should emphasize this in their marketing messages.

Market Players

In the Competitive Profiles section, we discuss sampling of the 10 providers that Gartner estimates to hold the biggest shares in the CCNFW market. Other CCNFW providers not mentioned in this sampling may have equally competitive offerings as these mentioned here.

Gartner estimates the total CCNFW market at roughly $1.3 billion. Table 1 shows estimates of how this is shared between those 10 providers.

Table 1. CCNFW Market Share Estimates

Provider	Estimated 2013 Revenue ($M)	Share
Cisco	347.2	27.8%
Juniper Networks	310.0	24.8%
Check Point Software Technologies	225.0	18.0%
Fortinet	106.0	8.5%
Huawei	64.80	5.2%
F5	31.9	2.6%
Stoke	16.0	1.3%
Palo Alto Networks	13.2	1.1%
Dell SonicWALL	12.4	1.0%
Intel Security	5.4	0.4%
Others	116.8	9.4%
Total	1,248.7	100%
Note: Percentages may not add up to 100% because of rounding		
Source: Gartner (October 2014)		

The Future of Competition

The dominating players in the CSP firewall space have been Juniper Networks, Cisco, Check Point Software Technologies and Fortinet. Other providers that have a wide CSP customer base are Palo Alto Networks and Huawei. However, CSPs' network migrations and the ongoing shift from fixed to mobile creates new challenges that vendors in this space will need to overcome. A relatively new breed of vendors and market entrants has emerged — for example, providers such as Stoke, which specializes in the S1 interface that is unique to CSPs rolling out LTE and LTE-A services. This is an area that providers of CCNFWs should embrace.

Providers in the CCNFW space have either existing solutions that may be virtualized or road maps for supporting CCNFWs in a virtualized environment and working with the SDN controller vendors. Others have either built or acquired an SDN controller for a more end-to-end offering. For example, Cisco and Juniper have their own SDN controller solution and also work with the major SDN vendors for interoperability, in order to offer the CSPs more flexibility when choosing a firewall.

A possible market disrupter in the CCNFW market is CSPs moving toward software-defined networks and virtualizing network functions for more network flexibility. Carriers will be looking for technology providers that can support security features such as URL filtering, DDoS and intrusion prevention/detection that can be deployed under SDN control. Also, while convergence of security technologies has long been postponed due, in part, to performance limitations, NFV could displace such convergence as security features and functions under SDN control become more elastic and therefore more "on demand" versus static.

It is important that all providers support CLIs. However, the notion of centralized management consoles or Web/thick GUIs and thin clients in the CSP space may become evident as network changes take place, particularly SDN. Additionally, providers need to have the ability to scale as the CSPs' needs are changing — firewall solutions will need to handle increasingly heavy payloads during peak hours and at times when session volumes are expected to increase exponentially, such as during media voting events and holidays, while performing other necessary functions. Furthermore, the advanced and robust services and capabilities CSPs are providing will considerably increase daily traffic volumes. The technology providers will need to be able to go well beyond 10 Gbps in order to meet CSPs' needs.

Competitive Profiles

Check Point Software Technologies

Estimated carrier revenue: $225.0 million

Market Overview

Check Point Software Technologies is based in Tel Aviv, Israel, and has been a staple in the firewall and information security industry since its founding in 1993. Check Point is well-known for its 61000 next-generation firewall product for CSPs, and its entire product portfolio is based on unified Software Blade Architecture.

Check Point is a well-known firewall vendor within the carrier space and has over 2,500 CSP customers worldwide. It is actively increasing its dedicated sales force for the CSP segment and has been working with mobile system integrators to enhance its products. It offers a comprehensive set of professional services and has a product road map that closely aligns with industry trends.

Check Point offers the 61000, 41000, 21000 and 13800 platforms. The 61000 scales from two to 12 Security Gateway Modules and has firewall throughput of up to 400 Gbps and up to 130 Gbps IPS protection when fully loaded. It can support 210 million concurrent connections and 3 million sessions per second. The 21000 and 13800 are offered as two rack-unit appliances. The 13800 has clean pipe value-add services, carrier-grade NAT (CGNAT) supporting IPv4 and IPv6, and it supports LTE protocols including GTP, SCTP and Diameter.

Check Point's carrier security platforms support all hypervisor technologies including OpenStack and VMware vSphere Hypervisor, and work with system integrators on NFV integration projects. The company is also working closely with SDN controller vendors for more integrated solutions, and in April announced its Security Gateway Virtual Edition solution, which fully integrates with VMware NSX.

Check Point offers a centralized management console, Provider-1, as part of its Software Blade Architecture. It enables creating and managing multiple virtual domains and uses a drag-and-drop-type GUI.

How This Provider Competes

Check Point competes through a 100% sales channel strategy. Among its channel partners are Nokia Networks, and ZTE for system integration (testing, certification and deploying) of Check Point products in their CSP environments. HP, Dimension Data and Fujitsu are strategic partners offering product integration, and it uses Cisco for services.

From a product perspective, Check Point offers optional clean pipe value-add services that leverage its enterprise-grade software blade security with IPS, antivirus, URL filtering, application control and anti-botnet protection.

Being a well-known player in the carrier space, it has deployments in large Tier 1 CSPs and multiple-system operators (MSOs) worldwide, Check Point can leverage its installed base with its worldwide customers as CSPs move toward virtualized environments and roll out LTE services. It has dedicated R&D resources in telco, cloud and NFV as strategic investments in its firewall product portfolio. It also has recently announced a threat intelligence store concept it calls "IntelliStore" as part of its ThreatCloud offerings. The ThreatCloud IntelliStore helps deliver additional blocking capabilities for clean pipe services from third-party intelligence providers, which help address defense against advanced targeted attacks, advanced malware and phishing attacks.

Check Point's closest competitors are Cisco, Fortinet, Palo Alto Networks and Juniper.

Cisco

Estimated carrier revenue: $347.2 million

Market Overview

Cisco designs, manufactures and sells IP-based networking products that facilitate transmission of voice, data and video traffic over networks. It is well-known in the CSP space for its routing platforms and has been investing in its security platforms for CSPs. Although having a stronger presence in the enterprise space, its strong global presence provides the company an opportunity to increase its carrier market visibility and promote its sales activities. Globally, the company has presence in the U.S. and Canada, European markets, emerging markets and Asia/Pacific.

Cisco offers its Adaptive Security Appliance (ASA) 5585-X series of firewall appliances for service providers and large enterprises, typically for data centers. These appliances are offered in a two rack unit (RU) chassis running a high-performance firewall processor blade as a base configuration, with the option to add multifunctional advanced security services modules. They are built on x86 platforms with some proprietary components based on application-specific integrated circuits (ASICs) for specific functions to improve speed and performance.

At the high end of the series, the ASA 5585-X appliance is capable of supporting 40 Gbps firewall throughput and 350,000 connections per second for a total of 10 million concurrent connections. These platforms support clustering of up to 16 nodes and can scale to 640 Gbps firewall throughput, 2.5 million connections per second and 110 million concurrent connections. The ASA series is a standards-compliant stateful firewall with routing, VPN, application layer inspections and scalable NAT functionality for IPv4 and IPv6 traffic.

Cisco also offers platform-based subscription FirePOWER Services for the ASA platforms, which come from the acquisition of Sourcefire in July 2013. The services include next-generation IPS (NGIPS), next-generation firewall (NGFW) and advanced malware protection (AMP) capabilities, which can also be offered as virtualized functions. Products include the ASAv (virtual firewall), vNGIPS (virtual NGIPS), WSAv (virtual Web security appliance) and ESAv (virtual email security appliance). The virtual security appliances can be integrated into varied SDN and NFV environments as well as Cisco's, third-party and open-source orchestration solutions. It also has its own SDN controller, Application Policy Infrastructure Controller (APIC), which can manage the ASA 5585-X. The ASA can also integrate with other SDN controllers.

How This Provider Competes

Having a strong footprint in the carrier space with its high-end routers and switches, Cisco generally takes an end-to-end approach as part of its overall strategy. It has been investing in its security product portfolio and evolved its solution toward an open security platform architecture for security service orchestration and chaining across physical and virtual infrastructures. As it has ingrained programmability into the security platform itself, Cisco security products will integrate into any SDN and NFV technologies. For example, because of the open API, the management system is optional as it can be programmed directly into the platform. Cisco offers its own SDN APIC as trends dictate that CSPs are moving toward SDN environments. The company's recent acquisitions of ThreatGrid and Sourcefire have provided it with the ability to quickly analyze and identify malware through payload analysis and endpoint telemetry, and generate enhanced intelligence information for detection and blocking purposes in its various ASA appliances. These new capabilities are offered as part of the Cisco ASA-55xx FirePOWER services software.

Cisco offers security "plan and build services" through its partners. Services commonly include:

- Security technology readiness assessments
- Security design and deployment
- Security deployment and implementation
- Security engineering
- Security knowledge transfer
- A supplemental 30-day post-deployment service — a remote optimization tuning activity to improve the security solution (such as limit system "noise" or improve alerting)

Cisco's firewall product is capable of clustering up to 16 appliances and also offers multilayered security services such as botnet filter protection, IPS, URL filtering and advanced malware protection, with the aim of providing high performance and speeds.

Cisco's direct competitors are Check Point, Juniper and Fortinet.

Dell SonicWALL

Estimated carrier market revenue: $12.4 million

Market Overview

Dell entered the network firewall market in May 2012 through the acquisition of SonicWALL. Dell SonicWALL is best known in the network firewall market for its unified threat management, next-generation firewall products and competitive pricing. Its products' deployment simplicity, user interface design, real-time application visualization, inspection performance and scalability have also been significant distinguishing factors.

In the carrier market, Dell SonicWALL currently offers its range of SuperMassive E10000 series appliances for the CSP and data center network firewall markets. The company currently offers appliance models capable of 10, 20 and 40 Gbps in its E10000 series lineup. The E10800 is currently only offered in a 4RU appliance form

factor, which has 6x 10 Gbps small form-factor pluggable (SFP+) and 16x 1 Gbps SFP interfaces. The company currently claims throughput rates of up to 40 Gbps of stateful packet inspection, 30 Gbps of application inspection and intrusion protection and up to 12 Gbps of deep packet inspection (DPI) when combined with full threat prevention. Dell SonicWALL does not currently offer virtualized firewall appliances for VMware or KVM environments, and is focusing on support for software-defined networks through active work on DPI security integration into OpenStack environments.

Dell SonicWALL also offers a centralized security management console it calls the Dell SonicWALL Global Management System (GMS). The GMS provides real-time monitoring and alerting of firewall activity in security events, can manage all models of its next-generation firewall and UTM platforms, and can be deployed as software, hardware or as a virtual appliance. GMS also offers change management through a new workflow automation feature that uses processes for configuring, comparing, validating, reviewing and approving policies prior to deployment. GMS is currently targeted toward distributed enterprises, service providers and SuperMassive installations. It supports CLI-, API- and role-based management. Additionally, the company offers network flow analysis software called Scrutinizer NetFlow Traffic Analyzer. The Scrutinizer software supports multivendor, flow-based application traffic analytics as well as visualization and reporting, and is available as a Windows-based appliance or virtual appliance.

How This Provider Competes

Its Reassembly-Free Deep Packet Inspection (RFDPI) engine gives it some product performance advantages over some of its smaller rivals, and allows it to move beyond its unified threat management roots to having an NGFW-class of products. Although the company does well in third-party competitive tests for security effectiveness and overall inspected throughput, its carrier-class SuperMassive product line has remained relatively unchanged during the last year. For CSP networks, the company also offers an integrated WAN acceleration, optimization and content caching appliance — Dell SonicWALL WXA Series — which can provide an advantage in some competitive situations in carrier deals.

Dell SonicWALL commonly engages in direct competition with competitors such as Palo Alto Networks, Check Point, Fortinet and Cisco, and seeks to compete more effectively against these rivals.

F5

Estimated carrier market revenue: $31.9 million

Market Overview

Founded in 1996, F5 is headquartered in Seattle, Washington, and is an infrastructure provider focused on modular application delivery controllers (ADCs). It also has security products enabled as add-ons to its primary BIG-IP family of products. In the carrier space, its firewall products include software services for SDN and advanced routing, the BIG-IP Local Traffic Manager, Global Traffic Manager, Application Acceleration Manager, Advanced Firewall Manager, Policy Enforcement Manager, Application Security Manager and BIG-IP CGNAT modules. Each module has its own set of functionalities, such as load balancing, SSL proxy and services. IPv6 support is part of the BIG-IP Local Traffic Manager, and the BIG-IP Global Traffic Manager handles global server load balancing, DNS services, geolocation and DNS DDoS protection. The other modules provide a network firewall, Web application firewall functionality and subscriber/application controls. F5 also offers a virtual edition for many hypervisors, including VMware ESX/ESXi, Citrix XenServer, Microsoft Hyper-V, Linux KVM and Amazon EC2. Additionally, OpenStack load balancing as a service is available for NFV integration. It is also SDN-ready and lab-validated.

BIG-IP supports IPv6 and in a 16RU can support up to 640 Gbps throughput, up to 8 million connections per second, and 576 million concurrent connections. In 2013, it introduced the Advanced Firewall Manager supporting CLI, API and Web GUI interfaces.

F5's professional services include engagements that serve a variety of purposes, including strategic guidance, architecture and design, competitive migrations, system deployments, security policy creation and deployment, system upgrades, performance testing, emergency responses, troubleshooting, development relating to its extensible features, and general security support. Pricing is generally determined on a defined hourly basis.

How This Provider Competes

F5's modular approach focuses marketing on its multilayered redundant security architecture, which targets CSP desires for resiliency and network redundancy. Its claim also extends toward addressing potential vulnerabilities by avoiding stand-alone point products designed for specific security needs. As a full proxy it provides flexibility and customization, allowing CSPs to develop applications and services quickly on the same platform. Viewing the carrier network on a holistic basis, F5 also looks to add a security focus to the application, signaling and data planes, with DDoS solutions across all layers.

It has a long list of partners it leverages in its Unity partner program, including vendors in security such as Websense, Splunk and Symantec, as well as reseller partners such as HP, IBM and Dimension Data. It also has a Guardian professional services program, whose partners have expanded globally to include the U.S., Brazil, the Middle East and Africa, Japan and Hong Kong.

In 2013, F5 acquired two companies related to security: Versafe, for the real-time protection of communications between end-user devices and Web/mobile applications software; and LineRate Systems, for software-defined application services. In 2014, F5 also acquired Defense.Net for its cloud-based security services and DDoS protection capabilities.

In the carrier space, F5 competes with the firewall vendors Juniper, Fortinet, Check Point and Huawei. It also competes with Citrix in the ADC space with firewall security capabilities. Because its firewall capabilities require the ADC, it has won contracts from earlier deployments and in some cases due to price/performance.

Fortinet

Estimated carrier revenue: $106.0 million

Market Overview

Founded in 2000, Fortinet is most widely known for the research and development of its own design of ASIC-based network firewall platforms, its FortiOS operating system and as a unified threat management (UTM) provider to small and midsize businesses. During the last several years, the company has extended its marketing and product development efforts toward larger organizations such as enterprise data centers and carriers with higher-performing solution announcements.

In the carrier market, Fortinet offers its FortiGate-5000 Series products. This consists of the FortiGate-5001C, 5001B, 5101C and the FortiSwitch-5203B, supporting inspection throughput capabilities ranging from 10 to 40 Gbps of traffic. The FortiGate-5000 Series is an AdvancedTCA-compliant, blade-based firewall chassis targeted at large, complex networks and data center environments.

The company offers its FortiCarrier 5.0 software specifically for the multitenant aspects of firewall management — for carrier-class deployments including firewall and intrusion prevention/inspection capabilities specifically for GTP and SCTP, to protect the evolved packet core (EPC). FortiCarrier also includes a multimedia messaging service (MMS) as well as anti-spam and anti-fraud features, which are attractive to carrier deployments where MM1, MM4 and MM7 security inspection and enforcement capabilities are desired.

The FortiCarrier solution can be managed using the company's FortiManager Security Management product. FortiManager supports APIs, Web GUIs and CLIs, and can manage up to 5,000 virtual domains.

Fortinet offers its firewall on custom ASICs that offload and accelerate network security tasks, such as firewall, VPN and IPv6 translation in-silicon. The latest generation of these processors, NP6, supports offloading of IPv4 and IPv6 traffic, IPsec VPN encryption, CAPWAP traffic and multicast traffic. The NP6 has a capacity of 40 Gbps firewall throughput per processor. Fortinet also supports all major hypervisors (VMware, Xen, KVM, Hyper-V) for orchestrating virtual appliances for service insertion/chaining for NFV.

How This Provider Competes

Fortinet leverages its extensive channel and distribution network to compete head-to-head against its largest rivals in many regions of the globe. The company continues to orient itself to higher-end enterprise deals and has been taking some share against its rivals during the last year, based on annual Gartner market share estimates. In the carrier market, the company has been

most focused on beating the competition from a performance perspective, and actively markets its product's performance and deployment flexibility to meet the needs of carrier environments. Fortinet recently announced that it now has appliances capable of over one terabit per second (Tbps) firewall inspection performance. It uses this 1 Tbps performance as a proof point for carriers that require high throughput inspection requirements.

In August 2014, the company hired a new channel marketing veteran with a strong background in supporting channel-oriented organizations from market rival Juniper, which signals that the company is continuing to focus its efforts on channel execution and expansion. To help broaden the company's organic support, it recently expanded its training program with the announcement of a new network security expert certification, which includes eight levels ranging from entry-level training to architect-level.

Huawei

Estimated carrier revenue: $64.8 million

Market Overview

Huawei, headquartered in Shenzhen, China, was founded in 1987 and is the largest multinational telecommunications vendor worldwide. Its carrier products include solutions for fixed, mobile, over-the-top and cable operators for both networks and security. It also has products that serve enterprise and consumer markets. In 2013, Huawei released its Eudemon platform for mid- to low-end series products providing up to 40 Gbps throughput, with security capabilities including antivirus, URL, IPS functions and application, content, time, user, attack, location (ACTUAL) awareness and smart policy built in.

Huawei offers security firewall products in the enterprise and carrier spaces under different brands. For the enterprise market, Huawei offers the Unified Security Gateway (USG) series. For the carrier market, it offers the Eudemon 8000E and 1000E series. The platforms are built on the same chassis but offer some different features. Huawei kept the Eudemon brand for its familiarity among CSPs. The Eudemon 8000 series can provide up to 1 Tbps throughput performance and offers linear expansion capabilities as well as CGNAT, IPsec VPN tunneling, DPI, anti-DDoS and IPS functions. The Eudemon 8000E is available in COTS and proprietary formats and there are plans for it to support x86 and hypervisors for future SDN and NFV implementations. The Eudemon platform has generally been sold as part of end-to-end deployments with mobile and fixed broadband networks.

Value-add features include CGNAT features such as NAT64, 6RD, DS-lite; VPN features such as IPsec/IKEv2, GRE, L2TP and MPLS; and anti-DDoS features such as defense for both SYN/TCP/UDP flooding attacks and DNS/HTTP/NTP attacks.

How This Provider Competes

Huawei has been most successful with its firewall deployments in Asia/Pacific and has some presence in EMEA (for example, with Telefonica, T-Mobile, Swisscom, Turkcell, du, Telekom Austria and Etisalat), in Russia (VimpelCom and MegaFon, for example) and in CALA (Telefonica) regions. Its firewall solutions share similar command line configurations as its switches and routers, so maintenance costs can be reduced by managing them with the same network management system. Huawei sees this as a clear opportunity to market its firewall solutions to its existing large customer base. It also relies on a 100% direct sales model and does not engage in partners for technology that may limit its opportunity beyond its existing customer base. It is currently in internal discussions to cooperate with other technology vendors to gain visibility in the market.

Huawei has also been known for being competitively priced, which coupled with its ability to scale to 1 Tbps and linear expansion capabilities, gives it a slight competitive advantage in the CSP market. Offering low- to mid-end products in this space also gives the CSPs a variety to choose from in terms of scaling from 10 Gbps for specialized use cases to as high as 1 Tbps for extremely dense deployments where higher speeds are desired. Huawei also has good IPv6 capabilities and more IPv6 deployments than its competitors.

Its closest competitors are Check Point, Juniper, Fortinet and Cisco.

Intel Security

Estimated carrier revenue: $5.4 millions

Market Overview

Intel Security (formerly McAfee) entered the CCNFW market with the acquisition of Stonesoft.

Prior to the acquisition, the company focused most of its sales efforts in Europe and toward enterprise customers. Stonesoft was best known for its network-based anti-evasion capabilities and custom TCP/IP stack, which focuses on normalizing (anti-evasion) network traffic prior to firewall and threat inspection. In the carrier market, Intel Security currently offers its NGF-5206 and NGF-3206 high-availability firewall appliances supporting 120 Gbps and 60 Gbps of throughput, respectively. The company's offerings include firewall inspection features such as DPI, application control, anti-spam, antivirus, anti-evasion, botnet prevention, URL filtering and IPS. The Intel Security firewalls have extensive clustering capabilities that the company claims can create clusters with up to 16 nodes and five-nines reliability. In version 5.5 of the McAfee Next Generation Firewall, one physical appliance can now support up to 250 virtual network security devices (or Virtual Security Engines) to support carrier and service provider multitenant deployments. Intel Security also offers virtual appliances for both VMware and KVM hypervisor environments, and claims to support up to 8 Gbps of firewall throughput.

Intel Security also offers centralized management as part of its McAfee Security Management Center (SMC) software, which can be deployed on several versions of Windows and Linux. The SMC is designed with a customer Web portal capability and API integration that caters to carrier and managed security service provider deployments. Intel Security continues to work on rolling out updates to its management capabilities, both in its appliances and its centralized management console, but its current firewall offerings do not have per-appliance Web-based configuration capabilities. The company continues to improve software-defined network support and recently announced the availability of its Intel Security Controller, an SDN security service insertion orchestration layer for VMware environments. However, the product currently supports only the stand-alone network intrusion prevention appliances, not yet the next-generation firewall (NGFW) line of products.

How This Provider Competes

Intel Security is focused on monetizing both its Stonesoft and McAfee acquisitions and has gone through structural organizational changes during the last year that have positively impacted its sales organization and its marketing department. Intel Security has had a strong marketing program surrounding the sales of its NGFW products, with direct-to-channel marketing on channel websites such as CRN, The VAR Guy and MSPmentor. It has also been actively pursuing new resellers interested in selling its network security products lines.

Its channel marketing message contains the slogan "Extend your capabilities," aligned to value-add resellers that may not already be actively selling network security products. In its outbound marketing, the company's primary focus has been on messaging against advanced evasion techniques, where it feels the Stonesoft technology has a significant advantage against competitive TCP/IP stack normalization approaches. The Stonesoft acquisition is strategic in the way that it provides inroads to the carrier environment, particularly in the EMEA region. The company now needs to strengthen its marketing messages toward the needs of CSPs in order to gain more traction.

Juniper Networks

Estimated carrier market revenue: $310 million

Market Overview

Juniper Networks is a well-known vendor in the carrier space for routers, switches and security platforms. Its headquarters is based in Sunnyvale, California. It entered the network infrastructure market offering high-performance and a lower-cost alternative to its strongest competitor, Cisco.

In 2012, Juniper bought Contrail Systems, a manufacturer of an SDN controller, in response to CSPs moving toward SDN. It offers several security products for carriers grouped as the SRX Series Services Gateways, comprising the SRX1400, the SRX3K series (3400, 3600), and the SRX5K series (5400, 5600, 5800). Juniper introduced Services Processing Cards to the 5K series to enable the largest, the 5800, to support up to 300 Gbps firewall throughput. They include next-generation firewall protection with application awareness, IPS, user role-based control options, and UTM as part of their capabilities. As adjuncts, Juniper offers Firefly Perimeter and Junos DDoS Secure, and its MX series of routers can also be deployed as a service control gateway. These platforms and technologies can be deployed in either VM form factor or as hardware-based solutions. All are based on Juniper's Junos OS.

How This Provider Competes

Juniper leverages its vast ecosystem, spanning from system integrators such as Ericsson and Nokia to security vendors such as Verisign, Sophos and Websense. It chooses technology partners that it believes will provide best-of-breed security capabilities as well as build the cloud infrastructure needed to support a full NFV offering. Juniper also leverages its other key alliance partners such as IBM, Amdocs and Dimension Data. These partners extend and expand Juniper's global support and technologies — Nokia and Ericsson, for example, integrate and test Juniper's security products in end-to-end solutions, including its Mobile Security Gateway for securing mobile endpoints to mobile edge networks.

Juniper takes an overall insertion point strategy, approaching the CSP market by focusing on four verticals: fixed, mobile, cable and Web 2.0 providers, where each has a unique topology and protocols, and whose security needs should be approached differently. It has targeted solutions such as Firefly Perimeter and Junos DDoS Secure that provide a multitude of security needs in a variety of use cases. For example, managed security solutions for a wireline CSP and a mobile CSP radio access network (RAN) for encryption and security would require a different set of components and technologies, which Juniper can provide either in virtual form factors or as hardware-based solutions.

It also leverages its existing CSP relationships in the router space, where it has long been running second to Cisco. It also has a solid understanding of CSPs' needs in protecting its own assets, intellectual property (including customer and financial information) and customer data.

Palo Alto Networks

Estimated carrier revenue: $13.2 million

Market Overview

Palo Alto Networks was founded in 2005 and is best known for its introduction of the NGFW concept into the network firewall market. It offers an entire range of network appliances including offerings for carriers, high-end enterprises, midsize organizations and branch offices. The company gained attention with its application identification (App-ID) technology, which leverages DPI to identify and control applications versus ports and protocols. The company also met customer needs by introducing the first network firewall that detected advanced forms of malware entering networks — a service it calls WildFire. With the unknown forms of advanced malware it detects, it generates shared threat intelligence for blocking across its deployed customer base.

In the carrier market, the company currently offers its PA-7050 blade chassis and its Panorama management console. It also offers the PA-5060 platform that carriers are utilizing for smaller-scale deployments. The PA-7050 supports an array of inspection features including application visibility and control, VPN connectivity, intrusion prevention and URL filtering. The PA-7050 chassis supports up to six expansion network processing cards (NPCs), each with 20 Gbps of firewall throughput capacity (App-ID-enabled). NPCs can be combined to support up to 120 Gbits of combined firewall inspection throughput (App-ID-enabled) and up to 60 Gbps of threat inspection throughput, which includes IPS, antivirus, anti-spyware and botnet defense. Similar to alternative providers of CCNFW appliances, the PA-7050 offers virtual systems to support requirements for multitenancy managed services deployment (purchased as an additional license).

Along with the PA-7050, Palo Alto Networks also offers the VM-Series line of virtual appliances to support carriers' cloud and NFV initiatives. The same PAN-OS operating system that runs on both the physical and virtual platforms supports granular, role-based access control, which helps support both customers or managed security partners perform individual device management, and the segmentation of duties at the device level. Currently, the company's carrier offering does not offer Advanced Telecommunications Computing Architecture specification-compliant equipment.

The company's Panorama management console offers global device management for carriers. It also supports role-based access control, device groupings and policy templates to ease administration costs and enable carriers to operate managed security service operations more efficiently. In addition to Panorama, Palo Alto Networks offers CLI-, Web- and API-based management of its CCNFW platforms.

How This Provider Competes

Palo Alto Networks has built a significant business in the firewall market over a short period of time. The company entered the network firewall market with the right concept at the right time, when many organizations realized their port and protocol visibility was no longer enough to properly protect their enterprises. The company competes by leveraging its first-to-market solution for application identification and the single pass architecture approach to firewalling. Version 6 of PAN-OS offers DNS traffic monitoring and blocking to detect and prevent botnet command and control communications. Its most recent R&D activities have focused on evolving its appliance business toward support for NFV, virtualized environments and software-defined networks. It currently performs this integration through exposed Rest APIs.

In competitive deals, the company most commonly competes directly with Check Point, Fortinet and Juniper.

Stoke

Estimated carrier revenue: $16.0 million

Market Overview

Privately held, Stoke was founded in 2004 and is headquartered in Santa Clara, California. It is funded by a mixture of venture capitalists (Sequoia Capital, Kleiner Perkins, Focus Ventures, Samsung Ventures) and the telecom industry (NTT Docomo, Reliance Communications, Samsung, NetOne).

Stoke offers its Stoke Security eXchange (SSX-3000) gateway, which supports the key functions unique to the RAN-core border and essential to protecting user communications and mobile network infrastructure. It provides a high density of encrypted eNodeB S1 links and a rich, extensible set of features for IKE, PSK, PKI and IPsec, compatible with all major eNodeB provider and operator applications. It supports up to 80 Gbps throughput, 180,000 IPsec tunnels to the EPC, 104 million packets per second and less than 30 microseconds of latency when fully loaded. It also interoperates with all the major eNodeB vendors (Ericsson, Nokia Networks, Alcatel-Lucent, ZTE). The current operating system version is 13.1, and Version 14.1 is scheduled for release in the last quarter of 2014. Its OS software follows the Posix standard and can be used across multiple industry-standard platforms. It also offers an added feature called Mobile Border Agent, which further protects the EPC by monitoring signaling load and applying traffic-shaping policies or blacklisting to mitigate overload threats.

Stoke's platform already has separation of the control plane and data plane for independent scaling and deployment of the solution based on dynamic resourcing requirements. On the data plane, the operating system is architected for general-purpose multicore processors. Stoke is planning to launch its NFV-compliant product in the first half of 2015.

Stoke also offers its Systems Manager for managing networks of SSX-3000 security gateways. It's a browser-based GUI for network element status reporting, performance monitoring and troubleshooting. It also offers context-based node CLI access for configuration and deeper troubleshooting.

How This Provider Competes

Stoke's solution works as a full proxy and is essentially targeting the LTE network, particularly the S1 interface. It promises to encrypt and decrypt traffic at line rate and also conduct analysis of the specific protocols used in the RAN to EPC mobile access border without latency from the perspective of the control plane, user plane, session and RAN visibility, which is not a common function in other nodes.

Stoke also competes by leveraging its relationship with the EPC providers, as it can interoperate with the individual nodes in the EPC such as the MME, PDN and SGW. This will also expand its global customer reach as CSPs in EMEA and APAC continue to roll out LTE, LTE-A and VoLTE. It has strong marketing messages around the EPC and S1 interface protection, which resonate well with CSPs.

Stoke's competitive landscape includes wireless EPC providers such as Ericsson, Cisco and Alcatel-Lucent, where security functionality is built into their EPC products, as well as vendors in the traditional firewall space such as Check Point, Fortinet and Juniper.

References and Methodology

Gartner conducted interviews and briefings with the technology providers as well as a formal survey, to which all the technology providers responded. We also held discussions with the CSPs and conducted another survey.

Note 1
Network Service Header Proposed Draft RFC

See the full draft of the proposed Network Service Header here.

Acronym Key and Glossary Terms

ADC	Application delivery controller
API	Application programming interface
ASIC	Application-specific integrated circuit
CAPWAP	The Control and Provisioning of Wireless Access Points
CCNFW	Carrier-class network firewall
CGNAT	Carrier-grade NAT
CLI	Command line interface
COTS	Commercial off-the-shelf
DDoS	Distributed denial of service
DNS	Domain Name System
DPI	Deep packet inspection
EPC	Evolved packet core
GUI	Graphical user interface
IoT	Internet of Things
IP	Internet Protocol
IPS/IDS	Intrusion prevention/detection system
LTE	Long Term Evolution
LTE-A	LTE-Advanced
MSSP	Managed security service provider
NFV	Network function virtualization
NGFW	Next-generation firewall
POP	Point of presence
RAN	Radio access network
SDN	Software-defined networking
UTM	Unified threat management
VM	Virtual machine
VoLTE	Voice over LTE

Source: Gartner Research, G00261627, Deborah Kish, Lawrence Pingree, 10 October 2014

About Fortinet

Contact Us

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management, next generation firewall and high performance datacenter firewall. Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

A key differentiator, Fortinet's custom-built FortiASIC content and network processors enable our flagship FortiGate systems to detect and eliminate even complex, blended threats in real time without degrading network performance, while an extensive set of complementary management, analysis, database and endpoint protection solutions increases deployment flexibility, assists in compliance with industry and government regulations, and reduces the operational costs of security management.

US Headquarters
1090 Kifer Road
Sunnyvale, CA 94086
USA
Tel: +1-408-235-7700
Fax: +1-408-235-7737