Magic Quadrant for Enterprise Network Firewalls

7 February 2013 ID:G00229302

Analyst(s): Greg Young

VIEW SUMMARY

Advances in threats have driven mainstream firewall demand for next-generation firewall capabilities. Buyers should focus on the quality, not quantity, of the features and the R&D behind them. This market includes mature vendors and new entrants.

Market Definition/Description

The enterprise network firewall market represented by this Magic Quadrant is composed primarily of purpose-built appliances and virtualized models for securing corporate networks. Products must be able to support single-enterprise firewall deployments and large global deployments, including branch offices. These products are accompanied by highly scalable management and reporting consoles, products, and a sales and support ecosystem focused on the enterprise.

The firewall market has evolved from simple stateful firewalls to NGFWs, incorporating full-stack inspection to support intrusion prevention, application-level inspection and granular policy control. Such NGFWs will eventually subsume mainstream deployments of stand-alone network intrusion prevention system (IPS) appliance technology at the enterprise edge. Gartner already sees this shift in the form of reduced IPS buying activity and a flattening of IPS market growth, but Gartner believes the security-conscious segment of the market will continue to use separate IPSs. The reality of product life spans cannot be ignored in this market shift, however: Enterprises refresh individual firewalls, on average, every five years, and IPSs are refreshed about four years or less, so the market won't shift quickly.

Although firewall/VPN and IPS are converging, other security products are not. All-in-one or unified threat management (UTM) products are suitable for small or midsize businesses (SMBs) but *not* for the enterprise: Gartner forecasts that this separation will continue until at least 2016. Branch-office firewalls are becoming specialized products, diverging from the SMB products (for more information, see "Magic Quadrant for Unified Threat Management").

Gartner has successively increased the Magic Quadrant evaluation weighting for NGFW features. This edition signals a significant increase in the weighting of NGFW capabilities reflecting the changing markets and enterprise needs.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls

STRATEGIC PLANNING ASSUMPTIONS

Virtualized versions of enterprise network safeguards will not exceed 20% of unit sales by year-end 2016.

Through 2015, more than 75% of enterprises will continue to seek network security from a vendor different from their infrastructure vendor.

Less than 10% of Internet connections today are secured using next-generation firewalls (NGFWs). By year-end 2014, this will rise to 35% of the installed base, with 60% of new purchases being NGFWs.

ACRONYM KEY AND GLOSSARY TERMS

ADC	application delivery controller
AIM	accelerated interface module
AMC	Advanced Mezzanine Card
AIP-SSM	Advanced Inspection and Prevention Security Services Model
ASA	Adaptive Security Appliance
ASIC	application-specific integrated circuit
CEF	Common Event Format
CLF	Common Log Format
ELA	Enterprise License Agreement
ePO	ePolicy Orchestrator
FPM	firewall policy management
FIPS	Federal Information Processing Standard
FMC	Fortinet Mezzanine Card
Gbps	gigabits per second
GTI	Global Threat Intelligence
IOS	Internetwork Operating System
IP	Internet Protocol
IPO	initial public offering
IPS	intrusion prevention system
IPv6	Internet Protocol version 6
ISP	Internet service provider
LEEF	Log Event Enhanced Format
MFE	McAfee Firewall Enterprise
MSSP	managed security service provider
NAT	network-address translation
NGFW	next-generation firewall
NSM	Network Security and Manager
P2P	peer-to-peer
SMB	small or midsize business
NSA	Network Security Appliance

Source: Gartner (February 2013)

Return to Top

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks (www.barracudanetworks.com) acquired European firewall vendor phion in 2009. Barracuda has been focused primarily on selling to the low end of the midsize-enterprise market at low cost. The former phion firewall is now branded as the Barracuda NG Firewall family across a range of appliances and a virtual version. Barracuda is assessed as a Niche Player for enterprises, mostly because it serves a set of placements when the Leaders are otherwise not welcome. We do not see the Barracuda NG Firewall frequently displacing Leaders otherwise. The firewall has application control and reputation services, and the Barracuda NG Firewall Vx is a virtual version.

Strengths

- The Barracuda NG Firewall is a good option for Barracuda customers who want to get a firewall product from the same vendor, especially for those organizations that are outgrowing their current UTM and/or moving into point products.
- The Barracuda NG Firewall unit support staff offer good local language support, especially in Germany, Switzerland and Austria.
- The Barracuda NG Firewall is a strong competitor in situations where price is highly weighted in the selection.

Cautions

- Barracuda customers are primarily SMBs, and the vendor does not yet have well-established enterprise network security channels or support.
- No vendor we surveyed listed Barracuda as a significant enterprise competitive threat. Barracuda has not been visible on the firewall shortlists of Gartner customers. Most interest has been instead via incumbent customers who have other Barracuda products.
- Full Internet Protocol version 6 (IPv6) still needs to be implemented. Some clients Gartner interacted with commented that the IPS reporting could be improved.

Return to Top

Check Point Software Technologies

SSL	Secure Sockets Layer
USG	unified security gateway
UTM	unified threat management
VE	Virtual Edition
WELF	WebTrends Enhanced Log File Format
XCS	Extensible Content Security

EVIDENCE

This Magic Quadrant was conducted in accordance with Gartner's well-defined methodology. The analysis in this report was based primarily on interviews and interactions during firewall inquiries with Gartner clients since the last report. We also consider surveys completed by vendors, vendor briefings conducted at the vendors' request throughout the year, interviews with references provided by the vendors, and supporting Gartner quantitative research on market share.

Guidelines for responding to the full survey were provided at the time of issue of the survey. Responses were nevertheless of variable quality. Responses that were lower quality (for example, ignored the question, poor grammar, inability to explain key concepts, inability to provide high-quality explanations of use cases, and inability to go beyond technical capabilities and demonstrate an understanding of the business environment) or did not meet the guidelines generally tended to score lower. Vendors that declined to provide a survey response were assessed by Gartner as to what the likely reply would have been (usually this is in relation to specific revenue breakdowns). Some vendors declined to answer certain questions due to market restrictions and therefore did not fare as well under some of the scoring criteria.

We asked for a specific number of references from each vendor, and each reference customer is supplied with a structured survey. References are scored on the basis of both the quality of the reference and what they tell us. For each vendor, we take into account comments from both that vendor's own references, and what other vendors' customers say about that particular vendor. Vendors can be notably affected by the inability to have sufficient reference customers provide input.

NOTE 1
TYPE A, B AND C ENTERPRISES

Enterprises vary in their aggression and risk-taking characteristics. Type A enterprises seek the newest security technologies and concepts, tolerate procurement failure and are willing to invest for innovation that might deliver lead time against their competition; this is the "lean forward" or aggressive security posture. For Type A enterprises, technology is crucial to business success. Type B enterprises are "middle of the road." They are neither the first, nor the last, to bring in a new technology or concept. For Type B enterprises, technology is important to the business. Type C enterprises are risk-averse for

Check Point Software Technologies (www.checkpoint.com) is a well-known, pure-play security company with the largest firewall installed base, and strong and broad channel support.

The majority of enterprises choose to use Check Point-branded appliances, although options are also available for a software install on self-sourced servers, a virtual machine install (Secure Gateway Virtual Edition [VE]), or the remaining partners, such as Crossbeam (recently acquired by Blue Coat Systems). The IPSO and SecurePlatform operating systems are unified under the new GAiA operating system release.

Check Point has continued to expand its software "blade" strategy (that is, preloaded software modules enabled through subscription keys). Gartner believes that the blades, which match NGFW features (for example, IPS, user identity, application control and anti-bot), will continue to have high attach rates, but there will be little demand for some blades that enable other features (for example, email security and Web antivirus).

Check Point is assessed as a Leader for enterprises, because we continuously see the vendor competing in demanding selections, providing an NGFW development path that customers are asking for, and retaining customers based on its features and channel strength.

Strengths

- Check Point scored high as a significant enterprise competitive threat by all vendors Gartner surveyed. Gartner observes that Check Point is in most shortlists in which security protection is weighted highly. The Check Point Experience user events continue to be an effective platform for new announcements and maintaining loyalty.
- The Check Point management console is ranked highly by customers with a large number of firewalls with differing configurations or a significant compliance burden: Check Point continues to invest considerable intellectual property into the management console, in recognition of the importance configuration has to administrators in enterprise deployments. Surveyed clients were consistently managing complex environments with many firewalls and users.
- Check Point has a strong field of product options, such as Virtual Systems for virtualized firewalling, VE for running in virtualized environments, and its SmartEvent correlation product. The wide availability of appliance models and software options enables Check Point to meet the requirements for complex enterprise networks. Check Point has performed favorably on third-party IPS testing, and Gartner clients comment that the IPS is a significant improvement over previous Check Point IPS products.
- Check Point has good capability for meeting large-enterprise requirements with the newer high-end 21000 and 61000 series appliances.
- Check Point continues to have the strongest third-party ecosystem of security products that integrate easily with Check Point's management platform. Gartner has received positive feedback from clients regarding the stability and use of Check Point's GAiA operating system release.

Cautions

- High price is a common reason provided by Gartner customers for replacing or considering replacing Check Point firewalls. This is not an issue in new placements, in which a premium firewall function is required and justifies the investment. In firewall selections and support renewals, Gartner often hears that support pricing is complex, and price negotiations are difficult.
- Gartner views the Check Point Software Blade architecture as having only short-term attractiveness; it is a difficult long-term strategy option for enterprises. Enterprises are cautious about adding new functions to firewalls. With 12 blades now available for the Check Point firewall, Gartner believes charging for features that are included by competitors is challenging and can appear "UTM-like," thus alienating enterprises.
- In the survey to vendors, Check Point was listed second most often as the vendor they replace. Although a longtime Magic Quadrant Leader, Check Point needs to take a more aggressive R&D and marketing path if it wishes to change its current trajectory.
- Gartner believes the new managed security service provider (MSSP) offering will likely alienate some MSSP partners.

Return to Top

Cisco

Cisco (www.cisco.com) has an exceptionally broad network security product portfolio across the network security, Web security and email security tiers. Cisco has chosen to retain the Adaptive Security Appliance (ASA) firewall brand, and it has added application control under the CX feature brand and has appended the X designator as a suffix to newer models that include IPS. Cisco is assessed as a Challenger for enterprises over the evaluation period, because we did not see it frequently displacing Leaders based on vision or feature, and it does not effectively compete in the NGFW field that is visible to Gartner. Instead, Gartner sees Cisco winning mostly procurements through sales/channel execution or aggressive discounting for large Cisco networks when firewall features are not highly weighted evaluation criteria (that is, as part of a solution sell in which security is one component). Gartner expects IPS to be added to the CX models in 2013, whereas

procurement, perhaps are investment-challenged and are willing to cede innovation to others. They wait, let others work out the nuances and then leverage their learning; this is the "lean back" security posture more accustomed to monitoring rather than blocking. For Type C enterprises, technology is critical to the business and is clearly a supporting function.

NOTE 2
CONFUSION OF BUYERS CONCERNING WAFS

The advent of application control in firewalls has led to some natural confusion between the NGFW and WAF markets in the minds of buyers. These markets today remain very distinct. The critical difference is of direction: application control in NGFW is concerned primarily with applications external to the enterprise (for example, peer-to-peer and Facebook), whereas WAF is concerned with protecting custom Web applications on servers internal to the enterprise. Although a few firewalls offer optional WAF modules, these are rarely enabled; instead, we see WAF deployed either as a stand-alone product (such as from Imperva), an off-premises service (such as from Akamai), or within an ADC (such as from F5).

NOTE 3
FPM TOOLS

Third-party FPM vendors (such as AlgoSec, Tufin and FireMon) continue to exploit the absence of firewall consoles to optimize, visualize and reduce firewall rules and policies. Although the FPM market is still somewhat small, the customers requiring help with complexity are the very largest, and the market is growing. Additionally, very large enterprises may have firewall products from different vendors — usually by accident via acquisition, rather than through choice, because a single vendor solution is usually the best choice. All FPM vendors support multiple firewall products, whereas no firewall vendor will effectively manage a competing product, and FPM vendors are expanding into managing other network security devices, such as IPS.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product / Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution / Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be

currently a choice must be made: either application control or IPS. Also in 2013, a single management console is likely (for more information, see "Vendor Rating: Cisco").

Strengths

- Cisco has significant market share in security. The new option for an Enterprise License Agreement (ELA) for security software and hardware is of interest to Cisco security customers who are undertaking multiyear deployments and wish to maintain a timetable and product flexibility.
- Gartner clients consistently rate as excellent the Cisco support network, which is the most-often-cited reason for loyalty to Cisco security products. The vendor has strong channels, broad geographic support and the availability of other security products. Surveyed Cisco firewall clients consistently ranked having other products from this vendor as the most important factor in the selection.
- Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall ASA, with firewalls also available via the Firewall Services Module blade for 6500 series switches, Cisco ASA 1000V Cloud Firewall, and on Cisco's Internetwork Operating System (IOS)-based Integrated Services Router.
- The integration of reputation features across Cisco security products is a differentiator that is often missed in enterprise selections. Although many competitors have reputation features, the breadth of the Cisco reputation feed is a quality factor.

Cautions

- Cisco firewall products are selected more often when security offerings are added to Cisco's infrastructure, rather than when there is a shortlist with competing firewall appliances. Cisco was listed by competitors as the product they most often replace. Gartner does not view Cisco's security strategy as messaging effectively in the broader NGFW market.
- The requirement to add a hardware module (the Advanced Inspection and Prevention Security Services Model [AIP-SSM]) to add IPS capability to some models of ASA firewall appliance remains a barrier to deployment and a competitive disadvantage for branch-office deployments. The add-in module does, however, provide processing help with the deep inspection load. If the SSM module is used for IPS, then it cannot be used for other content inspection. However, Gartner does not expect Cisco to continue selling the non-X models beyond 2014.
- The security strategy, product offering nomenclature and product descriptions are often cited by Gartner clients as confusing and orthogonal to competitors' terms and road maps. By using terms such as "context-aware" and "CX" rather than application control or NGFW, Cisco is sometimes excluded as clients experience confusion in comparing Cisco's offering to competitors' offerings.

Return to Top

Dell SonicWALL

SonicWALL (www.sonicwall.com), formerly owned by Thoma Bravo and acquired in 2012 by Dell, is now renamed Dell SonicWALL and is headquartered in California. Although the majority of Dell SonicWALL's business had been selling UTM to SMBs, the SuperMassive line is aimed at the high end at very competitive price/performance points. Other Dell SonicWALL security products include Secure Sockets Layer (SSL) VPN, email security gateways, clean wireless and backup/recovery offerings. The company's firewall offerings are in four branded lines: SuperMassive, E-Class Network Security Appliance (NSA), NSA and TZ. Dell SonicWALL is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well (for example, retail, upper-midsize businesses and service providers), and we do not see it often displacing Leaders.

Strengths

- Dell SonicWALL's broad model range is a good option for wide remote-office deployments requiring many smaller devices, such as in retail or franchise outlets, or with Type C enterprises (see Note 1). The Dell acquisition represents a broader channel for SonicWALL products, especially into midsize organizations or organizations that already have a strong Dell relationship.
- Dell SonicWALL has improved its enterprise go-to-market ability, rather than attempting to push an SMB UTM upmarket, by aligning product lines specifically to the horizontal — SuperMassive for data centers, service providers and ISPs, and the E-Class NSA for enterprises.
- The SuperMassive line has achieved market traction in high-throughput firewall deployments, such as carriers and service providers, in which firewall throughput, low latency and price are foremost. Clients that Gartner surveyed liked the high performance of the SuperMassive appliance.

Cautions

- Most of Dell SonicWALL's firewall and other security product lines have been primarily SMB-focused and not competitive in most enterprises. Dell SonicWALL does not yet have a broad-enough enterprise channel, support and management console features to be considered in competition with the Leaders and to become a bigger part of the NGFW conversation. Some

driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical / Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

clients that Gartner interacts with have reported that the console management of the SuperMassive appliance needs integration improvements for the lower-tier firewall appliances.

- Dell SecureWorks presents a channel conflict for sales to other MSSPs, which can view Dell SonicWALL as part of a competitor. Gartner rarely sees Dell SonicWALL in most Type A and Type B enterprise firewall selections.
- Dell SonicWALL scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in the Gartner customer base. Although it has a good NGFW feature set, Dell SonicWALL has not been visible in NGFW selections as seen by Gartner.

Return to Top

Fortinet

California-based Fortinet (www.fortinet.com) has long focused on using purpose-built hardware to produce UTM appliances at strong price/performance points. Although the firewall features in its UTM products met most of the needs of firewall-focused large-enterprise buyers, Fortinet's approach and philosophy continue to be focused on "everything in one box," which has caused its brand and channel support to be slow to evolve from its SMB base. Fortinet continues to make progress within the Gartner customer base, usually by expanding out from branch-office or retail deployments to capture the primary or core firewalls, and it is seen winning some data center implementations. Fortinet is a significant threat to competitors in this market because of the company's hardware expertise, competitive pricing and steady revenue growth. Fortinet is a viable shortlist contender for most of the enterprise firewall market. It is assessed as a Challenger mostly because we see it displacing competitors on value and performance, but not often beating Leaders in mainstream enterprise selections. Fortinet has steadily been expanding its support offerings to be better-aligned to the enterprise, including options for dedicated technical account managers.

Strengths

- Fortinet has a large R&D team and uses this to outmaneuver competitors that often rely on OEM arrangements. Fortinet continuously delivers new features in the application-specific integrated circuit (ASIC) and operating system, providing extensive pressure on competitors and pleasing the channel. Fortinet maintains road map agility to get to the market quickly, with new features that are fully console-integrated. This also has enabled Fortinet to expand its portfolio of nonfirewall network security offerings, which provides increasing cross-selling opportunities.
- Fortinet continues to increase its wins against the larger firewall incumbents when customers are deploying in emerging areas — such as in-the-cloud firewalls, MSSPs and service providers — and carriers and ISPs are deploying in areas in which high-end performance is required. Fortinet is price-competitive, especially when using multiple virtual domains, and appliance reliability is reported as very high. Fortinet has invested significantly in obtaining and completing certifications.
- Its firewalls have high-end performance from purpose-built hardware and a wide model range, including bladed appliances for large enterprises and carriers, as well as SMB and branch-office solutions. Although many competitors are increasing their reliance on chips from Intel or other third-party providers for their future performance gains, Fortinet (much as in its software development) maintains control of its own dual processors — one ASIC for network security operations and the second for content inspection.
- The Fortinet Mezzanine Card (FMC) and Advanced Mezzanine Card (AMC) accelerated interface modules (AIMs) are options for some enterprises and carriers to expand performance or networking interfaces without having to resort to appliance replacements.

Cautions

- Management capabilities were most often listed as the reason when Fortinet was shortlisted but not selected in enterprises. However, where aggressive console use is not required, or where multiple firewalls share the same policy, the Fortinet console is highly competitive.
- Fortinet does not have a dedicated NGFW, but instead presents its UTM product, expecting a subset of product features to be used. Fortinet's marketing focus on using UTM for enterprises has persisted in what is effectively an attempt to change enterprise buying behavior. This can steer away enterprise customers. Fortinet also has historically defined enterprises as 500 users — about half the number used by Gartner and competitors. The UTM messaging also has enterprises excluding Fortinet from NGFW shortlists, even when the necessary capabilities (such as application control) are present.
- Gartner believes Fortinet does not have a strong third-party security vendor ecosystem, and Fortinet does not hold any customer conferences.

Return to Top

HP

Acquired in 2009 as part of HP's acquisition of 3Com, China-based H3C Technologies was formed as a joint partnership between Huawei and 3Com, and it has been shipping firewalls since 2003. Now that H3C is part of HP (www.hp.com), the former H3C firewalls are being leveraged by HP, especially in its current customer base. Models include the HP F5000 and F1000 (also called the A Series Firewalls in some marketing material), an add-in module for switches, the HP Threat Management Services zl

module, and firewall software that can be added to the HP E5400 zl and E8200 zl series switches. HP is assessed as a Niche Player primarily because of its geographic sales and presence, and the current absence of NGFW features, such as IPS and application control. (See "Vendor Rating: HP" for more information.)

Strengths

- HP and legacy H3C have a strong regional presence in China and the Asia/Pacific region, and sales are increasing for incumbent HP networking customers. HP and H3C firewalls will be of most interest to China-based enterprises, especially where other H3C or 3Com networking equipment is used.
- There is a wide range of models (including a high-throughput, blade-based chassis), branch-office models and enterprise models, all with a flat-fee URL model.
- It has broad IPv6 support.

Cautions

- HP firewalls are not visible outside the Asia/Pacific region, and HP has to address concerns from many geographies about relying on technology developed in China. This situation has led to HP having to recommend competitors' firewall products as optional replacements for HP firewall products' end of life.
- The firewall lacks certifications and third-party testing, such as Common Criteria for Information Technology Security Evaluation, which is usually seen in enterprise contenders.
- HP does not currently have a coherent network security strategy that is able to challenge market Leaders.

Return to Top

Huawei

China-based Huawei (www.huawei.com) has been shipping firewall products for almost a decade (for more information, see "Vendor Rating: Huawei").The range of appliances and models is extensive, especially for higher-throughput options, and for customers who already have Huawei products and wish to expand that business to firewalls. Unified security gateway (USG) is the primary enterprise line, and Eudemon is the line for carriers and service providers. The majority of Huawei firewalls are sold to carriers, ISPs and cloud and service providers. Although Huawei has received negative coverage in North America and Europe regarding suspicions of "back doors," this is not a concern in all regions and verticals.

Strengths

- Gartner assesses Huawei as having a very good overall network security strategy.
- Customers whose networks are based primarily on Huawei infrastructure products can include Huawei firewalls.
- The top end of the Huawei firewall line has a very high throughput and is a good shortlist candidate for carriers.

Cautions

- The majority of Huawei firewalls have very little visibility outside the Asia/Pacific region; however, placements in EMEA represent a significant share.
- Despite significant steps undertaken by Huawei to address concerns about relying on technology developed in China, the concerns remain for many prospective customers.

Return to Top

Juniper Networks

Firewall offerings of California-based Juniper Networks (www.juniper.net/us/en) are in multiple model lines: SRX, SSG, ISG and vGW. The Juniper SRX firewall, the primary firewall offering, offers a router as a basic element of the firewall, and it runs the same Junos operating system as is on other Juniper infrastructure components. Having routing in the firewall is of interest to a narrow segment of customers. Juniper has AppSecure for application control and visibility, and it has added a hypervisor-based stateful firewall under the vGW product name. Juniper's Junos Space Security Design is the successor product for the current security management within Juniper Network Security and Manager (NSM). Juniper is assessed as a Challenger for enterprises, because we see Juniper selected in concert with other Juniper offerings, rather than displacing competitors based on its vision or features. Juniper is, however, often shortlisted and/or selected in mobile service provider deployments and enterprise data center deployments, primarily because of price and high throughput on its largest appliances. Gartner sees Juniper mostly selected as an adjunct to the Juniper network infrastructure business.

Strengths

- Customers whose networks are already standardized on Juniper's Junos-based infrastructure products can benefit from the Space Security Design console, as it is part of the Junos Space

network management platform.

- Where Juniper was selected, clients cited a global logistics channel and/or good price for high firewall throughput.
- Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models. Juniper has a strong range of branch-office firewalls complementing the enterprise products. Its branch-office firewalls include WAN optimization controller and an Avaya voice gateway.

Cautions

- As a network infrastructure vendor, Juniper is sometimes at a disadvantage selling into Cisco networks, where buying any Juniper security equipment can be resisted as a Cisco network equipment replacement. Some Gartner clients report that having Security Design as part of Space can be perceived as a challenging proposition versus pure-play dedicated firewall consoles. Juniper clients that Gartner interacts with have commented that Space Security Design is not yet fully featured.
- Gartner does not assess Juniper as having a highly compelling or differentiated security vision, or one well-known to non-Juniper customers. Juniper's emphasis on the Mykonos technology is not effective with network buyers in competing with the NGFW messaging of Leaders. Gartner rarely sees Juniper considered on shortlists by customers looking for an NGFW and instead sees Juniper more often mentioned by customers looking to replace a firewall.
- Gartner believes that most enterprises want an operating system in their security products that differs from the one in infrastructure components.

Return to Top

McAfee

McAfee (www.mcafee.com/us) was acquired by Intel in early 2011. McAfee obtained its firewall products through the acquisition of Secure Computing in late 2008. The former Sidewinder product has been renamed to the McAfee Firewall Enterprise. McAfee has seven product models and a VX virtualized version. The McAfee Firewall Enterprise is certified for use on Crossbeam X-Series blades, CloudShield CS-4000 and Riverbed Steelhead appliances.

The road map for Firewall Enterprise is more important for consideration than the current features in the product. A re-engineered Firewall Enterprise integrated with the McAfee IPS on a purpose-built hardware platform will be the milestone for which to watch and a road map toward an NGFW. McAfee is assessed as a Niche Player for enterprises, mostly because it serves a set of placements when the Leaders are otherwise not welcome.

Strengths

- The wide breadth of the McAfee Global Threat Intelligence (GTI) reputation feed is a positive quality element, as is the TrustedSource feature used to block known bad Internet Protocol (IP) addresses.
- The McAfee Event Reporter for Firewall provides guidance on firewall configuration and is included with the product. MFE has good identity and geolocation options.
- Visibility of ePolicy Orchestrator (ePO) host information within the firewall reporting and console tools is of interest to current McAfee ePO customers.
- The "one price" of Firewall Enterprise is an advantage versus the complex pricing schemes of many competitors. URL filtering is included at no charge.

Cautions

- Gartner believes that the Intel acquisition has presented a significant distraction for the McAfee network security unit. Gartner security analysts always believed that the network security appliance business made no sense for Intel and believe that this has proven true in the market.
- Although it has been four years since the acquisition of Secure Computing, the McAfee IntruShield IPS engine, available in the stand-alone IPS appliances, is not yet integrated into the Firewall Enterprise. The current Firewall Enterprise IPS capabilities are not competitive with leading NGFW vendors' capabilities, and users generally comment negatively to Gartner on the IPS configuration and performance.
- McAfee is rarely seen on Gartner client network firewall shortlists; however, when it is, the time taken to navigate the general McAfee support system is the most often listed criticism heard from Gartner clients during the selection process. McAfee was not listed by any vendor we surveyed as a significant enterprise competitive threat. Declining to participate in NSS Labs' firewall evaluation has not helped McAfee's visibility.

Return to Top

Netasq

Netasq (www.netasq.com) has been a pure-play network security vendor headquartered in France for more than a decade, selling firewalls, vulnerability management and messaging security gateways. The acquisition of Netasq by Cassidian CyberSecurity (an EADS company) is now completed. Netasq

will continue to operate as an independent company. Netasq products mostly appeal to both EU-based midsize businesses and enterprise companies. Virtual versions are also available in the V line. Netasq is assessed as a Niche Player for enterprises, mostly because it best serves midsize businesses, and agencies in portions of EMEA, or when the Leaders or Challengers do not have the usual advantages. Feature sets are divided between enterprise and UTM lines.

Strengths

- By not using traditional signatures and, instead, focusing on heuristics, Netasq has innovated on an IPS path that is different from mainstream firewall vendors, which has positioned it more uniquely for countering new kinds of attacks. Users report that they like its policy-based management and real-time policy warning.
- It is VPN-certified for "EU Restricted" use in the EU, which is of interest to governments and agencies looking for simpler procurement.
- Netasq gets good marks from midsize enterprises for features and ease of use, and it has good channel support in EMEA.
- Netasq users comment to Gartner that the branded training and EU support are very good. Cassidian projects can include Netasq firewalls as part of the solution.

Cautions

- The majority of Netasq's penetration, visibility and channel is focused on EMEA, especially France.
- Although having a good feature set, Netasq has not been part of NGFW selections as seen by Gartner because of the company's low visibility in other geographies.

Return to Top

Palo Alto Networks

Palo Alto Networks (www.paloaltonetworks.com) is a California-based pure-play network security company. Palo Alto Networks had a widely publicized initial public offering (IPO) in July 2012, added a virtual version, and held its first user conference. Palo Alto Networks continues to both drive competitors to react in the firewall market and to move the overall firewall market forward. It is assessed as a Leader, mostly because of its NGFW design, direction of the market along the NGFW path, consistent displacement of competitors, rapidly increasing revenue and market share, and market disruption that forces competitors in all quadrants to react.

Strengths

- A crisp focus on enterprise NGFW features and messaging is viewed positively by firewall operators in enterprises.
- Gartner clients consistently rate the Palo Alto Networks application identification (App-ID) and IPS higher than competitors' offerings for ease of use and quality. The firewall and IPS are closely integrated, with App-ID implemented within the firewall and throughout the inspection stream. This "single pass" is a design advantage versus unnecessary inspection that can occur in competing products that process traffic in serial order — from firewall to IPS, and then to application control.
- Palo Alto Networks continued through 2012 to generate the most firewall inquiries among Gartner customers by a significant margin. Palo Alto Networks was consistently on most NGFW competitive shortlists, and we observed high customer loyalty and satisfaction from early adopters. A simple pricing structure helps in procurements versus competitors who charge for features that Palo Alto includes.
- Most firewall vendor road maps are following the Palo Alto Networks NGFW road map, placing these vendors at a competitive disadvantage.

Cautions

- The PA series of firewalls do not yet have certification at the EAL4+ level for the Common Criteria for Information Technology Security Evaluation.
- Palo Alto Networks does not have appliances with the higher throughput of some competitors, meaning they are less often considered for larger data center placements.
- The company does not have products in adjacent security markets, which would allow for cross-selling opportunities. The company has room to develop a third-party product support ecosystem.
- With product pricing higher than that of competitors that have fewer features, Palo Alto Networks is challenged to win RFPs, whereby price is the greatest weighted factor, especially for selections that are firewall only (that is, no IPS or application control).

Return to Top

Sophos

Security company Sophos (www.sophos.com) has co-headquarters in the U.K. and the U.S. The Sophos UTM necessarily targets SMBs. Gartner observes Sophos usually scoring highly where price is

the primary factor and where Sophos products are already in place. Sophos is assessed as a Niche Player for enterprises, mostly because it wins over Leaders in some selections based on features or with a very specific channel. The Sophos UTM is available as an appliance or software load, and as a certified Amazon Virtual Private Cloud connector, and it has application control.

Strengths

- Sophos' endpoint product customers can have the same vendor provide them their UTM solution.
- Users like Sophos' price, and surveyed users consistently comment on the ease of installation as a strong point.
- A free firewall is available in the "UTM Essential Firewall" edition that includes firewall, network-address translation (NAT), routing and Web GUI. The free edition runs on a PC, within a virtual machine or in the VMware vSphere Edition.
- The Sophos blog has been a visible medium in the security ecosystem for establishing Sophos as a broader security participant.

Cautions

- The Sophos firewall is not often seen in enterprise selections in the Gartner client base. As a UTM, the product is not a match for most enterprises and instead is seen more often in SMBs. The Sophos UTM usually competes with other SMB firewall vendors' solutions.
- Sophos was not listed by any vendor we surveyed as a significant enterprise competitive threat, and it has not been highly visible on NGFW shortlists among Gartner clients.

Return to Top

Stonesoft

Headquartered in Finland, public company Stonesoft (www.stonesoft.com) has expanded its operations into North America and other geographies, especially Eastern Europe. Stonesoft is focused on network security and has been very innovative in analyzing threat evasion techniques, and it is known for its well-functioning clustering and active-active options. Stonesoft is assessed as a Visionary for enterprises, because it has firewall features that are not seen in many competitors' products, and its firewall features are both innovative against modern and advanced threats and focused on the enterprise. Stonesoft also provides stand-alone IPS and SSL VPN products. The StoneGate brand has been dropped in favor of the Stonesoft name. The Stonesoft NGFW product is offered across a wide range of appliances, including branch office and a virtualized firewall version that is certified for VMware. Furthermore, the MIL-320 model was introduced as a military-grade ruggedized appliance.

Strengths

- Stonesoft's threat research concerning evasive attacks has increased security credibility and visibility for the company and products. As a company headquartered neither in the U.S. or China, Stonesoft is being shortlisted where enterprise operations span multiple countries, including the U.S. and China.
- Stonesoft has a long legacy with high-availability technology, and it has very reliable clustering and active-active deployability. Almost all surveyed Stonesoft clients ranked these features as important in their selections.
- The Stonesoft Management Center console can send and receive logs in multiple formats — such as syslog, Common Event Format (CEF), Log Event Enhanced Format (LEEF), Common Log Format (CLF) and WebTrends Enhanced Log File Format (WELF) — from non-Stonesoft devices to aid in correlation and reporting.
- Support pricing is slightly lower than the industry average, and it has a loyal customer base.

Cautions

- Stonesoft has limited market visibility and channel strength outside of EMEA, and it has low visibility within the Gartner customer base, although its firewall and company revenue has increased also outside of EMEA.
- Although the Stonesoft product has many next-generation features, the Stonesoft brand is not yet widely known.

Return to Top

WatchGuard

WatchGuard (www.watchguard.com) is a Seattle-based network security company that has primarily seen success in selling UTM products to midsize enterprises. Its XTM series of products span performance and feature ranges demanded by large enterprises; however, WatchGuard's branding, channel support and management capabilities tend to be more oriented toward SMBs. A well-established security-focused company, WatchGuard also has products that include SSL VPN and the Extensible Content Security (XCS) email and Web security line. The XTM-branded firewall models fall into two categories. The XTM 2 Series and XTM 5 Series are UTM, and the XTM 8 Series and the XTM 1050 and 2050 models are targeted for the enterprise. One important strategic improvement has

been WatchGuard's introduction of the "NGFW Bundle" option for appliances that is better-suited to enterprise buyers than the UTM-only approach. WatchGuard is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well, and we do not see it often displacing Leaders. In May 2012, WatchGuard obtained EAL4+ Common Criteria certification for the XTM line.

Strengths

- WatchGuard's strong price/performance has enabled it to win price-sensitive competitions across retail, branch-office, remote-office and Type C enterprise deployments. Gartner has observed an increase in visibility of WatchGuard in client inquiries since the last report.
- Users report high satisfaction with the reporting function in the WatchGuard management console. Enterprise models are correctly targeted at NGFW, rather than UTM functionality.
- WatchGuard's products have a low rate of product vulnerabilities compared with most competitors' products.
- The new RapidDeploy feature is of interest in areas where many firewalls will be deployed, such as in franchises or retail, or via an MSSP.

Cautions

- Gartner rarely sees WatchGuard in most Type A and Type B enterprise firewall selections. Enterprise channel and support will need to be expanded if WatchGuard wishes to compete in a broader segment of enterprises.
- Although having a good NGFW feature set, WatchGuard has not been part of many NGFW selections as seen by Gartner. WatchGuard clients that Gartner interacts with generally reported the IPS quality as being average.
- WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed and has low visibility in the Gartner customer base.

Return to Top

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Return to Top

Added

Huawei was added.

Dell acquired SonicWALL, which was in the previous Magic Quadrant, but the name has now changed.

Return to Top

Dropped

No vendors were dropped. AhnLab, Sourcefire, Cyberoam and F5 were examined as part of this analysis but did not yet meet the inclusion criteria at the time of the analysis of this report.

Return to Top

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall companies that meet the market definition and description were considered for this report under the following conditions:

- Gartner analysts assess that the company has an ability to effectively compete in the enterprise firewall market.
- Gartner clients generate inquiries about the company.
- The company regularly appears on shortlists for selection and purchases.
- The company demonstrates a competitive presence in enterprises and sales.
- Gartner analysts consider that aspects of the company's product execution and vision merit inclusion.
- The vendor has achieved enterprise firewall product sales (not including maintenance) in the past calendar year of more than $10 million and within a customer segment that is visible to Gartner.

Exclusion Criteria

Network firewall companies that were not included in this report may have been excluded for one or more of the following conditions:

- The company did not meet the inclusion criteria.
- The company has minimal or negligible apparent market share among Gartner clients, or it is not actively shipping products.
- The company is not the original manufacturer of the firewall product. That includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and ISPs that provide managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall, and we do not rate platform providers separately.
- The company's products sell as network firewalls, but do not have the capabilities, scalability and ability to directly compete with the larger firewall product/function view. Products that are suited for SMBs, such as UTM firewalls or those for small office/home office placements, are not targeted at the market this Magic Quadrant covers (enterprise) and are excluded.
- The company has primarily a network IPS with a non-enterprise-class firewall.
- The company has personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls (WAFs; see Note 2) — all of which are distinctly separate markets.

Return to Top

Evaluation Criteria

Ability to Execute

- *Product or service:* This includes service and customer satisfaction in enterprise firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that products are successfully and continuously deployed in enterprises, and the company wins a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and generate a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size or market share, although those factors can affect a company's ability to execute. Sales are a factor; however, winning in competitive environments through innovation and quality of product and service is foremost over revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and being able to support complex deployments and modern demilitarized zones. Having a low rate of vulnerabilities in the firewall is important. Logistical capabilities for managing appliance delivery, product service and port density matter. Support is rated on quality, breadth and value of offerings through the specific lens of enterprise needs.
- *Overall viability:* Overall business viability includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security markets. Growth of the customer base and revenue derived from sales are also considered. All vendors were required to disclose comparable market data, such as firewall revenue, competitive wins versus key competitors (and the wins are compared with Gartner data on such competitions held by our customers), and devices in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Instead, we consider use of these firewalls to protect the key business systems of enterprise clients and presence on competitive shortlists.
- *Sales execution/pricing:* We evaluate the company's pricing, deal size, installed base and use by enterprises, carriers and MSSPs. This includes the strength of the vendor's sales and distribution operations. Presales and postsale support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, including the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains. Cost of ownership over a typical firewall life cycle (three to five years) was assessed, as was the pricing model for conducting a refresh while staying with the same product and replacing a competing product without intolerable costs or interruptions. The robustness of the enterprise channel and third-party ecosystem is important.
- *Market responsiveness and track record:* This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's history of responsiveness to changes in the firewall market and how enterprises deploy network security.
- *Market execution:* Competitive visibility is a key factor, including which vendors are most commonly considered top competitive solutions, during the RFP and selection process, and which are considered top threats by each other. In addition to buyer and analyst feedback, this ranking looks at which vendors consider each other to be direct competitive threats, such as driving the market on innovative features co-packaged within the firewall, or offering innovative

pricing or support offerings. An NGFW capability is heavily weighted, as are enterprise-class capabilities, such as multidevice management, virtualization, adaptability of configuration and support for enterprise environments. Unacceptable device failure rates, vulnerabilities, poor performance and the inability of a product to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.

- *Customer experience and operations:* This includes management experience and track record, as well as the depth of staff experience specifically in the security marketplace. The greatest factor in this category is customer satisfaction throughout the sales and product life cycle. Low latency, throughput of the IPS capability and how the firewall fared under attack conditions are also important. Succeeding in complex networks with little intervention (for example, one-off patches) is highly considered.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	Standard
Customer Experience	High
Operations	Standard

Source: Gartner

Completeness of Vision

- *Market understanding and strategy:* This includes providing a track record of delivering on innovation that precedes customer demand rather than an "us too" road map. We also evaluate the vendor's overall understanding and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning road maps. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor and against future trends identified in Gartner research. Vendors cannot merely state an aggressive future goal; they must put a plan in place, show that they are following their plan and modify their plan as they forecast the market directions will change. Understanding and delivering on enterprise firewall realities and needs are important, and having a viable and progressive road map and delivery of NGFW is weighted very highly. The NGFW capabilities are expected to be integrated to achieve both correlation improvement and functional improvement.
- *Sales strategy:* Sales strategy includes preproduct and postproduct support, value for pricing, and providing clear explanations and recommendations for detection events. Building loyalty through credibility with full-time enterprise firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security buying center correctly, and to do so in a technically direct manner, rather than selling just fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on enterprises.
- *Offering strategy:* This criterion focuses on a vendor's product road map, current features, NGFW integration, virtualization and performance. Credible independent third-party certifications include the Common Criteria for Information Technology Security Evaluation. Integration with other security components is also weighted, as well as product integration into other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office. Innovation such as introducing practical new forms of intelligence that the firewall can apply policy to is highly rated.
- *Business model:* This includes the process and success rate for developing new features and innovation, and R&D spending.
- *Vertical, industry and geographic strategy:* This includes the ability and commitment to service geographies and vertical markets, such as complex enterprise international deployments, MSSPs, carriers or governments.
- *Innovation:* This includes R&D and quality differentiators, such as:
  - Performance, which includes low latency, new firewall mechanisms and achieving high IPS throughput and low appliance latency
  - Firewall virtualization and securing virtualized environments
  - Integration with other security products
  - Management interface and clarity of reporting — the more a product mirrors the workflow of the enterprise operation scenario, the better the vision

- "Gives back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity

Products that are not intuitive in deployments or operations are difficult to configure or have limited reporting, and they are scored accordingly.

The more a product mirrors the workflow of the enterprise operation scenario, the better the vision. Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Low

Source: Gartner (February 2013)

Quadrant Descriptions

Leaders

The Leaders quadrant contains a mix of large and midsize vendors, with the common element of making products that are built for enterprise requirements. These requirements include a wide range of models, support for virtualization and virtual LANs, and a management and reporting capability that is designed for complex and high-volume environments, such as multitier administration and rules/policy minimization. An NGFW capability is an important element as enterprises move away from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new safeguarding features, providing expert capability, rather than treating the firewall as a commodity, and having a good track record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss and options for hardware acceleration.

Return to Top

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not leading with features. Many Challengers are slow to work toward or do not plan for an NGFW capability, or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challenger products are often well-priced and, because of their strength in execution, vendors can offer economic security product bundles that others cannot. Many Challengers hold themselves back from becoming Leaders because they are obligated to place security or firewall products as a lower priority in their overall product sets. Firewall market Challengers will often have significant market share but trail smaller market share Leaders in the release of features.

Return to Top

Visionaries

Visionaries have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete with leaders and challengers. Most visionary products have a good NGFW capability but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations willing to update products more frequently and switch vendors if required. Where firewalling is a competitive element for an enterprise, Visionaries are good shortlist candidates. Vendors that do not have NGFW capabilities are adding them in a defensive move, while those with strong NGFW offerings are focused on manageability and usability. Gartner expects the next wave of innovation in this market to focus on better identification of malicious protocols at multi-Gbps rates.

Return to Top

Niche Players

Most vendors in the Niche Players quadrant are smaller vendors of enterprise firewalls, makers of multifunction firewalls for SMBs, or branch-office-only product makers attempting to break into the enterprise market. Many Niche Players are making larger SMB products, with the mistaken hope that this will satisfy enterprises. Some enterprises that have the firewall needs of an SMB (for example, some Type C "risk-averse" enterprises) may consider products from Niche Players, although other models from Leaders and Challengers may be more suited. If local geographic support is a critical factor, then Niche Players can be shortlisted.

Return to Top

Context

The enterprise firewall market is one of the largest and most mature security markets. It is populated with both mature vendors and some more recent entrants. Changes in threats, as well as increased enterprise demand for mobility, virtualization and use of the cloud, have increased demand for new firewall features and capabilities. Organizations' final product selection decisions must be driven by their specific requirements, especially in the relative importance of management capabilities, ease and speed of the deployment, acquisition costs, IT organization support capabilities, and integration with the established security and network infrastructure.

Return to Top

Market Overview

As the first line of defense between external threats and enterprise networks, firewalls need to continually evolve to maintain effectiveness, responding both to changes in threats and changes in enterprise network speed and complexity. The firewall market is highly penetrated in the larger markets (North America and Western Europe), which means to protect their installed base, incumbents must add improved capabilities and increase performance, or face either replacement by innovative new market entrants or commoditization by low-cost providers. Firewall policy management (FPM) products are increasingly used for managing complexity (see Note 3).

Next-Generation Firewalls

One key area of firewall evolution has been support for what Gartner called in 2009 "next-generation firewall" features — namely, integrated deep packet inspection intrusion detection, application identification and granular control. The key differentiators in these areas are IPS effectiveness, as demonstrated through third-party testing under realistic threat and network load conditions, and fine-grained policy enforcement in about the top 25 business applications. Identity-based policy enforcement or abilities to enforce policy on thousands of applications have been highly touted but rarely used.

Because it is highly penetrated, the firewall market is driven by refresh cycles. We have seen some common patterns in the firewall market as enterprises with three- to five-year-old firewalls and IPSs evaluate replacement:

- Enterprises not currently using IPS at all migrate to NGFW with minimal use of advanced features.
- Enterprises with firewalls and stand-alone IPSs employed primarily in detection mode (that is, using minimal signature sets) migrate to NGFW using the built-in IPS capabilities.
- Enterprises with firewalls and stand-alone IPS used for active prevention with large signature sets and some custom signatures migrate to NGFW for the firewall but continue using stand-alone IPS.
- High-security environments upgrade to NGFW for the firewall and upgrade IPS to next-generation IPS (NGIPS; see "Defining Next-Generation Network Intrusion Prevention").

Virtualized Firewalls

As data center virtualization has continued, demand for virtual appliance support has grown. Performance and the ability to manage firewall policy through a single integrated management console for stand-alone appliances or virtual appliances are key differentiators. Gartner has not seen the firewall features of virtualization platforms, such as those offered with VMware, as major competitors to firewall vendors, as the need for separation of duties drives reluctance to trust the infrastructure to protect the infrastructure. As other virtualization platforms, such as Xen and Hyper-V, gain traction, managing heterogeneous virtualized firewalls will present a challenge. Performance remains a barrier to wider deployment: Almost all network firewalls today are delivered on purpose-built appliances because of the poorer performance of running firewalls on general-purpose servers. Almost all operating systems within firewall appliances are uniquely hardened, subject to stringent third-party security evaluations. Security-minded enterprises are also rightly skeptical of running firewalls within a hypervisor that is between the threat and the firewall.

New Firewall Players

Acquisitions continued during the evaluation period, but there were also new entrants into the firewall market. Dell acquired SonicWALL, and Cassidian CyberSecurity (an EADS company) acquired Netasq. Palo Alto Networks had its IPO in July 2012. In December 2011, Sourcefire announced a firewall product, and in January 2012, F5 announced that the Big-IP data center firewall had been certified as a network firewall by ICSA Labs. Asia-based vendors, such as Huawei, began to explore expanding outside of their home geographies, with the Mideast and Eastern European markets the initial target geographies.

During the evaluation period, the firewall market grew to $6.3 billion in 2011. This is on target with our estimate in the previous Magic Quadrant. For 2012, Gartner estimates the firewall market will have grown 10% to reach $6.93 billion. For 2013, Gartner expects the enterprise firewall market will grow 11%, reaching $7.7 billion. We forecast this market will reach a compound annual growth rate of 10% through 2016.

Confusing Use of "Application" and "Firewall" in Three Distinct Products

Overlapping terminology and confusing marketing can lead to confusion between the three distinct issues of application control, WAFs and firewalls on application delivery controllers (ADCs). The firewall application control approaches by most NGFW vendors, such as Check Point, Fortinet, Palo Alto Networks and Dell SonicWALL, are mostly about controlling external applications, such as Facebook and peer-to-peer (P2P) file sharing.

WAFs are different: WAFs are placed primarily in front of Web servers in the data centers. Pure-play WAF companies, such as Imperva, or data center infrastructure vendors that provide WAF technology within their ADCs are concerned with custom internal Web applications.

While some ADC vendors, such as F5, are now introducing network firewalling within their ADCs as well, Gartner does not see NGFW and WAF technologies converging because they are for different tasks at different placements. As Gartner advises clients, most enterprises have a single brand of network firewall for all the placements, including Internet-facing, virtualized, data center and branch (see "One Brand of Firewall Is a Best Practice for Most Enterprises"). These data center firewalls will be challenged to gain any noteworthy share until they can provide competitive firewalling for all enterprise placements; they can, however, serve a very niche set of placements, such as in cases in which the data center is a separate business with its own firewall operations staff.

Return to Top