

Magic Quadrant for Enterprise Network Firewalls

Greg Young, John Pescatore

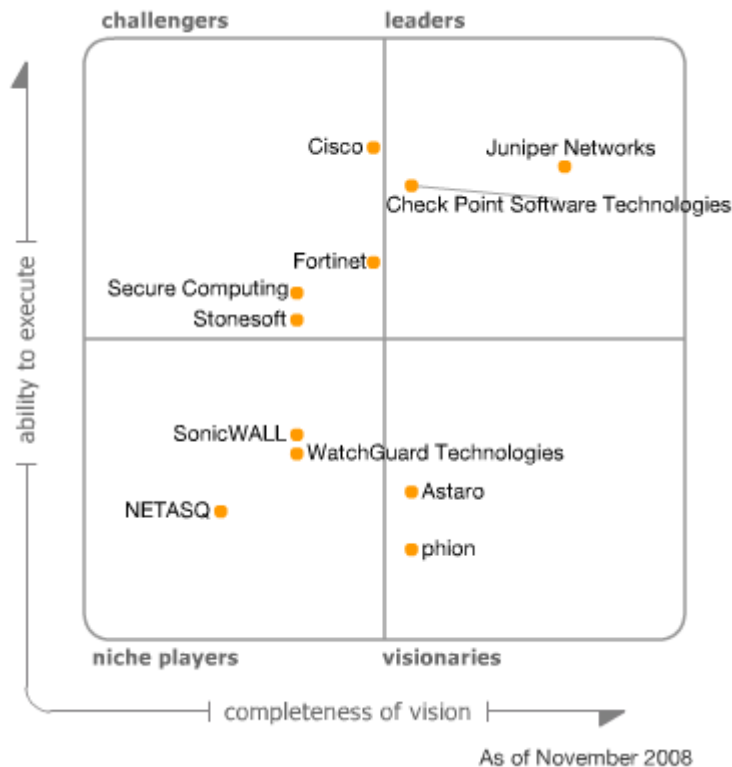
The enterprise network firewall market experienced limited overall innovation from the majority of vendors. Incumbent vendors must offer innovation or lower prices, or they will be displaced by lower-cost competitors.

WHAT YOU NEED TO KNOW

The enterprise firewall (see Note 1) market is one of the largest and most mature security markets. It is populated with mature vendors, and shortlists are fairly homogeneous among horizontal and vertical markets. Innovation has been limited, and opportunities for reducing firewall unit costs have increased because of fewer points of differentiation between competing products and virtualization. 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.

MAGIC QUADRANT

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (November 2008)

Market Overview

Firewalls are a necessary security control for policy enforcement at any network trust boundary, but changing business and threat conditions are putting pressure on growth in the firewall market. Enterprises are redesigning their demilitarized zones (DMZs) to react to the business realities of how staff and customers connect, which drives firewall demand up. However, the increasing requirement for network defense against more-complex threats has increased the deployment of

network intrusion prevention, and driven vendors to provide products that support complex deployments and rule sets that mix traditional port/protocol firewall defense with deep-packet inspection intrusion prevention. Because firewall-only products are not effective against the new breed of threats, price pressure has increased on those offerings.

Virtualization has created the opportunity for new firewall platforms that enable many separate physical firewall appliances to be replaced with a single firewall switch, a blade server running multiple virtual firewalls or new virtual firewalls to be run within virtualized servers. This can increase the number of firewall units required and also increase pricing pressure — enterprises expect software licenses to decrease in virtualized environments. Firewall technology has also not kept up with the security needs of virtualization (see "Limited Choices Are Available for Network Firewalls in Virtualized Servers"). Virtualization innovation has been mostly limited to the first level of virtualization support, a few products being VMware-certified, as with Astaro, Stonesoft and Check Point Software Technologies. Altor Networks (www.altornetworks.com) has a VMware-only firewall that additionally controls VMotion migration.

Business continues to drive DMZ change, with greater depth required to support multitier applications in at least three layers for Web, application and data servers, but also in breadth. The breadth is reflecting the requirement to support multiple methods or classes of Internet access, and also providing greater flexibility of support for connections not originating from the Internet. The management capability of firewalls continues to be a critical selection requirement for large data center and e-commerce deployments, especially to support the complexity of a rich DMZ and potentially thousands of rules. Reporting remains important, and new reporting is boosted by increasingly detailed audit requirements incorporating not only what change was made, but also who made it and why it was done.

The pressure on pricing is evident in the slow growth of the firewall market in 2007. Gartner estimates that revenue for the enterprise network firewall market in 2007 reached approximately \$2.8 billion for purpose-built hardware, approximately 6.5% growth over 2006 revenue. The average price per Gbps of enterprise firewall throughput was approximately \$8,000, a slight decrease from last year. Note that revenue is not included in the enterprise totals for companies servicing only small and midsize businesses (SMBs) or using general-purpose server platforms as appliances but not sourced through a firewall vendor. For a detailed market share, see "Market Share: Enterprise Network Security Equipment, Worldwide, 2007."

Most vendors include maintenance with support. Combined support and maintenance percentages were, on average, 19%, with the best rates being about 15% and the highest about 35%. These rates tended to correspond to the features offered, with the feature-rich products charging more. Enterprises need to look at the total cost of ownership (TCO) — purchase price plus annual support plus full-time-equivalent needs throughout a five-year period — when comparing products, because considerable differences exist among vendors about what is included.

Small and lower-end midsize businesses (approximately 100 to 500 users) usually are served by the SMB multifunction firewall market (see "MarketScope for Multifunction Firewalls for Small and Midsize Businesses"). Using the same firewall vendor for main and branch offices provides a management and support advantage, rather than bringing in a second vendor focused on smaller appliances. Branch-office firewalls are distinct from SMB firewalls. The branch device is centrally managed, often has a WAN optimization controller (WOC), and does not use some safeguards that are already provided elsewhere in the enterprise (for example, anti-spam).

The Next-Generation Firewall

Changing business processes and threats are driving new requirements for network security. Increasing bandwidth and new application communication (such as Web 2.0) are changing how

protocols are used and how data is presented. Software as a service is moving critical data off-site, and an increasing reliance on critical IT is pushing security in new directions. Threats are focusing on getting vulnerable users to install targeted malicious executables that attempt to avoid detection. Simply enforcing proper protocol use on standard ports is no longer of sufficient value in this environment. If firewall vendors do not make these changes, enterprises will demand price concessions to reduce firewall costs substantially

The next-generation firewall (NGFW) builds on the traditional enterprise firewall, and can include the following:

- *Integrated Deep-Packet Inspection:* Intrusion prevention systems (IPSs) and firewalls are complementary and can converge. Both are latency sensitive, often are co-located, are complementary (with firewalls allowing only specified traffic and IPS blocking only specified traffic) and are usually managed by the same operations staff. Beyond having IPS in the same appliance and management console as the firewall, the deep-packet inspection (DPI) properties of IPS can be integrated. An example of this integration would be the IPS initiating operator workflow or directly instructing the firewall to block a source of persisting attacks found via the computationally heavy load of DPI. Enterprises require an IPS that is of the same or better quality than that offered by stand-alone IPS appliances today. The low quality of IPSs offered in most firewalls has buoyed the stand-alone IPS market to approximately \$1 billion, and threatens to commoditize the enterprise firewall market.
- *Application Identification:* With more communication going through fewer ports and via fewer protocols, port/protocol decisions become less relevant. Whereas IPSs inspect for known malware, application inspection can involve the identification of an application operating by using permitted ports and protocols, such as those for HTTP and HTTPS. Examples would be blocking or alerting on customized policy violations, such as the use of Web mail, anonymizers, peer-to-peer or PC remote control. Destination IP addresses are not enough, because redirectors make a definitive list impossible to achieve, and policy granularity requires the blocking of only some types of application communication to an otherwise permissible destination.
- *Extra-Firewall Intelligence:* Increasingly, the firewall will be able to use security-relevant information that is often available via other safeguards. One example is the information from URL filtering, where there are known hostile addresses, and neither the firewall nor the integrated IPS should waste time (subject to a configuration setting) performing any decision making other than rejecting traffic.
- *Firewall Policy Management:* A secondary market has emerged for products to better manage firewalls for compliance and reporting, especially where firewalls from multiple vendors are deployed. Large organizations can have many firewalls, products from multiple vendors or firewalls with extraordinarily large rule bases. The consoles and reporting tools from the firewall vendors are often found lacking, and third-party firewall policy management products from companies such as AlgoSec, Exaprotect, Tufin Technologies, Secure Passage and Skybox Security are being used for rule optimization and compliance-related activities, such as reporting workflow and better separation of duties (SOD).

Market Definition/Description

The enterprise network firewall market represented by this Magic Quadrant is composed of purpose-built software and appliances for securing corporate networks. Products must be able to

support single-firewall deployments, as well as large deployments and high throughput. These products are accompanied by branch-office firewalls and management and reporting products.

As the firewall market evolves, other security functions, such as network IPS and malicious software prevention, will also be provided within an NGFW. The NGFW market will eventually subsume the stand-alone network IPS appliance market at the enterprise edge. This will not be immediate, however, because enterprise firewall vendors have been slow to imbue the IPS within their NGFW products with the same capabilities as the stand-alone firewall appliances they offer, and many IPS vendors do not have firewalls in their products that can compete with current enterprise-class firewalls. Additionally, new network security technologies are often provided through separate appliances before being included in other offerings. Although many firewalls may be accompanied by an IPS, close integration is not present in many of these products.

As part of increasing the effectiveness and efficiency of firewalls, enterprises need to add more blocking capability to them as part of the base product, go beyond port/protocol identification and move toward a service view of traffic. Firewalls and intrusion-prevention products need to evolve as threats evolve, and provide mechanisms for detecting and blocking targeted attacks.

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall companies that meet Gartner's market definition and description were considered for this Magic Quadrant under the following conditions:

- Gartner has a generally favorable opinion about the vendor's ability to effectively compete in the enterprise market.
- Gartner clients generate inquiries about the vendor.
- The vendor regularly appears on enterprise shortlists for final selection.
- The vendor demonstrates competitive presence in enterprises and in worldwide sales.
- Gartner considers that aspects of the vendor's product execution and vision are important enough to merit inclusion.
- The vendor has achieved enterprise firewall product sales (not including maintenance) in the past year of more than \$10 million within a customer segment that is visible to Gartner.

Exclusion Criteria

Companies with insufficient information for assessment or those that did not meet Gartner's inclusion criteria were excluded from the Magic Quadrant based on the following conditions:

- The vendor has minimal or negligible apparent market share among Gartner clients or is not actively shipping products.
- The vendor is not the original manufacturer of the firewall product, which includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, and carriers and Internet service providers that offer managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall and do not rate platform providers separately.

- Products sold as network firewalls but do not have the capability, scalability and ability to directly compete with the larger firewall product/function view are not included. Products suited for SMBs, such as multifunction appliances or small office/home office products, are not targeted at the market this Magic Quadrant covers.
- Products that are primarily network IPSs and are without an enterprise-class firewall (not NGFW) are not included.
- Personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls — all of which are distinct markets — are not included.
- Stand-alone network IPS appliances are a distinct market and are covered in "Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08."

Specific vendors assessed but not included:

- *Palo Alto Networks* (www.paloaltonetworks.com): Palo Alto Networks did not meet the inclusion requirements for this iteration of the Magic Quadrant; however, Gartner continues to track and monitor its progress closely. Unlike established firewall vendors that have to integrate NGFW capabilities into their firewall products, Palo Alto had the advantage of developing an NGFW without legacy constraints. Palo Alto now offers three models of appliance. In the majority of placements, Gartner has previously seen Palo Alto taking an alternate sales path into enterprises: selling as a second-tier firewall, application inspection product, or a Secure Web Gateway (SWG). This does not indicate any trend in the firewall market, but is, rather, a strategy intended to allow deployments, whereby Palo Alto can increasingly replace the incumbent edge firewall vendors after showing value and having had time to get product certifications (see "Cool Vendors in Infrastructure Protection, 2008").
- *Tech Mahindra (iPolicy Networks)* (www.ipolicynetworks.com/index.html): Tech Mahindra acquired the iPolicy firewall in 2006. The iPolicy firewall business does not meet the inclusion criteria, and we have seen considerable defection from the iPolicy product. However, the iPolicy firewall has maintained its business with a few large customers and can be considered by Tech Mahindra enterprise customers.
- *Alcatel-Lucent* (www.alcatel-lucent.com): The Alcatel-Lucent VPN Firewall Brick comes in four models. We have not observed the Brick on any Gartner customer shortlists for at least three years. Gartner assesses that most activity around the Brick is for incumbent customers, or with customers of Alcatel-Lucent network infrastructure equipment that have limited firewall requirements or want the firewall equipment to be part of a single invoice and service agreement.

Added

None

Dropped

None

Evaluation Criteria

Ability to Execute

- *Product or Service*: This also includes customer satisfaction in deployments and considers factors related to getting products sold, installed, supported and in users'

hands. Strong execution means that a company has demonstrated to Gartner that its products are successfully and continuously deployed in enterprises and win 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. 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 is foremost over revenue. Key features, such as virtualization, console quality, low latency, range of models, secondary product capabilities (logging, event management and compliance), and being able to support complex deployments and modern DMZs, are weighted heavily.

- **Overall Viability:** This includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security market. 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 vs. key competitors (which is compared to Gartner data on such competitions held by our customers) and devices in deployment. Firewalls shipped are not a key measure of execution. Instead, we consider use of these firewalls to protect the key business systems of Gartner enterprise clients.
- **Sales Execution/Pricing:** This includes pricing, deal size, the installed base — and use by enterprises, carriers and managed security service provider (MSSPs) — the strength of sales and distribution operations in the vendors. Pre- and post-sales support are evaluated. Pricing was 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. TCO 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.
- **Market Responsiveness and Track Record:** This includes the 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 provider's history of responsiveness.
- **Market Execution:** This addresses awareness of the product in the market. We recognize companies that are consistently identified by Gartner clients and often appear on their preliminary shortlists.
- **Customer Experience and Operations:** This includes management experience and track record and 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. Also important is low latency, throughput of the IPS capability and how the firewall fared under attack conditions.

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

Evaluation Criteria	Weighting
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	High
Operations	Standard

Source: Gartner (November 2008)

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 and an overall understanding and commitment to the security market (specifically the network security market). 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 yearly 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 that market directions will change.
- Sales Strategy:* This includes pre- and post-product support, value for pricing, and 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.
- Offering Strategy:* The emphasis is on the vendor's product road map, current features, NGFW capabilities, virtualization and performance. Credible independent third-party certifications, such as Common Criteria, are included. Integrating with other security components is also weighted, as well as product integration into other IT systems. As threats change and become more targeted and complex, we highly weight vendors with road maps toward being able to move beyond pure signature-based, deep-packet inspection techniques.
- 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 international deployments, MSSPs, carriers or governments.
- Innovation:* This includes product innovation, such as R&D, and quality differentiators, such as performance, virtualization, integration with other security products, a management interface and clarity of reporting.

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	Standard
Marketing Strategy	Standard
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Standard

Source: Gartner (November 2008)

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. 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.

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 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.

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 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, visionary vendors are good shortlist candidates.

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 companies 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 niche products, although other models from leaders and challengers may be more suited. If local geographic support is a critical factor, then niche products can be shortlisted.

Vendor Strengths and Cautions

Astaro

Strengths

- Users like Astaro's (www.astaro.com) clustering features and price, and ease of installation is reported as good. The Astaro Security Gateway supports a high number of concurrent connections.
- Astaro's leverage and integration of a wide range of open-source components provide an attractive price point.
- Astaro was early in having a VMware-certified version of its firewall. Additionally, the Astaro Security Gateway is available as an appliance or software load.
- Strong growth of the firewall business for Astaro, and having offerings for Web Security Gateway and Mail Gateway, supports enterprise buying behaviors.

Cautions

- Astaro has limited visibility outside of Europe, the Middle East and Africa (EMEA) and outside of its Novell channel.
- Users report they don't like that Astaro does not offer a wider choice of other safeguards and that the vendor needs to improve reporting.
- Its unified threat management (UTM) focus is less a match for enterprises and better for SMBs (see "MarketScope for Multifunction Firewalls for Small and Midsize Businesses"). Astaro is short on enterprise features and competes usually with other SMB firewall vendors.

Check Point Software Technologies

Strengths

- Check Point Software Technologies (www.checkpoint.com) is a well-known pure-play security company with a well-entrenched installed base and a strong, established channel. Check Point scored high as a significant enterprise competitive threat by the vendors Gartner surveyed.
- A large number of firewall administrators are invested with this vendor by being certified as a Check Point firewall administrator, and the value of these training certifications has been maintained.

- Check Point has historically been a software provider, relying on third-party appliance providers, such as Nokia and Crossbeam Systems. Check Point has taken a major strategy shift by offering its own branded appliances. This offers not only greater revenue but should also allow for more updates and agility in not having to move at the rate of the slowest OEM partner.
- It has a strong field of product options, such as VSX for virtualized firewalling and its Eventia security information and event management (SIEM) product. SecurePlatform allows for a loading of the firewall, along with a hardened operating system onto off-the-shelf server hardware. The wide availability of appliance and software options enables Check Point to meet the requirements for complex enterprise networks.
- Check Point has a strong and mature management interface with the ability to handle complex DMZ deployments and large numbers of devices. Provider-1 users we surveyed generally report a high level of satisfaction.
- The new Check Point-branded VPN Power-1 appliance offers a higher-end solution in two models, the 5070 and 9070. Check Point recently introduced VMware-certified versions for VPN Power-1 (VPN-1 VE) and VPN-1 UTM running in a container on ESX. Check Point has recently placed significant resources into its IPS unit, signaling that Smart Defense will be improved.

Cautions

- Although Check Point has lowered prices on models aimed at small businesses, enterprise prices are high. Products may be expensive for enterprises with low-end requirements or static networks/users. Where Check Point was shortlisted but not selected, price was most often listed as the reason.
- The proposed sale by Nokia of its appliance unit (see "Nokia's Planned Security Sale Will Not Benefit Customers") could cause disruption to sales revenue in the short term. According to Gartner, Check Point on Nokia held the No. 2 position in market share in 2007 for hardware appliance firewalls, meaning that this is a significant channel. Any disruption during the sale gives competitors not based on Check Point an opening for replacing Nokia and Check Point.
- SmartDefense remains a weak competitor to the deep inspection options of competitors. Check Point still has not updated Smart Defense with the IPS capabilities it obtained with the NFR acquisition; however, Gartner expects it to do so in the near term. IPS-1 is still not integrated into the Smart Center management console, whereas most competing firewall vendors offer stand-alone IPS management under the same console as the firewall.
- Check Point remains overly secretive about its road map and longer-term strategies, leaving its customers guessing and leaving itself vulnerable to replacement by competitors.
- Check Point is challenged in succeeding with network security products outside the firewall market and has diluted its focus in this market as it tries to attack desktop security. Check Point is missing significant growth opportunities in e-mail and Web security and will continue to be challenged by replacement by competing vendors.

Cisco

Strengths

- Cisco (www.cisco.com) has significant market share in security, including having the largest market share for firewall appliances, and is viewed as a significant (second highest) enterprise competitive threat by the vendors we surveyed.
- Cisco offers a single invoice, high discounts and a vendor relationship for "all-Cisco" networks, and it has a large market share. The Cisco support network is strong for larger customers.
- Adaptive Security Appliance (ASA) is a good replacement for the already-announced end-of-life Cisco PIX firewall, and an add-in IPS module (AIP-SSM) can replace a stand-alone IPS. The ASA is available in four editions, which clearly define what safeguards are being purchased.
- Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall/virtual private network (VPN) ASA, with firewalls also available via the Firewall Services Module blade for Catalyst switches, and on Cisco IOS-based Integrated Services Router (ISR). Gartner believes that Cisco is in a strong position to launch "security as a service" offerings in the future.
- The vendor has strong channels, broad geographic support and the availability of other security products, such as the Cisco Security Agent (CSA), its Monitoring, Analysis and Response System (CS-MARS) SIEM; and IPS products (4200 series and IDSM).
- Within Cisco during the last year, the network security product groups have undergone a significant change. Ironport was acquired by Cisco in 2007, and the former Ironport CEO was appointed to head a consolidated security group, rather than a Cisco insider. This telegraphs that best-of-breed capabilities and more-direct competition with other security companies will be the new goal rather than operating solely as a supporting element for nonsecurity Cisco products.
- The value of Cisco security training certifications has greatly increased in general recognition, and has done well in maintaining operator loyalty.
- Cisco has one of the lowest basic support fees of the vendors we surveyed.

Cautions

- Despite its large market share, Cisco is rarely seen on competitive firewall shortlists by Gartner customers. 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 replace, although this is less significant given Cisco's large market share.
- Where Cisco firewalls were shortlisted, but not selected, quality and usability of the management console, Cisco Security Manager (CSM), were the factors most often cited.
- In comparison with competitors, Cisco firewall products have one of the highest rates of product vulnerabilities. Although Cisco, like Microsoft and others, is a "big target," it must improve the internal security of its firewall products to more effectively compete in best-of-breed selections.

- The requirement to add a hardware module (the AIP-SSM) to add IPS capability to the ASA firewall appliance is a barrier to deployment and a competitive disadvantage. 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.
- Customers report that the road map for feature improvements for enterprise firewall products is not rich enough for their needs. This can provide openings for competitors after the initial successes of Cisco's ASA product, especially with the end-of-life of the Cisco PIX firewall. Fortunately for Cisco, competitors have not been effective in aggressively targeting PIX replacements and are allowing Cisco to effectively deploy ASA with incumbent PIX customers.
- Gartner customers report that the push of the CS-MARS product as part of Cisco firewall proposals leaves them the impression that Cisco must sell an additional product to compete with the console capability of competitors, such as Check Point and Juniper Networks. We also hear many comments that the performance of MARS does not live up to presales claims.
- Cisco has the highest product price in dollars per Gbps of the vendors we surveyed.

Fortinet

Strengths

- Users consistently like the continued pace of development and delivery of Fortinet's (www.fortinet.com) new features and products, and report easy deployment. Ease of installation is rated high.
- Fortinet has increased its wins against market leaders and gained additional footholds in emerging areas, such as in-the-cloud firewalls.
- It has good performance from purpose-built hardware and a wide model range, including bladed appliances for large enterprise and carriers, as well as SMB and branch-office solutions.
- The new dual application-specific integrated circuit (ASIC) strategy — which is used in its FortiGate-310B and FortiGate-620B models, with one processor for network handling for the firewall and VPN and the other for content inspection — is a significant performance enabler. The AMC expansion slot options for the enterprise-class models include an onboard security ASIC with additional ports, or a hard drive.
- Fortinet is price-competitive, especially when using multiple virtual domains.

Cautions

- Where Fortinet was shortlisted but not selected in enterprises, the IPS was most often listed as the reason. Post-sales service and support did not get high ratings from users. Gartner believes this is because of the high growth rate of Fortinet and the challenge in growing the support network at the same pace.
- Marketing focused on using UTM undervalues its enterprise offerings and steers away larger customers.

Juniper Networks

Strengths

- Ease of management and technical support were most often listed by users as what they like about Juniper (www.juniper.net) firewalls. Post-sales support was rated highly by users, although first-line support satisfaction is more mixed. Users don't like the split between its Integrated Security Gateway and Secure Services Gateway (SSG) model ranges, and would like a unified line of models. Firewall deep inspection is rated as satisfactory by users but is not competitive with stand-alone IPS market leaders.
- Juniper Networks has a strong enterprise option in Juniper SSG for high-end, purpose-built appliances, and expresses a clear road map for firewall and security customers.
- Juniper has good branch-office firewalls, complementing the enterprise products, and recognizes that enterprises want the same vendor for central and branch deployments. Its branch-office firewalls include WOC and an Avaya voice gateway.
- It has good networking support for routing, protocols and port composition. Juniper's price/management/performance blend is the strongest of the competitors.
- Juniper recently released two new high-end, chassis-based products — the SRX 5600 and 5800 models. The SRX combines firewall, IPS and nonsecurity functions, such as routing.
- Juniper's OEM deal with Q1 Labs gives Juniper a competitive single-vendor SIEM offering.
- Juniper was identified as the greatest network firewall competitor by the majority of companies surveyed.

Cautions

- As a network infrastructure vendor, rather than a pure-play security vendor, Juniper faces heavy competition from Cisco networks, where buying any Juniper equipment can be resisted as a Cisco network equipment replacement.
- Like most competitors, integration between IPS and the firewall is limited, although Juniper has the best in-the-firewall IPS in the market.
- Juniper is generally high-priced and often allows competitors an opening on price alone; however, customers report that they recognize the value/price proposition.
- Users commented that they would like more Web security products from Juniper.
- The replacement of ScreenOS with JUNOS could be problematic if Juniper does not maintain strict quality control, and keep JUNOS free from vulnerabilities. Although JUNOS has had more vulnerabilities than ScreenOS, JUNOS has had few vulnerabilities in comparison with other network infrastructure operating systems.

NETASQ

Strengths

- NETASQ (www.netasq.com) has a good mix of features in comparison to competitors in class. Users report that they like its policy-based management and real-time policy warning.
- NETASQ is focused on the requirements of midsize customers and provides good channel support.
- Users report that the appliance throughput lives up to performance claims, including when the IPS is enabled.
- EMEA customers looking for an EMEA-based vendor are attracted to NETASQ.

Cautions

- NETASQ has a narrow international base, with almost all its deployments in EMEA.
- The product focus is less a match for enterprises and better for SMBs. Like most SMB-focused firewall companies, NETASQ does not offer a high end of appliances for larger enterprises; however, its sales success has been on serving organizations of less than 1,000 employees (see "MarketScope for Multifunction Firewalls for Small and Midsize Businesses").
- NETASQ follows competitors in some enterprise features, such as number of virtual LANs supported. NETASQ scored low as a significant enterprise competitive threat by the vendors we surveyed.

phion

Strengths

- Designed for enterprises, phion (www.phion.com) is a good alternative to established large competitors.
- Enterprise customers have well-established local support in Germany, Switzerland and Austria, and increasingly elsewhere in EMEA.
- The phion firewall has features that make it an MSSP-friendly design.
- It has developed NGFW capabilities, although with a limited IPS signature set, and phion has some unique instant messaging protection features.
- Post-sales service is strong, and the quality of its technical support is rated high.

Cautions

- Users rate phion's IPS capability low. Users don't like that phion does not offer a wider choice of other safeguards beyond firewall.
- It has a narrow international base, with most customers buying products in EMEA.
- The vendor has limited market visibility for its netfence firewall.

- Its product family includes Web application firewall capabilities, which may divert resources from its primary firewall business.

Secure Computing

Strengths

- The announced acquisition of Secure Computing (www.securecomputing.com) by McAfee could provide a strong NGFW by combining the Sidewinder firewall with the McAfee IPS, although this combination was not identified as a driver for this deal and will take some time. The wider sales reach of McAfee will be beneficial. (see "Secure Computing Buy Will Strengthen McAfee Network Security").
- The TrustedSource feature blocks known bad IP addresses from connecting to the firewall and is a differentiating feature.
- Secure Computing has increased its market visibility, product set and potential for execution after its CipherTrust acquisition (see "CipherTrust Buy a Bold but Challenging Move for Secure Computing").
- It offers strong features for government, military and other "security first" requirements.
- The vendor's integration of reputation services across network, Web and e-mail security product lines provides a strong cross-selling opportunity.
- It has a reputation of producing secure products, having greatly improved support and being a well-established firewall player.
- Secure Computing appliances have good product prices in terms of dollars per Gbps in comparison with many competitors.

Cautions

- The announced acquisition by McAfee will be disruptive for the Secure Computing firewall unit. Gartner believes that firewall manageability will be decreased if McAfee tries to focus on migrating firewall and IPS management under its desktop-oriented Enterprise Policy Orchestrator (ePO) console; however, McAfee has not done this with its other network security products.
- Secure Computing is slow to innovate and respond to the wider firewall market from its established base. The company has more emphasis on the former Ironmail and WebWasher products.
- It has low market visibility against market leaders as a result of positioning itself as a second-line firewall and as an alternative to stateful inspection firewalls. Gartner does not often see Secure Computing firewalls competing in enterprise customer shortlists.
- Secure Computing has one of the highest support fee rates of the vendors we surveyed. It scored low as a significant enterprise threat to competitors.

SonicWALL

Strengths

- SonicWALL's (www.sonicwall.com) competitive prices have resulted in strong solutions for wide remote-office deployments (such as in retail outlets) and SMBs.

- The company has the reputation and track record of strong channel support.
- The Aventail Secure Sockets Layer (SSL) VPN acquisition brought an enterprise sales force in which SonicWALL has avoided attrition through good merger and acquisition management, providing a base for a potential SonicWALL move into the enterprise market.
- The new NSA series is a good option for nontraditional deployments, such as an all-in-one firewall for an in-the-cloud provider. SonicWALL recently added application identification/inspection as an included feature, under the name Application Firewall.
- Being a public company allows SonicWALL transparency for customers rating its viability.

Cautions

- SonicWALL's firewall product line is primarily SMB-focused and not competitive in most enterprises. "Enterprise" has really meant a midsize company in SonicWALL's product portfolio (see "MarketScope for Multifunction Firewalls for Small and Midsize Businesses").
- Like most SMB-focused firewall companies, SonicWALL does not offer a high end of appliances for larger enterprises.
- SonicWall scored low as a significant enterprise competitive threat by the vendors we surveyed.

Stonesoft

Strengths

- An enterprise focus makes Stonesoft (www.stonesoft.com) firewalls distinct from most European competitors, which focus on SMBs. Although the majority of Stonesoft's business is in EMEA, North American sales and visibility have been growing.
- Stonesoft has a pragmatic range of security offerings that reflect the buying and operations realities in enterprises, with firewall with IPsec VPNs, stand-alone IPSs, and SSL VPNs.
- Stonesoft offers a virtualized StoneGate version that is certified for VMware. Both can be run under the StoneGate Management Center.
- Stonesoft offers support for clustering and high availability for the few enterprises that do not provide for this in the infrastructure outside the firewall. Support pricing is slightly lower than the industry average.
- Its appliances have a robust performance and feature set relative to company resources, and it has a loyal customer base, especially those looking for high availability. Its software quality is reported as being high, with no vulnerability-related patches in 2007.

Cautions

- Stonesoft has limited market visibility outside of EMEA.
- Its company size is small relative to competitors in the enterprise market.

- It's missing a few features that bigger competitors have, such as Layer 2 support.

WatchGuard Technologies

Strengths

- WatchGuard Technologies' (www.watchguard.com) competitive prices have resulted in strong solutions for wide remote-office deployments.
- WatchGuard has been active in developing new features and models, such as HTTPS inspection. Users report a high satisfaction with the reporting function in the WatchGuard management console.
- The WatchGuard management team has taken a customer-focused approach. Having a specific management console for MSSPs is a competitive factor. A software key to unlock appliance performance for some models can minimize appliance downtime when upgrading.

Cautions

- WatchGuard continues to push a proposition of an all-in-one firewall or UTM for enterprises, which does not match customer requirements. The new XTM line could have been a departure from SMB offerings and a new model range focused on enterprise requirements. Instead, WatchGuard is going counter to the requirements for enterprises and offering gateway antivirus and anti-spam in the XTM firewalls.
- WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed.

RECOMMENDED READING

"Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08"

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

Acronym Key and Glossary Terms

ASA	Adaptive Security Appliance
ASIC	application-specific integrated circuit
DMZ	demilitarized zone
DPI	deep-packet inspection
EMEA	Europe, the Middle East and Africa
IPS	intrusion prevention system
MSSP	managed security service provider
NGFW	next-generation firewall
SIEM	security information and event management
SMB	small or midsize business
SSG	Secure Services Gateway

SSL	Secure Sockets Layer
TCO	total cost of ownership
UTM	unified threat management
VPN	virtual private network
WOC	WAN optimization controller

Note 1 Why Firewalls?

The enterprise firewall market is driven primarily by the requirement to provide network policy enforcement and intrusion prevention at trust boundary points. Network firewalls are often the first line of defense and the primary implementers of a positive security model policy of "deny all except that which is expressly allowed." They are the enforcement points for creating DMZs for external connections.

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.

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 and skills, 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 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 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 and service-level agreements.

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 Web site, 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.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509