

Magic Quadrant for SSL VPN, North America, 3Q07

John Girard

Secure Sockets Layer virtual private networks can replace or complement IPsec remote-access VPNs. The consolidation of vendors and competition in endpoint security and usability continue to improve the appeal of SSL VPNs.

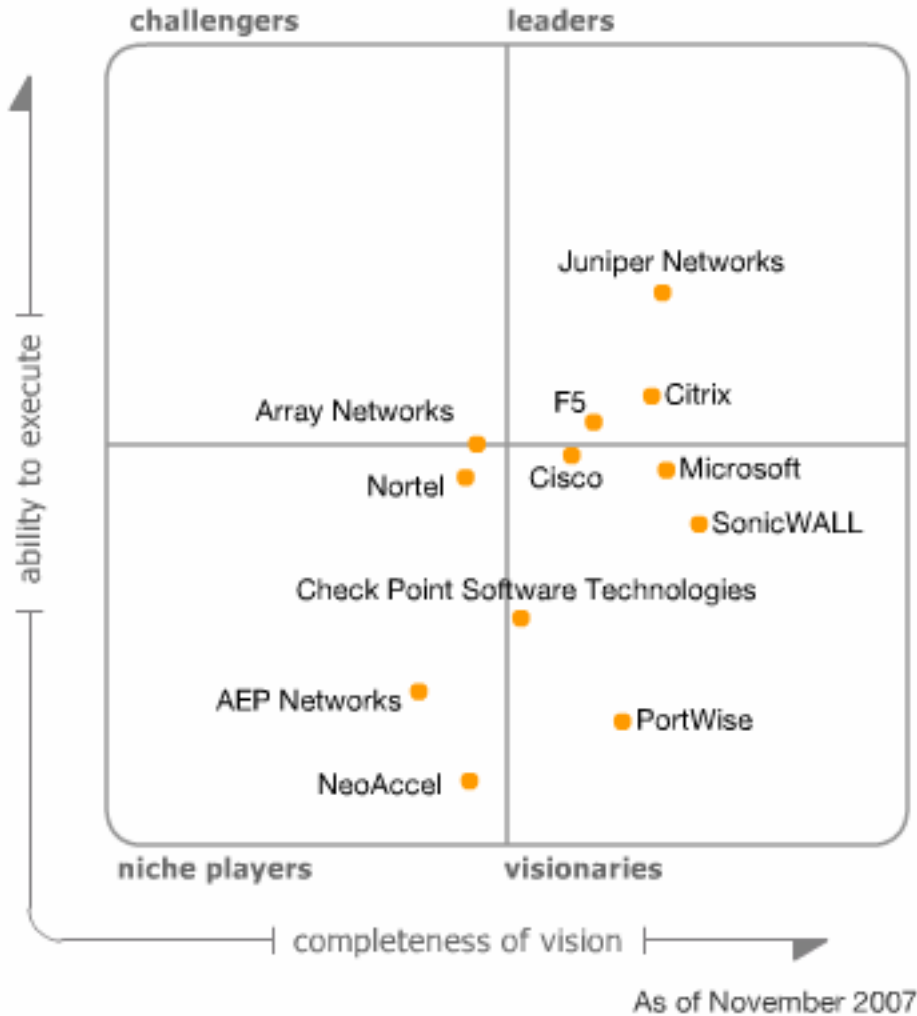
WHAT YOU NEED TO KNOW

The Secure Sockets Layer (SSL) virtual private network (VPN) is a fixture in many companies. SSL VPNs have superseded IPsec (the Internet security protocol) as the easiest choice for casual and ad hoc employee VPN access requests and for business partners, external maintenance providers and retired associates. SSL VPNs are easy to set up as application portals and as viable replacements for IPsec remote access. Remote LAN access can be achieved using open or closed tunnels, with performance that can approximate IPsec. Latency-sensitive applications, such as voice over IP (VoIP), work well because of proprietary quality-of-service enhancements that can be delivered through the browser or a formally installed VPN client.

Gartner ranks vendors in the Magic Quadrant (see Figure 1) based on performance for calendar year 2006 through the end of September 2007 and on additional road map and client reviews received up to publication date. The Magic Quadrant considers which vendors likely will dominate sales and influence technology directions through 2010, as well as which vendors are most visible among clients, generate the greatest number of requests for information and contract reviews, and account for the most new and ongoing installations in Gartner's client base.

MAGIC QUADRANT

Figure 1. Magic Quadrant for SSL VPN, North America, 3Q07



Source: Gartner (November 2007)

Market Overview

SSL VPNs have proved their value. By using the browser as the entry point, SSL VPNs can be delivered more easily to more devices than other VPNs, and SSL VPNs are capable of reliable operation, even on unreliable network connections.

SSL VPNs have evolved far beyond basic browser access. Starting with a browser session, WAN managers/administrators may offer access choices — ranging from completely portable clientless connections through thin-client-managed sessions with downloadable security features and application-specific services to full network connectivity (including routing) that emulates traditional tunnel VPNs, such as IPsec.

The connection may be restricted to one method or may be assigned dynamically according to user identity and system parameters. On-demand security features in SSL VPNs are the leading edge of remote access security and have driven new R&D to the endpoint IP security market. Delivered as thin-client components, these tools fortify the connection with on-demand security and network access center (NAC)-like health checks. This has led not only to a policy-based NAC decision but also to the use of rules to create multiple levels of trust at the entry point, ranging from menu-driven proxies to dedicated network tunnels.

The browser can be eliminated through the use of a manually installed client, while maintaining connectivity benefits. Additional SSL, UDP and IPsec tunnels can be opened dynamically, as needed, to isolate traffic and provide traffic isolation to improve quality of service for performance-sensitive applications, such as VoIP.

Although SSL VPNs have become popular for extranet user access, emergency access and some IPsec replacements, SSL VPNs have yet to take a dominant position over legacy IPsec VPNs for all aspects of remote access. Worldwide revenue for 2007 is forecast to reach \$340 million, which includes a 43% increase from the first half of 2006 to the first half of 2007. The compound annual growth rate (CAGR) forecast for 2006 through 2011 comes in lower, at 13.8%. Port shipments in the SSL VPN market grew 28% (more than 3.7 million seats) in 2006 vs. 2005 and are expected to increase slightly in 2007.

Long-term CAGR is forecast to average about 21% through 2011 — sufficient to keep more than 15 companies competitive. For example, seat sales are strong but still reflect only a fraction of the total business PCs in use. From 2004 through 2006, inclusively, more than 8.5 million concurrent seats were sold, with more than 3.2 million sold in 2006. Sales in the first three quarters of 2007 are already more than 3.7 million concurrent user seats. Optimistically speaking, many millions of business users have yet to be sold an SSL VPN. The reasons discussed in this research contribute to the slow growth, and vendors in this market must adjust to future sales opportunities by understanding all potential barriers.

IPsec is good enough for many users. The earliest adopters of IPsec replacements were companies with high incidents of VPN failures caused by network-address translation problems and unstable connections on unreliable WANs. Companies that don't experience failures or have conservative attitudes about VPN protocols are slower to consider SSL VPNs as complete replacements.

Large, incumbent players can afford to sell more slowly, making SSL an integral component of larger product architectures. Sales will be led by companies that can drive the commodity sales channel by appealing to legacy VPN buyers. This approach works well for companies like Juniper Networks and Cisco and will make pure network access sales more competitive for others. Smaller vendors will use quality of performance and support to gain attention from potential buyers.

Many companies remain in the life cycle of legacy VPN purchases, and replacement opportunities will continue as companies reach end of life on their legacy VPNs and seek easy ways to expand new VPN connections. Dedicated VPN appliances have a useful life of more than five years, as long as Windows Vista can be accommodated and the vendor does not declare end of life for support. All vendors can pick up new business as the cycles retire, but vendors' selling skills will be tested to qualify buyers at the right time and place.

Misunderstandings about clientless and thin-client VPNs have slowed some deployments. On-demand SSL VPN security has many options — and legacy IPsec buyers don't understand all the potential benefits. Vendors that can sell their products using case studies for emerging portable and mobile applications will fare best.

Specialized mobile VPNs (see "Specialized Mobile VPNs: A Niche Market Skirts the VPN Mainstream") have tied up some entry points for SSL VPNs on handhelds and highly mobile notebooks through vertical applications and proprietary WAN optimization schemes. These VPNs use a mix of UDP, WTLS, IPsec and other protocols combined in proprietary clients and WAN controllers, thus making sidesteps in the march toward VPN standards.

SSL VPN vendors largely have ignored the handheld market, instead pursuing easier sales on notebooks and desktops. It's time for competitive vendors to understand and directly address the business value proposition for highly mobile users by introducing better handheld clients and strong value case studies. Wireless/roaming users on notebooks, tablets and handhelds can become sales growth opportunities, but SSL VPN vendors must compete directly against the perceived values of specialized mobile VPNs. Vendors such as Aventail (now SonicWALL) have demonstrated capabilities and are building case studies, but all vendors must work more aggressively to promote their products' mobile benefits.

Alternative VPN access for nondisaster scenarios will continue to grow as an investment strategy, where a company is not willing to replace IPsec for reasons including support for nonmanaged systems belonging to employees, partners and contractors. SSL VPNs are particularly effective for this purpose, and this opportunity serves well for all vendors, because buyers don't presume that their legacy VPN vendors are the only choices. However, these types of sales will not lead to replacements, unless the SSL VPN vendor builds a relationship to prove ongoing value and to dispel the belief that the new VPN is only an alternative and not a comprehensive replacement.

Although alternative emergency access for disaster scenarios will continue to grow as an investment strategy, this is not viable as a stand-alone revenue opportunity. Emergency licenses are heavily discounted and are intended for temporary use.

Secure intranet portals based on SSL gateways provide a means to maintain security in a deperimeterized network. However, sales for this purpose remain small, perhaps because the popular conceptions about deperimeterization are slow to be accepted for common use.

Application-driven access for specific tasks is a growth opportunity that expands beyond conventional VPNs to include single-application access, such as e-mail and secure Web application portals for business-to-business and business-to-consumer applications. Sales for these purposes require entry into different buying centers than are typical for VPNs. Citrix is clearly the company most prepared to sell in this manner, and the company's high performance in seat sales and revenue proves this point. Similarities in future vision and road map responses from Array Networks, F5, Juniper Networks and Microsoft indicate a willingness to follow Citrix into the application-driven model.

Market Definition/Description

Products in the SSL VPN market provide secure and private connections for individuals to reach company gateways via the Internet using VPN from a workstation, such as a desktop, laptop or a smaller, end-user computing device, such as a PDA or smartphone. This research evaluates SSL VPN products that are sold for purchase and use within enterprises.

Our primary focus is midsize to large enterprises in North America, for which the U.S. provides the largest, single-border growth market worldwide. Global market presence is a contributing factor to execution and vision. Services built from the products and offered by third parties are considered additive to the product vendor ranking but did not drive the evaluation.

SSL VPN products combine browser security enhancement software with a VPN gateway that may be delivered as a stand-alone gateway appliance or as software to be installed on a user-supplied gateway server. The market is dominated by appliances; pure software products have

proved to be less competitive than drop-in, plug-and-play solutions. Menu-driven, "point and click" browser access to programs and resources characterize the default interface for an SSL VPN; however, several companies offer nonbrowser clients to more closely imitate an IPsec VPN, and a few companies omit the menu interface altogether.

SSL VPNs support the strong authentication and logging desired for VPN protection and application access audits, and support the roaming required for mobile users. End-user security features are a visionary competitive differentiator that drives vendors to provide on-demand protection mechanisms — embedded or bundled — that perform NAC functions, block malicious code, clean up data and enforce firewall settings, even on completely unmanaged workstations.

Inclusion and Exclusion Criteria

Inclusion Criteria

SSL VPN companies that meet the market definition and description were considered for this research under the following conditions:

- Gartner analysts have a generally favorable opinion about the company's ability to compete in the market.
- Gartner clients generate inquiries about the company.
- The company causes clients to change or delay their procurement plans for competing products.
- Competitors regard the company as a serious threat.
- The company regularly appears on shortlists for final selection.
- The company demonstrates a competitive presence and sales to Gartner analysts.
- Gartner analysts consider that aspects of the company's product execution and vision are important enough to merit inclusion.

For 2007, the minimum thresholds for seat sales and revenue were not applied. All 12 companies that participated in the survey were ranked.

Exclusion Criteria

SSL VPN companies not included in the document might have been excluded for one or more of the following conditions:

- The company did not have a product on the market for a sufficient time during the study period to establish a visible, competitive position.
- The company was invited to participate but did not reply to an annual request for information and did not otherwise meet the inclusion criteria.
- The company had a minimal or negligible apparent market share among Gartner clients or had no products shipping.
- The company was not the original manufacturer of the SSL VPN product — this includes resellers that repackage products that qualify from original manufacturers, as well as carriers and Internet service providers that provide managed services.

- The company sells the product as an application firewall and is not competing directly within the larger SSL VPN product/function view.
- The company sells SSL accelerators and load balancers as stand-alone products for other purposes besides SSL VPNs.
- The company sells Web-enabled personal remote-control products that are not true multiuser access gateways.

Other Companies

The following vendors were contacted but did not participate. None of these companies generates client inquiries that would otherwise merit inclusion.

- Blue Coat Systems, Secure Computing and Sun declined to return the survey.
- Dialogic (formerly Eicon), Cavium Networks and Menlo Logic (acquired by Cavium in 2006) did not reply to inquiries.

Added

- NeoAccel: The company is still in startup mode but has established multiple OEM deals and sold well in the first half of 2007, potentially outperforming some older and established companies.
- SonicWALL: The company's incumbent products were sold exclusively in the small or midsize business (SMB) market and were outside the scope of previous Magic Quadrants. SonicWALL's acquisition of Aventail brings SonicWALL into the research.

Dropped

- Caymas Systems: The company ceased business in 2007. Relevant parts of its technology and some staff were acquired by Citrix.
- Nokia: The organization ceased to sell a differentiated product for the SSL VPN market.
- Aventail: The company was acquired by SonicWALL and is now tracked as SonicWALL.

Evaluation Criteria

Ability to Execute

Execution considers factors related to getting products sold, installed, supported and in users' hands. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients and a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size and income; however, as the market matures, larger companies tend to have a greater influence.

Product/Service: Compares the completeness and appropriateness of core SSL VPN products sold for use in the enterprise remote-access market. The SSL VPN market defined in this research is product-focused, but related service areas may contribute, including consulting services and managed service resellers. A strong product focus is critical to demonstrating that the vendor can generate market awareness.

Overall Viability (Business Unit, Financial, Strategy, Organization): Considers the company's history and its demonstrated commitment in the SSL VPN market, as well as the difference

between a company's stated goals for the evaluation period vs. actual performance, as compared with the rest of the market. The growth of the customer base and the revenue derived from sales are considered. All vendors were asked to disclose comparable market data, such as SSL VPN revenue, the number of unique companies under contract and information about seats sold year by year (defined as concurrent active license seats deployed on sold products).

Some vendors did not provide all competitive information in the format requested for comparison. In these situations, other quantitative sources of Gartner information were considered, but qualitative evidence from client feedback and peer analyst feedback become more important. Indirect measures of product penetration, such as "boxes shipped," were not used to measure execution in this research. Instead, we considered concurrent seats sold, licensed and accessible to the buyer as evidence that the products are being used. Vendors were asked to convert to the concurrent seat formula as necessary, and the actual numbers reported were treated as guidance rather than as hard facts.

Sales Execution/Pricing: Compares the strength of vendors' sales and distribution operations, as well as their discounted list pricing for systems supporting as few as 50 concurrent users up to more than 10,000 concurrent users. Pricing was compared in first-year, cost-per-concurrent-active-license seats, including the cost of all hardware and support.

Low pricing does not guarantee high execution or client interest, and the market, as a whole, did not move to commodity status in 2007, although Cisco experienced an unprecedented spike in low-cost seat sales. Buyers want good results more than they want bargains, and they respond more strongly to sales techniques led by case studies and return-on-investment projections. In any case, the benefits of a well-implemented SSL VPN can outweigh the initial costs.

Market Responsiveness and Track Record and Marketing Execution: Rates competitive visibility as the key factor, including which vendors are most commonly considered top competitive threats during the RFP process and which are considered top threats by each other. In addition to buyer and analyst feedback, this rating considers feedback from clients, analysts and the vendors themselves. Strong ratings mean that a company has demonstrated to Gartner analysts that the enterprise can get listed in RFPs early and can win a large percentage of competition with other vendors.

Customer Experience: Is subjectively rated from clients' feedback to analysts, the opinions of Gartner analysts in security, network and platform research groups, and vendor-supplied references, where needed. Intense interest in SSL VPNs from Gartner clients provided a year's worth of ample feedback to frame the market.

Operations: Considers the ability of a vendor to pursue goals in a manner that enhances and grows its influence in all execution categories.

Table 1 provides an overview of the evaluation criteria for the ability to execute.

Table 1. Ability to Execute Evaluation Criteria

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

Evaluation Criteria	Weighting
Customer Experience	Standard
Operations	Standard

Source: Gartner

Completeness of Vision

Market Understanding and Marketing Strategy: Assessed through direct observation of the degree to which a vendor's products, road maps and mission anticipate leading-edge thinking about buyers' wants and needs. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and by reading planning documents, marketing and sales literature, and press releases. 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 these plans in place, show that they are following the plans and modify the plans as market directions change.

Sales Strategy: Examines vendors' strategies for selling products, including sales messages, techniques, marketing, distribution and channels. This ranking factor is the bridge between marketing execution and product strategy.

Offering (Product) Strategy: Is ranked through an examination of the breadth of functions, platform and operating-system support for the SSL client, the VPN gateway operating system and features, and the investments made by the vendor to optimize and support applications accessed through the gateway. R&D investments are credited in this category.

Business Model: Takes into account a vendor's underlying business objectives for its products and its ongoing ability to pursue R&D goals in a manner that enhances all vision categories.

Vertical/Industry Strategy: Considers a vendor's ability to communicate a vision that appeals to specific industries and verticals. Good performance in selected markets improves a vendor's ability to communicate its reputation and vision.

Innovation: Takes into consideration the degree to which vendors invest in core requirements for the successful use of their products. Criteria include a vendor's internal investments in value-added security tools and technology road maps, as well as external efforts to expand interoperability, alliances and partnerships with companies in related security markets. A vendor with a strong vision creates communities with other companies, and this, in turn, helps other companies, as well as buyers, view the SSL VPN vendor as a necessary component of larger business solutions.

Geographic Strategy: Takes into account a vendor's strategy to direct its resources, skills, products and services outside North American markets. However, all vendors are ranked in this Magic Quadrant primarily for their performance in North America.

Table 2 gives an overview of the evaluation criteria for completeness of vision.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Standard
Sales Strategy	Standard

Evaluation Criteria	Weighting
Offering (Product) Strategy	Standard
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	Standard
Geographic Strategy	Standard

Source: Gartner

Leaders

Leaders demonstrate balanced progress and effort on all execution and vision categories. Their actions raise the competitive bar for all products in the market, and they can change the course of the industry. To remain in the Leaders quadrant, vendors must excel in mobile access and protection and must dominate in sales. However, a leading vendor is not a default choice for all buyers, and clients are warned not to assume that they should buy only from the Leaders quadrant.

Challengers

Challengers have solid products that address the typical needs of the market with strong sales, visibility and clout that add up to higher execution than niche players. Challengers are good at winning contracts, but they do so by competing on a basic or limited selection of functions rather than on advanced features. Challengers are efficient and expedient choices for defined access problems. Many clients consider challengers to be the conservative, safe alternative to niche players.

Visionaries

Visionaries invest in the leading-edge or "bleeding edge" features that will be significant in next-generation products and will give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they lack the execution influence to outmaneuver challengers and leaders. Clients pick visionaries for best-of-breed features, and, in the case of small vendors, may obtain more personal attention.

Niche Players

Niche players offer viable, dependable solutions that meet the typical needs of buyers and fare well when given a chance to compete in a product evaluation. Niche players respond to market changes and new technologies, but they generally lack the clout to change the course of the market. Niche players may serve conservative and risk-averse buyers more efficiently than leaders. Clients tend to select niche players when stability and focus on a few important functions and features is more important than a wide and long road map.

Vendor Strengths and Cautions

AEP Networks

Strengths

- AEP Networks has hardware products that are certified to Federal Information Processing Standard (FIPS) 140 Security Level 4.

- The company's products appeal to small/midsize buyers that want a small number of seat licenses.
- It also has a steady market presence and reliable products that emphasize policy and access controls.
- AEP is pursuing public relations efforts to communicate new clients sold and competitive wins.

Cautions

- The pursuit of NAC, SSL VPN and IPsec VPN as separate product lines demands a lot of R&D commitment in a small company.
- Revenue and market seat sales are low for a long-established company and below the average for vendors in this Magic Quadrant, even when combined with consideration for AEP's other product lines.

Array Networks

Strengths

- Array Networks has excellent price/performance and scalability for large and demanding access needs, while also offering an affordable, low-end entry point. Array's Universal Access Controller and secure access and application delivery solutions road maps are dedicated to growing a seamless product line.
- The company's mission is committed to making VPN as easy as possible to set up and use, thereby reducing barriers to IPsec replacements.
- Array's products sell well outside North America.
- Acceleration is standard/included on all models and platforms.
- Array was the first vendor to offer fully managed, audited remote control (RDP-based) in the gateway, eliminating the need/risk of allowing user-initiated, personal/Web remote control tools that can't be logged or managed. Array also was first to offer site-to-site SSL VPN and to have some client installations.

Cautions

- Although Array had some impressive customer wins, it was mentioned infrequently by Gartner clients and is not considered a competitive threat by peers. In general, clients have reported that they were attracted by Array's raw performance and scalability.
- Array needs to build its competitive presence in North American markets, where it currently earns less than 30% of its SSL revenue.
- As compared with larger incumbents with longer time in market and larger distribution channels, Array's share earns extra merit for execution. To maintain a strong execution ranking, Array must increase the awareness of its vision and the effectiveness of its marketing and communications. The company also needs to be seen frequently in head-on competition in Gartner client RFPs with companies ranked as leaders.

Check Point Software Technologies

Strengths

- Check Point Software Technologies has a complete and well-designed product, with a comprehensive set of on-demand security features.
- SSL VPN is available as a stand-alone product or can be integrated with the Check Point Firewall.
- The product is available as software, a hardware appliance and as a VMware ESX Server virtual appliance.
- Check Point's operating system is certified for FIPS 140-2 and Common Criteria (CC) Evaluation Assurance Level (EAL) 4.
- Broad features for handheld platforms include local Bluetooth and firewall controls.

Cautions

- Check Point should reduce its requirements for administrative rights to operate its on-demand browser security tools.
- On-demand security has a fee after 25 users, while most other vendors offer unlimited use of all or most of their endpoint security tools.
- Relatively low SSL VPN sales and visibility limit execution and reflect a blase approach to the market. IPsec is still the main product line and revenue stream for Check Point.
- Gartner clients that inquired about SSL VPNs are likely to consider a separate vendor for SSL, even if they use firewalls or IPsec from Check Point.

Cisco

Strengths

- Cisco is poised to drive SSL VPN to commodity status by placing it in major new product lines at the lowest entry costs among major vendors.
- Cisco's product includes strong, thin-client, on-demand endpoint security features at no extra charge, built from in-house technology.
- The company's fast ramping sales in 2007 are among the highest ever recorded in the market.
- All Cisco's Adaptive Security Appliance (ASA) 7.2.2 platforms include FIPS 140-2 certification. ASA 8.1 is in pre-validation phase. CC EAL 4 is in process.

Cautions

- Because Cisco sells disaster/standby/backup seats as regular seats, total sales cannot be directly counted toward execution.
- On-demand endpoint security tools are a missed opportunity because they aren't offered for OEM or for use in other purposes.

- Gartner clients have reported purchasing other SSL VPNs even when Cisco's product is already installed. This is a symptom of the disconnect between buying centers for application delivery purchases and pure network access.

Citrix

Strengths

- Citrix has the greatest experience of all market vendors in remote, thin-client application delivery. In the 1990s, the company developed the original, protected browserlike client (SecureICA) well ahead of the SSL VPN market and has the longest commercial experience with screen-oriented security, such as the ability to block cut and paste.
- Citrix acquired traffic inspection and acceleration technology and expertise from Caymas in 2007.
- Citrix released a new, more-integrated product line (Citrix Access Gateway) using Net6 and NetScaler technologies to scale from small office to carrier class.
- Leading sales and market share do not depend on selling to legacy VPN buyers. Citrix is leading sales in areas generally closed to networking equipment vendors.

Cautions

- Citrix has been less appealing for IPsec replacements because of the company's application delivery focus, but LAN access and IPsec replacements are supported.
- Legacy users of Citrix's WinFrame product and Presentation Server, as well as the IT networking staff who manage the demilitarized zone (DMZ), often are unaware that Citrix competes in the SSL VPN market. However, Citrix has improved its visibility since the previous Gartner evaluation.
- Citrix needs to demonstrate compelling application delivery on wireless handheld devices using the in-house technologies it has acquired during the past several years.

F5

Strengths

- F5 exhibits strong and steady growth in sales and revenue for this market without having to rely on IPsec sales for a backup plan, as do several other incumbent networking companies.
- Visual Policy Editor makes access control setups easy for administrators.
- The iRules scripting system enables complex gateway operations to be programmed that might otherwise require custom coding.
- Several global providers use F5's products to deliver remote-access services.

Cautions

- Although F5 is cited as a competitive threat by three-quarters of vendors in this review, it does not appear frequently on Gartner clients' shortlists. Greater visibility will be a factor in judging future execution scores.

- Further integration of the FirePass and BIG-IP platforms (planned for 2008) will help deliver F5's features at all purchase levels.

Juniper Networks

Strengths

- Juniper Networks delivers solid multiyear performance with strong sales and revenue in SSL VPNs and in IPsec.
- Juniper is the No. 1 competitive threat cited by all other peer vendors.
- The company appears on most shortlists discussed in Gartner client inquiries.
- Juniper's products earn a high satisfaction rate and few complaints, given its high degree of market penetration.
- Several global providers use Juniper's products to deliver remote-access services.
- All platforms have been CC EAL 2-certified since 2005.

Cautions

- Juniper's stated list prices are among the highest in the market.
- The scalability of cluster solutions could be larger for large clients and carrier/service provider applications.

Microsoft

Strengths

- The acquired products from Whale Communications filled a serious gap in Microsoft's secure application access strategy by adding a robust gateway and strong endpoint security.
- Microsoft's merging of Internet Security and Acceleration Server and the former Whale SSL VPN created an excellent new product, the Intelligent Application Gateway (IAG), with optimizations for the Microsoft SharePoint Server.
- Whale customers have been given generous extensions for software and hardware support.
- By attracting and retaining key personnel from Whale and Aventail, Microsoft built a better product than could have been created by incumbent Microsoft talent.
- Platforms and pricing are attractive for small to large enterprises and are sold with Forefront Security.
- IAG and related products are being handled aggressively in the Microsoft sales channels.

Cautions

- Microsoft continues to suffer from past and recent fragmented, uncoordinated VPN developments on different platforms and in different product groups. Microsoft has a long-term vision for a converged VPN architecture, but many years will pass before a

common architecture will be offered consistently across PCs and handhelds, with third-party support for non-Windows platforms.

- Microsoft's SSTP platform, intended to support common SSL VPN network service virtual adapters, will take time to gain acceptance. The platform will face inertia on the road to a potential de facto standard, given that each SSL VPN vendor has created its own encapsulation methods.

NeoAccel

Strengths

- NeoAccel has a growing list of OEM partners to provide a cushion while the company pursues sales under its own brand.
- The gateway is available in a hardware appliance or as software.
- A patented accelerator provides high-performance, network-level remote access, which is focused for IPsec replacements and suitable for client/server applications, multimedia applications and VoIP.
- NeoAccel supports site-to-site SSL VPN.
- The creative use of telemarketing stimulated sales for NeoAccel's first year in the market, in direct competition with other vendors in this Magic Quadrant.

Cautions

- NeoAccel is the newest entry in a mature, consolidating market.

Nortel

Strengths

- Nortel is a large, global company with extensive worldwide support.
- The company offers products that converge IPsec/SSL clients, giving the user one experience, regardless of access mode.
- Among major vendors, Nortel's seat pricing in large quantities is the second-lowest, after Cisco.
- Nortel's TunnelGuard endpoint security has been adapted for SSL and is compatible across SSL VPNs and IPsec VPNs.
- Nortel's products are being used to deliver remote-access services by a global public telecommunications service operator.
- Acceleration is standard/included on all models and platforms.

Cautions

- Nortel's market growth is slower than expected for a major, global-networking vendor with a strong reputation in IPsec VPNs.
- Gartner clients inquiring about SSL VPNs are likely to consider a separate vendor for SSL, even if they use IPsec from Nortel.

PortWise

Strengths

- PortWise is a stable vendor with steady sales and a growing OEM business (three confirmed partners and three in negotiation). The company was the first SSL VPN to be listed under VMware's Virtual Appliance Certification Program.
- PortWise is the only market vendor with integrated, strong authentication for mobile devices; 60% of buyers purchase PortWise's strong authentication to supplement the VPN.
- PortWise has extensive experience in delivering secure services and applications to handheld wireless devices.
- The company is successfully penetrating developing countries and markets, for example, financial services in India.
- PortWise has extensive experience and a long track record with sensitive applications, including retail banking.

Cautions

- Gartner clients have been unlikely to report PortWise as a shortlist candidate; however, verified case studies are of high quality.
- Market revenue and seat sales are relatively low for a long-established company.
- PortWise needs to build its competitive presence in North American markets, where it currently earns less than one-quarter of its annual business.

SonicWALL

Strengths

- SonicWALL provides the best explanation of and feature set for on-demand firewalling and tunnel controls supported within a thin-client SSL VPN.
- The company's vision is among the best and most-complete, long-term market road maps. This vision results from a complementary blending of road maps from Aventail and SonicWALL.
- Aventail's key personnel and business operations have been preserved and are valued by SonicWALL.
- The acquisition brings strong financial backing and new sales channels to Aventail products, which already had proved to be strong in the market.
- Aventail products continue to be used to deliver remote-access services through multiyear agreements with a large list of global providers.
- SonicWALL has a track record for rapid, new-product development and for deep traffic inspections.

Cautions

- Aventail's market visibility diminished for 2006 and 2007. However, SonicWALL can improve execution in 2008, depending on its ability to reposition its products to be competitive in midsize- to large-enterprise networking markets and by recovering Aventail's brand presence and continuing to build out its own emerging presence as a midsize- to large-enterprise player.
- SonicWALL's business prior to the acquisition was considered only partially because its SMB products were not counted in this research. Historically, SonicWALL's small-business focus has not met the inclusion criteria for this Magic Quadrant. Execution will be reassessed after the product lines are merged and the channels are fully engaged for the Aventail products.
- SonicWALL should pursue FIPS and/or CC certifications for Aventail products. Most vendors in this market offer some degree of certification.

RECOMMENDED READING

"Forecast: Enterprise Routers and IPsec VPN/Firewall Equipment, Worldwide, 2006-2011"

"Magic Quadrant for SSL VPN, North America, 3Q06"

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

"Market Share: Enterprise Network Security Equipment, Worldwide, 2006"

"'Panning for Gold' Outside the Leaders Quadrant of Gartner's Magic Quadrant"

"Specialized Mobile VPNs: A Niche Market Skirts the VPN Mainstream"

"Weigh Pros and Cons Before Choosing IPsec or SSL Remote-Access VPNs"

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, skills and others, 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, service-level agreements and others.

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