SSL Virtual Private Networks
METAspectrum℠ Evaluation
Market Definition
The Secure Sockets Layer virtual private network (SSL VPN) market is characterized by products — often referred to as application security gateways — used primarily to provide secure remote access to applications. To date, the primary user constituency has been an organization’s own employees (B2E); however, deployments encompassing extranet access (B2B) are increasingly common. Intranet usage also makes sense, but remains nascent. From a technology perspective, the key distinction is the use of SSL to deliver confidentiality and integrity capabilities without the need for a predeployed client component (which is the case with IPSec, the leading incumbent technology for secure remote access). The emphasis for this evaluation is products targeting the enterprise market, though not those focused predominantly on small enterprises (e.g., less fully featured offerings, SSL VPN capability as part of an all-in-one security gateway). Both private and publicly held companies have been included in the review. No minimum revenue requirements were imposed, but included vendors/products have been limited to those being used or evaluated within the META Group customer base. Specific product versions evaluated were generally available not later than June 1, 2004.

Market Forecast
Although the SSL VPN market is maturing rapidly, it is still quite rough around the edges. This is well reflected by the participants in this market, as well as by the steady stream of new entrants.

- A core group of market leaders continues to rapidly innovate and drive increasing degrees of functionality. Other contenders must often scramble to keep up.

- A few of the early leaders (in terms of market share and/or technology) have been acquired by a couple of large networking/security vendors. This has forced the remaining body of similarly large vendors to address the potential of this market. To date, they have done so primarily via in-house development, notably starting out in a trailing position, but have significant longer-term potential due to their size, resources, and established credibility.

- Finally, many smaller vendors from tangential markets (e.g., traffic management and optimization, application-layer security gateways) are also trying to capitalize on the tremendous opportunity that SSL VPN represents. In doing so, they are essentially “bending” their core technologies/products to become SSL VPN solutions. This is clearly beneficial from the standpoint of bringing increased focus to relevant, additional functionality. However, it also tends to imply, at least initially, reduced capabilities in other areas that are essential to an SSL VPN solution (e.g., breadth of application access, client-side security).

The net result of these various dynamics and diverse heritages is both a widening scope of features and a significant degree of variation in terms of the actual depth (or quality) of related capabilities. For example, while almost all SSL VPN vendors claim the ability to provide access to applications via only a browser on the client platform, some will in fact be able to provide access only to Web applications in this operating mode, and others will provide access to a much broader range of resources (e.g., e-mail, file services). Host integrity checking is another popular claim/feature set. Yet, in some instances the supported client operating systems will be very limited, and in others the volume of checks will be restricted to just detection of malware and trojans (versus also supporting extensive checks of the client station’s various security settings).

Another point that must be accounted for is the fact the vendors continue to move their products forward rapidly. Indeed, several of the participants in this study issued new releases between the evaluation cutoff date (June 1) and the publication date of this report. Furthermore, we fully expect that each competitor will release at least one additional version of its solution before the end of 2004.
Overall, this current state of the market leads to the familiar warning of “caveat emptor” — or at least the equally applicable “the devil is in the details.” In other words, buyers must still proceed cautiously in their selection process, taking the following key steps:

- Clearly establish how factors such as the type of application being accessed, browser make/type, and client operating system can impact the applicability of available access modes and security features. To this end, organizations should consider providing detailed use-case specifications to prospective vendors so they can clearly confirm applicability and related operating conditions of their solutions.

- Conduct a detailed pilot/testing period prior to wide-scale investment and implementation.

- Inquire about and give appropriate credit for competitors’ future plans.

- Possibly consider vendors beyond those covered in this evaluation. As we noted earlier, additional vendors are coming to market or our attention almost monthly. For example, we became aware of Caymas Systems too late to include a detailed evaluation of its offering in this report. However, its identity-driven access gateway looks promising. It appears to incorporate most of the features associated with the leaders in this study, while bringing a few unique characteristics to the table (e.g., custom silicon for packet/session processing — which bodes well for system performance and scalability).

We also note that, at least for now, longevity in the market corresponds to a solution having both broader and deeper capabilities. Therefore, organizations with particularly demanding requirements are advised to focus their attention on the more well-established players.

Notwithstanding the aforementioned functional inconsistencies, we must be careful not to paint a bleak picture. SSL VPNs are already capable of delivering great value to organizations and have even further upside potential going forward. Many of the benefits of SSL VPN technology are derived from its ability to securely provide clientless (or at least client-lite) access to applications and other computing resources. In this context, “clientless” is interpreted as requiring only a browser, while “client lite” also involves the download of Java or ActiveX components to provide additional access and security capabilities. Advantages are also derived from the ubiquity of browsers and the ability of associated Web protocols to traverse boundary firewalls. Overall, the benefits and opportunities to the organization include the following:

- Reduced cost of ownership is achieved by not having to deploy and manage client software, as is the case with the incumbent technology for secure remote access, IPSec.

- Increased productivity results from being able to economically extend secure remote access capabilities to a greater portion of the organization’s total user population. It is also based on users having access from anywhere and with practically any device (e.g., kiosks, home PCs, PDAs). All that is needed is a browser and an Internet connection.

- A greater degree of security is achievable — at least for some of the access modes that SSL VPN products support. Specifically, in many instances, SSL VPNs provide the user only with a connection to an application session, versus a full presence on the destination network (as is the case with IPSec). In addition, many of the SSL VPN gateways embrace proxy architecture. This is inherently more secure than other designs and also provides a foundation for advanced filtering capabilities.

**Note:** This brings up two significant areas of differentiation among available products.

1. While almost every product has a network extension mode to provide access to a wider range of applications, some products rely on this mode more heavily than others. The consequence is that these products are operating more frequently in a less secure state, because this mode essentially bypasses many of the gateway’s security functions.

2. Not all SSL VPN gateways incorporate proxy/reverse proxy architecture. This is most often revealed by a product’s inability to rewrite URLs and host names, which is essential for masking internal naming and addressing conventions.
• Enhanced business opportunities are typically a second-phase consideration for many organizations, and therefore remain a relatively untapped driver for SSL VPN market growth. Because it does not require predeployment of any components to partners' networks or computers, and because of the granular degree of access control it provides, SSL VPN technology is viewed quite favorably for extranet (i.e., B2B) solutions.

• Improved security can also be achieved for internal networks and systems, though such implementations are still relatively rare. Encryption across the intranet, granular access control, and in-depth logging capabilities are all viewed as favorable characteristics, particularly for organizations in vertical markets that are subject to numerous security and privacy regulations.

From a technology evolution standpoint, we expect significant emphasis to remain on establishing greater degrees of accessibility to applications, particularly without having to resort to full network connections. Vendors are also in the midst of adding significantly greater security functionality, both on the client (e.g., secure virtual workspace) and at their gateways (e.g., application-layer attack protection and filtering). Indeed, this seems to be the battleground du jour, despite the fact that many products still need to bolster relatively weak or inconsistent access capabilities. However, with the onset of widespread adoption and large-scale deployments (i.e., >1,000 concurrent users) during the next two years, the critical requirements will become scalable management functions (particularly configuration capabilities) and greater system performance/capacity. As with most other security solutions, vendors that best balance security, performance, and manageability — and in this case, accessibility to applications as well — will be positioned to dominate the market.

**Key Findings**

Several key findings and expectations have already been divulged in the previous section. Others depend on an understanding of the evaluation criteria that were used. At a high level, “performance” criteria represent items that a potential purchaser would most often use (e.g., technical capabilities, pricing), perhaps in the form of a request for information (RFI) or proposal (RFP). On the other hand, “presence” criteria are best characterized as items that a financial analyst would use to determine the business health and potential of a company and its offerings (e.g., vision, channel strategy).

For this evaluation, we placed only a slightly greater importance on the performance dimension. In general, for an emerging/maturing market, this weighting would be skewed even further in favor of performance. However, with SSL VPNs, there has been a relatively low barrier to entry. Indeed, we expect that maintaining differentiation, at least in the core areas of access and security, will become difficult within 12-18 months. As a result, presence criteria are already relatively important, and will be increasingly so going forward. Ultimately, this will favor larger, more diversified vendors, and only the topmost of the smaller (pure-play) vendors will be able to survive. To some extent, we are already seeing signs of this transition occurring, with some organizations opting to hold off on their investment until their favorite/incumbent networking or security behemoth can provide a more capable SSL VPN solution.

**Leaders**

Somewhat surprisingly, the leaders in this evaluation do not come from the ranks of incumbent, dominant security or networking infrastructure companies — with the exception of Juniper Networks, which finds itself in an overall leadership position by virtue of its acquisition of NetScreen, which had earlier acquired SSL VPN visionary Neoteris. Joining Juniper are Aventail, F5 Networks, and Whale Communications. Aventail and Juniper present a similar, highly refined vision of extending secured access to an ever widening user population. Both can lay claim to playing instrumental roles in the formation of this market segment, and their early participation is reflected in the relative maturity of their solutions. F5 networks owes its position in no small part to its acquisition of uRoam, another early entrant which possessed very good technology but was less blessed in the area of business acumen. Finally, Whale Communications has leveraged its proxy capabilities from previous products and now excels in its ability to deliver high degrees of application-specific filtering and attack protection. While only Juniper can be said to have dominant market share at this point, all four of these vendors
have set themselves apart by offering accessibility to a broad range of applications, while also excelling in one or more of each of the critical areas of security, manageability, and performance.

**Challengers**

Representing the majority of participants in this evaluation, the challengers fall into three discernible subgroups. The first of these (in no particular order) comprises Array Networks and NetScaler. Both have strong technical capabilities and are leaders in the area of performance due to core competencies in the discipline of traffic optimization. Despite having solid offerings, they are lacking primarily in terms of market and mind share, and to some extent in product maturity. The second group of challengers is characterized as the “large incumbents” from the networking infrastructure and security markets. It is composed of Cisco Systems, Nokia, Nortel Networks, and finally Check Point Software, which resides on the border between challengers and followers. Each of these companies is viewed as having strong potential based on their track records and considerable resources. In the case of Check Point, its borderline position is primarily the result of being very slow to market with a solution — one that is currently lagging but stands to be a legitimate contender before year’s end. Netilla forms the third subgroup, simply by virtue of not fitting into either of the two previous categorizations. Its specialization in the area of application access is coupled with decent capabilities in the other key areas, but only moderate market and mind share leave it in the middle of the pack.

Overall, the challengers should all be viewed as serious contenders. They tend to have areas of specialization that may align well with the needs of some organizations, or may be an incumbent vendor for others. In either case, organizations should not discount them, and in general should include the one or two players from this category that are best aligned with their needs in any evaluation.

**Followers**

Followers offer solutions that are generally lagging the pace of other competitors. Typically, this would be the result of the company being a relatively new entrant to the evaluated market — or perhaps due to a recent “shift in strategy.” Only rarely is it indicative of a truly weak offering. Indeed, the fact that a company/product is even included in the evaluation should itself be interpreted as a positive condition. The minimum requirements for participation ensure the fundamental viability of all vendors, as well as the general suitability and usage of their products within the META Group client base. Therefore, it is our view that “followers” not only have significant potential, but are also well on the path to achieving “challenger” status. In general, related products will deserve consideration in those instances when specific/unique capabilities and strengths align well with an organization’s requirements.

**Bottom Line**

In this still early stage of the market, organizations should focus on the basics — an access model that meshes with planned deployments and supports required applications in conjunction with an adequate security model. Looking to the future, organizations should focus on performance and adaptable security and user administration capabilities that will enable the extension of SSL VPN solutions beyond remote employee access to encompass partners and customers. We expect the larger incumbents from the networking and security markets to continue making significant headway, ultimately resulting in the demise of all but the top two or three independent players (by 2006).

**Business Impact:** SSL VPNs deserve consideration for the advantages they provide in the areas of secure remote, and non-remote, access to applications. Compared to alternative approaches, they have significant potential for yielding reduced cost of ownership, increased user productivity, enhanced business opportunities, and improved security.