

December 8, 2006

# The Forrester Wave™: SSL VPN Appliances, Q4 2006

by Robert Whiteley

TECH CHOICES



December 8, 2006

## The Forrester Wave™: SSL VPN Appliances, Q4 2006

Juniper Networks Leads The Pack, But Aventail And Citrix Are Closing In

by **Robert Whiteley**

with Simon Yates and Christine E. Atwood

### EXECUTIVE SUMMARY

Forrester evaluated leading SSL VPN appliance vendors across 57 criteria and found that Juniper Networks maintains its SSL VPN leadership thanks to its superior reverse proxy technology and focus on secure mobility. Aventail trails close behind with its fully integrated endpoint security and similar strength in mobile device access. Citrix Systems and Microsoft also provide leading technology that focuses on access and acceleration for corporate apps. Caymas Systems rounds out the Leaders with an innovative approach of combining remote and local network access control. F5 Networks, Cisco Systems, and Nortel Networks are all Strong Performers and round out the evaluation. Further integration of F5's technology into its application switch should nudge it into the Leaders category. Cisco and Nortel — with less application-oriented strategies — remain solid alternatives for firms that simply want to offer IPsec and SSL termination in a single appliance.

### TABLE OF CONTENTS

#### 2 **SSL VPNs Extend Applications To Remote And Mobile Workers**

Today's Solutions Bring New Access, Mobility, And Security Components

Tomorrow's Solutions Move From Network- To Application-Focused Control

#### 4 **SSL VPN Appliance Evaluation Overview**

Evaluation Criteria: Offering, Strategy, And Market Presence

Evaluated Vendors Meet Size, Application Access, And Integrated Security Criteria

#### 7 **SSL VPNs Have Matured**

Conducting Your Own Forrester Wave Analysis

#### 9 **Vendor Profiles**

Leaders: Focus On Application Access

Strong Performers: Focus On Network Access

#### 11 **Supplemental Material**

### NOTES & RESOURCES

Forrester conducted product evaluations in July 2006 and interviewed eight vendors and their reference customers: Aventail, Caymas Systems, Cisco Systems, Citrix Systems, F5 Networks, Juniper Networks, Microsoft, and Nortel Networks.

#### **Related Research Documents**

["Enterprise Remote-Access SSL VPN Adoption In 2006"](#)

June 15, 2006, Trends

["How To Choose An SSL VPN In Three Easy Steps"](#)

March 3, 2006, Tech Choices

["SSL VPNs Poised For Significant Growth"](#)

December 31, 2004, Trends

## TARGET AUDIENCE

IT infrastructure and operations professional, security and risk professional

## SSL VPNs EXTEND APPLICATIONS TO REMOTE AND MOBILE WORKERS

In today's changing business climate, firms must extend application access to an increasing number of corporate assets as well as remote users. As a result, Forrester sees clients in a constant struggle to provide adequate security for traveling employees, partners, suppliers, vendors, and offshore partners. Moreover, we also see many firms that are eager to incorporate better remote access alternatives to protect against workforce disruptions caused by any number of natural and man-made disasters. For many firms, the solution is to deploy SSL VPNs, which provide:

- **A streamlined technology that reduces operational costs.** SSL VPNs require fewer installed components, offer more automated configuration, and focus on end user transparency. The result? SSL VPNs provide an easier way to extend application and data to all employees and noncorporate remote users, while reducing help desk calls at the same time.
- **A framework for access control.** SSL VPNs provide more than just savings that go to the IT bottom line. Because SSL VPNs operate at the application layer — as opposed to IPsec, which operates at the network layer — they provide a wealth of authentication and authorization information. The result is more control for compliance and auditing, whether it's for internal security policies or because of external regulatory pressures like HIPAA.

## Today's Solutions Bring New Access, Mobility, And Security Components

SSL VPNs have evolved during the past four years. The technology started as a simple way to extend email and basic Web apps to employees outside of the firewall. But today's SSL VPN vendors now provide:

- **Sophisticated access methods.** SSL VPNs provide clientless access to corporate apps via a Web browser, but most solutions have expanded to include a traditional client, as well as on-demand agents that act in a semi-clientless mode using ActiveX or Java applets. Now, there's a range of firewall-friendly technologies that cover nearly 100% of all application scenarios — a compatibility issue that plagued earlier generations of SSL VPN appliances. Despite this range, though, clientless is still the preferred method to keep operational costs down, so look for leading vendors to continue to set themselves apart by providing as much browser-based access as possible.
- **Increased mobile device support.** SSL VPN appliance vendors have also turned their R&D efforts to supporting the ever-increasing variety of nontraditional computing devices including smartphones, PDAs, tablets, and purpose-built devices like retail point-of-sale (POS) scanners.

Most of these devices can default to access from a standard Web or WAP browser, but that's often insufficient for complex mobile apps. Leading vendors have built specific security, authorization, and access policies to support mobile devices out of the box.

- **Enhanced endpoint security tools.** Top-tier vendors have focused on three major components of endpoint security: 1) a basic host-checking capability, which scans the end device to make sure software like antivirus, personal firewall, and OS patch levels are installed and up to date; 2) a cache cleaner, which is used to wipe out the browser cache of any downloaded files and cookies; and 3) session encryption, which typically uses Java to build a virtual “sandbox,” so that all activity during the VPN session is isolated, encrypted, and removed once the user logs out. However, as this technology evolves, we see the innovative vendors now focus on embedded malware protection and client-side tools to limit functionality like file shares, printing, and USB flash drives that may lead to information leakage.<sup>1</sup>

### Tomorrow's Solutions Move From Network- To Application-Focused Control

SSL VPNs are already mature products, leaving only subtle differentiation among the leading vendors. But looking forward, we see a clear bifurcation of the SSL VPN market into vendors that are:

- **Network-focused.** The primary focus of these solutions is to provide full-network access to users. These SSL VPNs typically have both IPsec and SSL VPN termination in one appliance and focus on network-layer access control technologies like 802.1X. Moreover, vendors in this category will offer SSL VPNs as an option on several networking technologies such as routers, Ethernet switches, or all-in-one security appliances.
- **Application-focused.** Application-focused SSL VPNs tend to have a stronger emphasis on back-end application integration. They provide better access in a pure clientless mode such as a Web browser and focus on application-layer access control using single-sign on and identity management functionality. They do have endpoint security integration, but tend to be better at policy administration, providing more intuitive user interfaces, and enabling stronger geographic load-balancing capabilities.

Although network- versus application-focused may seem irrelevant, we see many of our most progressive clients turning to an “Internet-everywhere” model. What does this mean? Instead of relying on extensive private network infrastructure, the focus will be on assuming all users are coming in through the Internet and all are treated as “remote” and requiring VPN access. This approach increases the pressure to deploy more sophisticated, application-layer access control to ensure that only necessary corporate data is exposed to users.

## SSL VPN APPLIANCE EVALUATION OVERVIEW

To assess the state of the SSL VPN appliance market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top SSL VPN vendors.

### Evaluation Criteria: Offering, Strategy, And Market Presence

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria (see Figure 1). We evaluated vendors against approximately 57 criteria, which we grouped into three high-level buckets:

- **Current offering.** To assess product strength, we evaluated each offering against nine groups of criteria: product portfolio; core SSL VPN functionality; manageability and usability; scalability; reliability; performance; monitoring and reporting; security support; and mobility support.
- **Strategy.** We considered how well each vendor's plans for product enhancement position it to meet future demands from companies and, furthermore, the financial resources the company has to support its strategy, both product and corporate. We looked at the company resources dedicated to corporate client security and how the vendor prices its product to compete in this market.
- **Market presence.** To establish a product's market presence, we combined information about each vendor's installed base, revenues (overall and product), services, employee numbers, and partnerships.

### Evaluated Vendors Meet Size, Application Access, And Integrated Security Criteria

Forrester included eight vendors in the assessment: Aventail, Caymas Systems, Cisco Systems, Citrix Systems, F5 Networks, Juniper Networks, Microsoft, and Nortel Networks. Each of these vendors has (see Figure 2):

- **A generally available SSL VPN appliance.** We chose to focus on the most predominant SSL VPN form factor — appliances — as opposed to a software-based or managed services product. To participate, vendors had to have an appliance product that was currently shipping to customers.
- **Sufficient revenue and customers.** We chose to set participation requirements of at least \$5 million in annual product sales as well as at least 100 current SSL VPN customers.
- **Innovative application access and security functionality.** We chose to include vendors that had demonstrated specific functionality that went above and beyond in application access (advanced browser and OS support, mobile device support, etc.) and integrated security (integrated threat protection, antimalware, NAC, etc.).

- **Client interest.** Finally, we selected vendors about which we received at least three inquiries from our enterprise clients in the past two years.

---

**Figure 1** Evaluation Criteria
 

---

CURRENT OFFERING	
Product portfolio	How many different products are currently offered as part of the vendor's SSL VPN product portfolio?
Core SSL VPN functionality	How robust is the vendor's core SSL VPN access capabilities?
Manageability and usability	How easy is it to manage the appliance?
Scalability	How scalable is the appliance?
Reliability	What specific architectural options does the vendor offer for appliance reliability, including: embedded OS/software reliability, hardware redundancy, hot-swappable components, stateful failover, etc.?
Performance	How does the vendor assess the appliance's performance? How does the vendor measure and support quality of service (QoS)? What throughput can the vendor's appliance support? Does the vendor offer performance-enhancing functionality, including: caching, compression, load balancing, dedicated encryption hardware, protocol-specific optimization, etc.?
Monitoring and reporting	What monitoring and reporting capabilities does the vendor offer?
Security support	What additional security functions does the vendor's appliance support?
Mobility support	How well does the vendor's appliance support additional mobile remote access, including mobile devices, operating systems and session persistence, seamless roaming, and link optimization?
STRATEGY	
Product strategy	What's the vendor's overall product strategy and vision for SSL VPNs?
Corporate strategy	What's the vendor's overall corporate commitment to the SSL VPN space?
Financial resources to support strategy	Is the vendor profitable, and what is the vendor's cash flow? Does the company have sufficient revenues, profits, and cash flow to support its strategies?
Cost	What is the cost of this product?

36451

Source: Forrester Research, Inc.

**Figure 1** Evaluation Criteria (Cont.)

MARKET PRESENCE	
Installed base	How large is the vendor’s installed base of customers for this product and for all products?
Revenue	What is the vendor’s overall and SSL VPN revenue over the past four quarters?
Revenue growth	What is the vendor’s overall and SSL VPN year-over-year revenue growth over the past four quarters?
Services	How strong are the vendor’s implementation and training services?
Employees	How many engineers does the vendor have dedicated to this product? How big is the vendor’s sales presence?
Channel partners	How strongly do channel and go-to-market partners support this product?

36451

Source: Forrester Research, Inc.

**Figure 2** Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated
Aventail	Aventail EX-Family SSL VPN Appliance
Caymas Systems	Caymas Systems’ Identity-Driven Access Gateways
Cisco Systems	Cisco Systems’ ASA 5500 Adaptive Security Appliance
Citrix Systems	Citrix Systems’ Access Gateway
F5 Networks	F5 Networks’ FirePass
Juniper Networks	Juniper Networks’ Secure Access
Microsoft	Microsoft’s Intelligent Application Gateway
Nortel Networks	Nortel Networks’ VPN Gateway

**Vendor selection criteria**

**A generally available SSL VPN appliance.** All vendors have an appliance product that was currently shipping to customers.

**Sufficient revenue and customers.** All vendors have at least \$5 million in annual product sales as well as at least 100 current SSL VPN customers.

**Innovative application access and security functionality.** All vendors have demonstrated specific functionality that goes above and beyond basic application access (advanced browser and OS support, mobile device support, etc.) and integrated security (integrated threat protection, antimalware, NAC, etc.).

**Client interest.** Forrester’s enterprise clients have asked at least three inquiries in the last two years about each vendor.

36451

Source: Forrester Research, Inc.

## SSL VPNs HAVE MATURED

Forrester originally evaluated the SSL VPN market in 2004.<sup>2</sup> Although many of the players are the same, we found a market that was still maturing. Most vendors were in “catch-up” mode and trying to close feature-function gaps. Differentiation primarily rested on the viability of the companies. Two years later, we find a more mature market with large, well-established vendors carrying strong IT brands. Furthermore, differentiation is less focused on viability and more on the vendor’s vision for application-focused gateways. Specifically, we uncovered a market in which (see Figure 3):

- **Juniper and Aventail lead the pack.** Although we evaluated several vendors and found multiple vendors in the Leaders category, Juniper and Aventail outshone everyone. Juniper provides the most complete product with a solution that earned top scores in nearly every current offering criteria. Aventail, on the other hand, had the most advanced strategy with a forward-looking vision that’s most in line with Forrester’s requirements for an application-focused appliance.
- **Citrix, Microsoft, and Caymas offer competitive alternatives.** Coming up behind the two Leaders is a pack that includes Citrix, Microsoft, and Caymas. Citrix and Microsoft both offer a compelling application-focused appliance, with each plugging into a larger architecture. Citrix focuses on application delivery and Microsoft focuses on application security gateways. Caymas is the dark horse of this evaluation: It currently lacks the polish of the other four products, but its innovative, turnkey NAC functionality scores ahead of most competitors in the market.
- **F5, Cisco, and Nortel lag slightly behind.** Although all three are Strong Performers, we found that each vendor’s solution lacks specific application-focused criteria. Forrester believes that F5 will close the gap as it executes on further product integration, while Cisco and Nortel will remain the clear options for firms that require a network-focused product with dual IPsec and SSL VPN termination.

## Conducting Your Own Forrester Wave Analysis

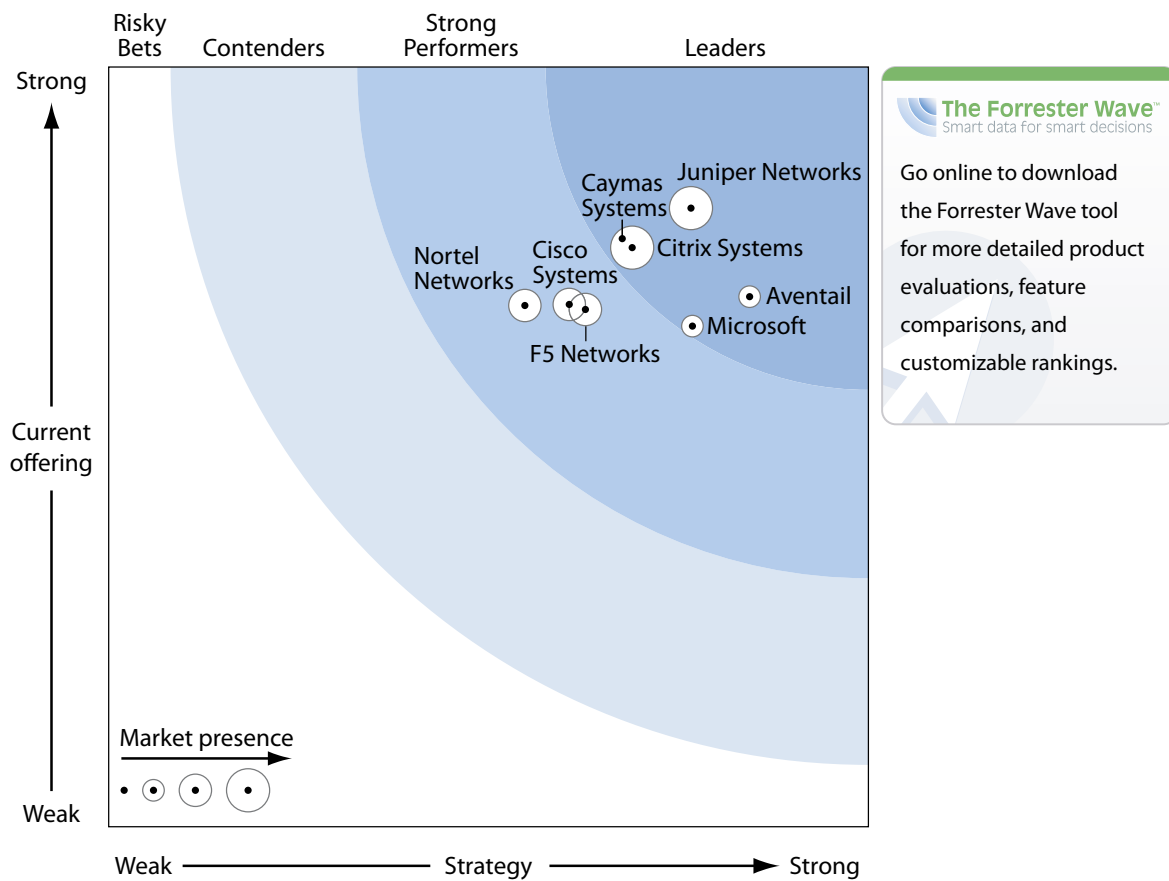
This evaluation of the SSL VPN appliance market is intended to be a starting point only. Readers are encouraged to view detailed product evaluations and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool. Three steps will help you to customize Forrester’s analysis:

- **Understand the evaluation criteria.** The criteria tab in the spreadsheet includes a description and grading scale for each criterion. Peruse these descriptions and mark the ones that are most important to you.
- **Change weightings as needed.** Forrester weighted the evaluation criteria based on what we feel is most important to meet our clients’ needs as a whole. But every company is different. For example, larger companies may have higher scalability requirements and hence, may want to adjust the weightings in favor of vendors that provide only 3,000 concurrent users per

appliance ore more. Alternatively, a retail institution with multiple regional offices may not need multiplatform support and instead would prefer role-based administration.

- **Determine your vendor shortlist with your customized Forrester Wave.** The Forrester Wave tab will automatically update the Wave graphic and vendor ranking, placing the best fits for your needs in the Leader category. You may also decide to develop your request for proposal (RFP) based on our evaluation criteria, as these are the areas in which we identified vendor differentiation.

**Figure 3** Forrester Wave™: SSL VPN Appliances, Q4 '06



36451

Source: Forrester Research, Inc.

**Figure 3** Forrester Wave™: SSL VPN Appliances, Q4 '06 (Cont.)

	Forrester's Weighting	Aventail	Caymas Systems	Cisco Systems	Citrix Systems	F5 Networks	Juniper Networks	Microsoft	Nortel Networks
<b>CURRENT OFFERING</b>	50%	3.49	3.87	3.42	3.81	3.40	4.06	3.30	3.42
Product portfolio	5%	3.00	2.00	5.00	4.00	2.00	3.00	3.00	4.00
Core SSL VPN functionality	25%	5.00	4.40	3.40	3.40	4.20	4.50	3.20	2.90
Manageability and usability	15%	4.40	3.90	2.80	3.80	4.00	4.20	4.00	3.30
Scalability	10%	2.00	5.00	5.00	4.40	2.00	2.80	3.20	5.00
Reliability	10%	3.00	5.00	1.00	5.00	3.00	5.00	3.00	3.00
Performance	10%	1.00	3.00	5.00	5.00	4.00	3.00	2.00	4.00
Monitoring and reporting	5%	4.00	4.00	3.00	5.00	3.00	4.00	5.00	3.00
Security support	15%	2.55	3.25	3.30	2.65	3.00	4.15	3.85	3.35
Mobility support	5%	5.00	2.00	3.00	2.00	3.00	5.00	2.00	3.00
<b>STRATEGY</b>	40%	4.22	3.38	3.04	3.45	3.14	3.83	3.84	2.74
Product strategy	60%	4.50	3.00	3.30	3.90	3.70	4.80	4.70	2.60
Corporate strategy	20%	4.50	4.25	2.00	1.75	1.50	2.25	2.25	1.50
Financial resources to support strategy	5%	3.00	2.00	5.00	4.00	3.00	4.00	5.00	4.00
Cost	15%	3.10	4.20	2.70	3.70	3.10	2.00	2.10	4.50
<b>MARKET PRESENCE</b>	10%	2.79	1.64	3.30	4.07	3.07	4.20	2.75	3.33
Installed base	30%	2.40	1.40	3.00	4.30	3.50	4.60	2.10	2.60
Revenue	30%	3.00	1.00	2.00	4.00	3.00	5.00	2.00	4.00
Revenue growth	10%	2.00	4.00	5.00	5.00	2.00	1.00	3.00	3.00
Services	10%	3.00	2.00	5.00	3.00	3.00	5.00	3.00	4.00
Employees	10%	2.40	1.20	4.20	2.80	2.40	3.40	4.20	4.20
Channel partners	10%	4.25	2.00	3.75	5.00	3.75	3.75	5.00	2.25

All scores are based on a scale of 0 (weak) to 5 (strong).

36451

Source: Forrester Research, Inc.

## VENDOR PROFILES

### Leaders: Focus On Application Access

- **Juniper Networks.** Juniper is the clear leader in the SSL VPN market. Although its solution has enjoyed a much more comfortable lead in the past, Juniper continues to maintain its success by focusing on superior client access, endpoint security, and reliability. The result is the most well-rounded solution that excels at all the core requirements. In fact, the only significant downside is its price which, according to our evaluation, had the highest MSRP. However, Juniper enjoys a substantially larger customer base than the other vendors, providing it with the best “operational experience.” In other words, if you’re looking to deploy an SSL VPN, you can

be confident that Juniper has seen similar requirements and will provide the necessary pre- and post-sales support to implement your remote access project.<sup>3</sup>

- **Aventail.** Aventail is perennial No. 2 in the SSL VPN market. Its solution provides market-leading functionality for clientless access, policy control, and mobile device connectivity. It lags No. 1 Juniper only because it lacks a broader security story, which Aventail has intentionally shied away from to maintain its purpose-built solution. The result is the best solution for IT and network administrators that are focused on providing application access without re-architecting the data center security perimeter. Aventail also has the best long-term strategy, which builds on its strength in endpoint security and authorization, to evolve into a broader application access control gateway — a market Forrester predicts will make the remote access VPN market obsolete within three years.<sup>4</sup>
- **Citrix Systems.** Citrix has been one of the fastest rising SSL VPN appliance vendors. Its solution — with technology from several acquisitions — has culminated in one of the highest performing solutions. Although it still lacks the additional threat protection, customization, and mobile device support of fellow leaders Aventail and Juniper, it has built a solid all-purpose appliance. If you're an existing Citrix customer, this is a much-needed component for extending apps to the Web without cumbersome publishing to Presentation Server. For non-Citrix environments, this SSL VPN appliance is still one of the best thanks to its ease of use and acceleration technologies.<sup>5</sup>
- **Microsoft.** Microsoft has moved quickly and efficiently into the SSL VPN appliance market with its acquisition of Whale Communications, now a wholly owned subsidiary. Whale's Intelligent Application Gateway places Microsoft among the top SSL VPN vendors and provides a critical component for enhancing its Internet Security and Acceleration (ISA) Server. The result should not only be a heavyweight contender for enterprise remote access, but an ideal architecture for small and medium-size businesses (SMBs) as well. Microsoft's SSL VPN crown jewel is its Intelligent Application Optimizer templates for deploying large applications, which will save hours of complex configuration for IT administrators.<sup>6</sup>
- **Caymas Systems.** Caymas is the smallest and least-known vendor in this evaluation, but we recommend that enterprises short-list this vendor. Why? Because its Identity-Driven Access Gateways provide an innovative combination of remote access — both SSL and IPsec VPN termination — as well as the necessary throughput and functionality for the red-hot network access control (NAC) space. Its SSL VPN lacks the polish of Juniper and Aventail for mobile device support, but its integrated approach will simplify network architectures and provide a consistent access policy for local — wired and wireless — and remote users.<sup>7</sup>

### Strong Performers: Focus On Network Access

- **F5 Networks.** F5 Networks has been heads-down on integrating its FirePass SSL VPN solution into its modular TMOS architecture, which runs on products like its flagship BIG-IP application

acceleration device. The result is a competitive solution, but the integration efforts have slipped F5 behind the leaders — especially in areas around scalability and security. However, F5's vision and strategy for 2007 will easily close any gaps and its underlying technology still scores well on ease of use and policy. Moreover, F5 is one of the best data center citizens — understanding the tough operational requirements of your data center — and leverages its partnerships for expertise in tuning specific application nuances from the likes of SAP, Oracle, and Microsoft.<sup>8</sup>

- **Cisco Systems.** Cisco has been a player in the SSL VPN market for several years, but last year's introduction of its ASA 5500 Adaptive Security Appliance moved Cisco up several rungs on the SSL VPN appliance ladder. But Cisco differs from leaders like Aventail, F5, and Juniper by focusing more on a network-based solution. What does that mean exactly? Rather than deep access control, Cisco focuses on a more flexible IPsec and SSL VPN solution with an impressive array of integrated security functions. The ASA provides a one-stop remote access and threat protection gateway, but we recommend evaluating other SSL VPN solutions if you require broad mobile device support and granular application-level authorization today.<sup>9</sup>
- **Nortel Networks.** Nortel currently lags behind the other eight vendors that we evaluated, but only by a narrow margin. Its strength is in marrying network-based technologies and a well-integrated IPsec and SSL VPN product. Borrowing from its successful Contivity and Alteon products, Nortel has one of the larger portfolios of SSL VPN options with its VPN Gateway series as the flagship appliance. If you're looking for a product to ease end user migration to SSL, then Nortel provides the best option today. If it continues to execute on its strategy, Nortel should close any remaining gaps — like bolstering policy support with better management tools — to move into the Leader category.<sup>10</sup>

## SUPPLEMENTAL MATERIAL

### Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

### Data Sources Used In This Forrester Wave

Forrester used a combination of two data sources to assess the strengths and weaknesses of each solution:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with one of each vendor's current customers.

## The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

## ENDNOTES

- <sup>1</sup> Forrester also defines integrated versus embedded endpoint security, which deals with how much of the functionality is offered natively instead of via third-party interoperation. See the March 3, 2006, Tech Choices "[How To Choose An SSL VPN In Three Easy Steps.](#)"
- <sup>2</sup> Forrester's first SSL VPN Wave found that Juniper (then NetScreen) led the charge with the most complete solution, while Nortel and Aventail were close behind with unique functionality. See the March 19, 2004, Tech Choices "[Making SSL VPNs A Strategic Part Of Your Network.](#)"
- <sup>3</sup> View the vendor summary for more detailed analysis on how Juniper Networks fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices "[Juniper Networks Leads The SSL VPN Appliance Market.](#)"
- <sup>4</sup> View the vendor summary for more detailed analysis on how Aventail fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices "[Aventail Is The Best Standalone Solution In The SSL VPN Appliance Market.](#)"
- <sup>5</sup> View the vendor summary for more detailed analysis on how Citrix Systems fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices "[Citrix Systems' App Performance Is Tops In The SSL VPN Appliances Market](#)"

- <sup>6</sup> View the vendor summary for more detailed analysis on how Microsoft fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices “[Microsoft Brings Application Optimization To The SSL VPN Appliance Market.](#)”
- <sup>7</sup> View the vendor summary for more detailed analysis on how Caymas Systems fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices “[Caymas Systems Introduces NAC To The SSL VPN Appliance Market.](#)”
- <sup>8</sup> View the vendor summary for more detailed analysis on how F5 Networks fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices “[F5 Networks Provides The Best Policy In The SSL VPN Appliance Market.](#)”
- <sup>9</sup> View the vendor summary for more detailed analysis on how Cisco Systems fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices “[Cisco Systems Offers The Most Integrated Security In The SSL VPN Appliance Market.](#)”
- <sup>10</sup> View the vendor summary for more detailed analysis on how Nortel Networks fared in this evaluation. See the December December 8, 2006, 2006, Tech Choices “[Nortel Networks Smoothly Integrates IPsec Into The SSL VPN Appliance Market.](#)”

# FORRESTER®

Helping Business Thrive On Technology Change

## Headquarters

Forrester Research, Inc.  
400 Technology Square  
Cambridge, MA 02139 USA  
Tel: +1 617/613-6000  
Fax: +1 617/613-5000  
Email: [forrester@forrester.com](mailto:forrester@forrester.com)  
Nasdaq symbol: FORR  
[www.forrester.com](http://www.forrester.com)

## Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations,  
visit [www.forrester.com/about](http://www.forrester.com/about).*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or [resourcecenter@forrester.com](mailto:resourcecenter@forrester.com). We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice about technology's impact on business and consumers. For 22 years, Forrester has been a thought leader and trusted advisor, helping global clients lead in their markets through its research, consulting, events, and peer-to-peer executive programs. For more information, visit [www.forrester.com](http://www.forrester.com).