Cisco Security Competitive Reference Guide

Version 2.0

CISCO TM

Contents

Introduction

Welcome to the 2010 Cisco® Security Competitive Reference Guide. This guide provides information about selected security competitors and highlights multiple perspectives: products, company background and financial data, weaknesses, and sales tactics. The objective of this guide is to outline the advantages of Cisco security products in comparison to competitive offerings, and to help you address Cisco competitors as you encounter them.

Organization

Introduction

- Cisco Security Solutions Positioning and Overview
- Competitor Comparison Tables: Company Overviews
- Cisco Secure Borderless Networks

Company Profiles and Products

- Firewall/IPsec VPN
- IDS/IPS
- NAC
- SSL VPN
- Email Messaging Security
- Web/URL Filtering

Sections in Each Company Guide

A. Company Overview

B. Financial Profile

C. Product Guide

D. Sales Tactics

E. Weaknesses

Conclusion

- Why Work with Cisco?
- Cisco Innovation
- Cisco Secure Borderless Networks
- Cisco Security Services and Support

Introduction

Company and Technology Grid

Table 1 provides a list of companies and the pages where you can find the breakdown of their respective products. The first time a company appears in the guide is where their company profile and financial overview appear.

Table 1: Company and Technology Grid

Company and Technology Grid

	Firewall/ IPsec VPN (and SSL VPN)	IDS/IPS	NAC	SSL and IPsec VPN	Email/ Messaging Security	Web/URL Filtering
3Com TippingPoint		74				
Barracuda Networks					160	186
Blue Coat Systems						190
Bradford Networks			106			
Check Point	16			126		
Cisco						
Citrix				130		
F5				142		
Finjan						194
Fortinet	28					
Google Apps and Postini					166	
IBM ISS		80				
Juniper Networks	40	87	112	146		
McAfee		92	116		174	198
Microsoft Forefront					170	
Palo Alto Networks	52					
SonicWALL	60			151		
Sourcefire		98				
Symantec			120		180	
Websense, Inc.						202

Cisco Security Solution Positioning and Overview

The Cisco Secure Borderless Network is for organizations of all sizes, public and private, that need to reduce IT security and compliance risk, enable adoption of collaboration technologies, protect valuable data and resources, all while decreasing IT administrative burden and reducing total cost of ownership (TCO). Unlike many security vendors who offer point products, Cisco offers security solutions that not only work together, but integrate into the rest of a network. Cisco offers one of the broadest and deepest product and service portfolios in the industry, with channel partners who are empowered to design and implement solutions customized to customers' unique requirements and a channel ecosystem for comprehensive coverage.

Cisco is helping create a new security paradigm – one in which a distributed and mobile workforce can collaborate, communicate, and access resources with optimal security and flexibility. Our solutions help organizations meet evolving security requirements while controlling cost and complexity.

Our strength is evidenced by our history of security innovations since 1995; our security market leadership position in firewalls, virtual private networks, intrusion prevention, and email security; numerous product awards; and organizations across the globe who are using Cisco security solutions to address their most challenging business requirements of maintaining and extending security to allow the right people to easily access the right resources, from any device and location. A number of vendors want to serve the security market, but their offerings often fall short of the comprehensive solutions required by today's demanding customers—and offered by Cisco.

Competitor Comparison Tables: Company Overviews

Tables 2 through 7 position the security solutions from commonly encountered competitors. You will see products listed multiple times as some have dual roles and are used differently in small-, medium-sized, and large networks; the tables are a guide as to how the devices can be used. There is also some overlap in company segment sizes. Competitor products were placed according to the competitor's positioning of the product; note that the higher-end small- and medium-sized business (SMB) products could be placed in the mid-market section, and vice versa.Table 2 lists the competitor firewall solutions mapped against Cisco firewall solutions as of January 2010.

Table 2: Firewall/VPN Solutions

Firewall/VPN Solutions

Companies	Cisco	Check Point	Fortinet	Juniper	Palo Alto Networks	SonicWALL
SMB	Cisco ASA 5505, 5510, and 5520, Cisco 860, 880, and 890 Series ISR	Safe@Office and UTM-1 Edge, UTM-1 272/276 and 132/136; IP 295 and 152	FortiGate 30B, 50B, 60B, 80C, 82C, 110C/111C	SSG 5, 5 Wireless, 20, 20 Wireless; SRX 100, 210, 240	PA-500	TZ 100, 180, 200, and 210

Introduction

Table 2: Firewall/VPN Solutions

Firewall/VPN Solutions (continued)

Companies	Cisco	Check Point	Fortinet	Juniper	Palo Alto Networks	SonicWALL
Mid-Market	Cisco ASA 5520, 5540, and 5550; Cisco 1900 and 2900 Series ISR	UTM-1: 572/576, 1073/1076, and 2073/2076; Power-1 5070; IP 565 and 395	FortiGate 200A, 200B, 224B, 300A, 310B, 311B, 400A, 500A, and 800	SSG 140, 320, 350, 520, and 550; SRX 650, 3400, and 3600	PA-2020, PA-2050	NSA 240, 2400, 3500, and 4500
Enterprise	Cisco ASA 5550, 5580-20, and 5580-40; Cisco 6500/7600 with FWSM, Cisco 2900 and 3900 Series ISR; Cisco ASR 1000 Series	UTM-1 3070; IAS M2, M6, M8; Power-1 5070, 9070, 11065, 11075, 11085; IP 2455, 1285, 695	FortiGate 1000A, 1000AFA2, 1240B, 3016B, 3600A, 3810A, 5020, 5050, and 5140	ISG 1000 and 2000 with optional IDP; NetScreen 5200 and 5400; SRX 3600, 5600, and 5800	PA-4020, PA-4050, and PA-4060	NSA E5500, E6500, and E7500

ISG = Integrated Security Gateway, NSA = Network Security Appliance, SSG = Secure Services Gateway, SRX = Services

Table 3 lists the SSL VPN competitor solutions mapped against Cisco solutions as of January 2010.

Table 3: SSL VPN Solutions

SSL VPN Solutions

Companies	Cisco	CheckPoint	Citrix	F5	Juniper	SonicWALL
SMB	Cisco ASA 5505, 5510, and 5520	Connectra 270	Access Gateway Standard and Advanced Editions 2010		Secure Access 700	SSL-VPN 200, and Aventail SRA E-Class EX-750
Mid-Market	Cisco ASA 5520, 5540, and 5550	Connectra 3070	Access Gateway Enterprise Edition 7000, 9010, and MPX 7500, and 9500	FirePass 1200	Secure Access 2500 and 4500	SRA 4200, SSL-VPN 4000, and Aventail E-Class SRA EX-6000
Enterprise	Cisco ASA 5550, 5580-20, and 5580-40	Connectra 9072	"Access Gateway Enterprise Edition 10010, and MPX 10500, 12500, 15000, and 17000"	FirePass 4100 and 4300	Secure Access 6500	Aventail E-Class SRA EX-7000

Table 4 lists competitor IDS/IPS solutions mapped against Cisco IDS/IPS solutions as of January 2010.

Table 4: IDS/IPS Solutions

IDS/IPS Solutions

Companies	Cisco	3Com TippingPoint	IBM ISS	Juniper	McAfee	Sourcefire
SMB	Cisco ASA 5510 with AIP10 or 20, Cisco ASA 5520 with AIP10, and Cisco IPS 4240 Sensor	TP-10, 110, and 210E	GX3002, GX4002, and GX4004	IDP 75 and IDP 250	M-1250 and M-1450	3D500, 3D1000, 3D2000, and 3D2100,

.

Table 5 lists competitor NAC solutions mapped against Cisco NAC solutions as of January 2010.

Table5: NAC Solutions

NAC Solutions

Companies	Cisco	Bradford	Juniper	McAfee	Symantec
SMB	Cisco NAC Appliance 335x	Sentry Family NS500	Juniper Networks Infranet Controller 4500 and Unified Access Control (UAC) Agent	McAfee NAC Unified Secure Access (N-450)	
Mid-Market	Cisco NAC Appliance 335x	Sentry Family NS1200/8200	Juniper Networks Infranet Controller 6500 and UAC Agent	McAfee NAC Unified Secure Access (N-450)	Symantec Network Access Control Enforcer 6100 Series DHCP Enforcer and SNAC Client, Symantec Network Access Control Enforcer 6100 Series LAN Enforcer and SNAC Client, and Symantec Network Access Control Enforcer 6100 Series Gateway Enforcer and SNAC Client[1]
Enterprise	Cisco NAC Appliance 339x	Sentry Family NS2200R/NS9200R	McAfee NAC Unified Secure Access (N-450)	Juniper Networks Infranet Controller 6500 and UAC Agent	

SNAC = SQL Native Client

[1] The three Symantec 6100 Series Enforcer appliances are also offered as software-only products. In addition, DHCP Enforcer is offered as a plug-in to a Microsoft Dynamic Host Configuration Protocol (DHCP) server.

Introduction

Table 6 lists competitor email messaging security solutions mapped against Cisco email messaging security solutions as of January 2010..

Table 6: Email Messaging Security Solutions

Email Messaging Security Solutions						
Companies	Cisco IronPort C-Series and X-Series	Barracuda Spam Firewall	Google Apps Powered by Postini	Microsoft	McAfee	Symantec
	C160, C360, C660, and X1060	100, 200, 300, 400, 600, 800, 900, and 1000	Email Security	Microsoft Forefront	McAfee Email Gateway (formerly IronMail) S10, S120, EG-5000, and EG-5500	Symantec Brightmail Gateway 8340, 8360, and 8380

Table 7 lists competitor web/URL filtering solutions mapped against Cisco secure web gateway and URL filtering solutions as of January 2010.

Table 7: Web/URL Filtering Solutions

Web/URL Filtering Solutions						
Companies	Cisco	Barracuda Networks	Blue Coat Systems	Finjan	McAfee	Websense
	IronPort S-Series S160, S360, and S660	Barracuda Web Filter 610, 810, 910, and 1010	Blue Coat SG 810-25, and 8100-30	Vital Security Web Appliance NG-5100, NG-6100 and NG-8100	McAfee Secure Web Gateway (formerly Webwasher) WW500E, WW1100E, WG-5000, and WG-5500	Websense Web Security and Websense V10000

Cisco Secure Borderless Networks

In the past, many businesses thought they had to make a choice when it came to security: they could use best-in-class products that were effective against specific types of emerging threats but did not fully integrate into a pervasive defense system, or they could take a systems approach that assimilated point products that were "good enough" into an intelligent system architecture. For modern businesses, however, neither option is enough. To meet today's security challenges, businesses need solutions that integrate into the network while providing a seamless experience.

Cisco offers one of the broadest and deepest product and services portfolios in the industry, with channel partners that are empowered to design and implement solutions customized to the unique requirements of any business. Building on a history of security innovation, Cisco provides a powerful suite of best-in-class security products, including market-leading firewall, VPN, intrusion prevention system (IPS), and email security technologies. These products have earned the praise of industry analysts and achieved numerous awards and are used by organizations worldwide to address the most challenging business and security needs. Cisco security services also provide organizations with a lifecycle methodology, enabling organizations to design, implement, operate, and optimize secure networks that are resilient and reliable and align technology investment with business strategy.

An Evolving Vision of Security

Cisco Secure Borderless Networks is a fundamental and integrated component of our Borderless Network architecture—the network is the platform for delivering pervasive security. As new business practices emerge so do evolving security needs. Cisco Security protects critical collaboration methods, services, applications, and new platforms such as software-as-a-service (SaaS) and cloud computing. We extend security to the distributed workforce for reliable anytime, anywhere access to people and information.

Organizations need to defend themselves against threats, protect valuable data and resources, and implement the necessary controls for regulatory compliance. However, the distributed workforce—and the borderless network that is used to support it—require a new security strategy to address the following issues:

- Enabling collaboration—Organizations are adopting new applications for integrated voice, video, and conferencing services. These applications need to be secured to protect against vulnerabilities, mitigate risks, and maintain availability.
- The "consumerization" of IT—The popularity of mobile computing devices in the consumer market has helped these devices make their way to corporate networks. While this trend presents flexibility for the end user, security and IT organizations need to consider how to secure the connectivity of these devices, as well as how to extend the right security services and policies to protect them.
- Software-as-a-service (SaaS) delivery models—Pushing more applications and services into the "cloud" can provide tremendous operational benefits, but organizations need assurance that their data is still protected when it is off the enterprise network, and a level of confidence that their security has not been compromised.

Introduction

The comprehensive Cisco Secure Borderless Networks architecture not only provides organizations with the state-of-the-art product capabilities they need to defend against serious emerging threats, but also provides a system that can continually adapt to the changing security landscape and autonomously respond to pervasive threats. In addition, it provides a range of services to help plan, deploy, operate, and optimize the secure system. Over the life of the network, collaboration among Cisco security products continually improves to provide better protection and reduce the time and effort required to achieve security objectives. Ultimately, these capabilities allow businesses to protect critical assets, enforce business policies, and reduce security compliance and IT risk, with less administrative burden and lower TCO.

NOTES

NOTES

Firewall/IPsec VPN

Companies	Sections in Each Company Guide
I. Check Point	A. Company Overview
II. Fortinet	B. Financial Profile
III. Juniper Networks	C. Product Guide
IV. Palo Alto Networks	D. Sales Tactics
V. SonicWALL	E. Weaknesses

Firewall/IPsec VPN: Check Point

I. Check Point

A. Check Point Overview

Check Point Software Technologies Ltd., together with its subsidiaries, develops, markets, and supports a range of software, and combined hardware and software products and services for IT security worldwide. The company offers its customers a portfolio of network and gateway security solutions, data and endpoint security solutions, and management solutions. Its solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways and provides a single agent for various endpoint securities.

The company's network and gateway security solutions include a firewall that inspects traffic as it passes through security gateways; intrusion prevention technologies; VPNs; content screening; messaging security; web-based communications; security acceleration; and virtualization. Its data and endpoint security technologies include personal firewall; data protection; remote access VPNs; and anti-malware. The company's security management solutions include centralized policy management, which enables defining various aspects of the security policy; provisioning tools that allow the daily deployment and removal of individual entities, such as new gateways, users, and devices; monitoring tools; auditing tools; and security information and event management. Check Point sells its products to enterprises, service providers, small and medium-sized businesses, and consumers through a network of channel partners, including distributors, resellers, value-added resellers, system integrators, and managed services providers. The company has strategic relationships with Crossbeam Systems, Inc.; Dell, Inc.; Hewlett-Packard Co.; IBM; Nokia Corporation; Microsoft Corporation; Nortel Networks Corp.; Siemens AG; and Sun Microsystems, Inc. Check Point Software Technologies was founded in 1993 and is headquartered in Tel Aviv, Israel.

B. Check Point Financial Profile

Table 8: Check Point Financial Profile

Check Point Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	808,490	730.88	575.14
Total Cost of Goods Sold (COGS)	92,609	82.3	36.43
Gross Margin (profit)	715,881	648.58	538.51
Sales and Marketing Costs	267,752	271.02	200.62
Research and Development	91,629	80.98	62.21
Administration	No information	No information	No information
Other Expenses	No information	17	1.06
Operating Income or Loss	**356,500**	**279.58**	**274.82**
Number of Employees	1880	1901	1568
Check Point Overall Market Share Position	3	3	3
Worldwide Network Security Market Share	9%	9%	9%

http://stocks.us.reuters.com/stocks/incomeStatement.asp?symbol=CHKP.O&period=A

Firewall/IPsec VPN: Check Point

C. Check Point Product Guide

Table 9: Check Point Products

Check Point Products											
Products	Safe@Office	UTM-1 Edge	UTM-1 130	UTM-1 270	UTM-1 570	UTM-1 1070	UTM-1 2070	UTM-1 3070	IAS M2	IAS M6	IAS M8
Positioning	Small and medium-sized business (SMB) and remote office or branch office (ROBO)	SMB and ROBO	SMB and ROBO	SMB and ROBO	Mid-Sized business	Mid-Sized Business	Mid-Sized Business	Enterprise	Enterprise	Enterprise	Enterprise
Cisco Equivalent	Cisco ASA 5505 and Cisco 880 Series ISR	Cisco ASA 5505 and Cisco 880 Series ISR	Cisco ASA 5520 and Cisco 1900 Series ISR	Cisco ASA 5540 and Cisco 2900 Series ISR	Cisco ASA 5550 and Cisco 3800 Series ISR	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary											
Maximum Firewall Throughput	190 Mbps	190 Mbps	400 Mbps	600 Mbps	1.1 Gbps	2 Gbps	3 Gbps	4.5 Gbps	7 Gbps	16 Gbps	20 Gbps
Maximum Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) VPN Throughput	35 Mbps	35 Mbps	100 Mbps	100 Mbps	250 Mbps	250 Mbps	280 Mbps	1.1 Gbps	2.4 Gbps	3 Gbps	4 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	100	100	No information	No information	No information	No information	No information	No information	No information	No information	No information
Maximum SSL VPN User Sessions	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Maximum Connections	8000	8000	300,000	600,000	1,100,000	1,100,000	1,100,000	1,100,000	1,200,000	1,200,000	1,200,000
Maximum Connections per Second	No information	No information	No information	No information	No information	No information	No information	No information	45,000	65,000	105,000
Packets per Second (64-byte)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Number of Policies Supported	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Technical Summary											
Memory	No information	No information	80 GB HD	160 GB HD	160 GB HD	160 GB HD	160 GB HD	160 GB HD	2 GB	4 GB	8 GB
Minimum System Flash Memory (MB)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Integrated Ports (maximum listed, not default)	4X 10/100	4X 10/100	1X 10/100 and 4X 10/100/1000	4X 10/100/1000	6X 10/100/1000	6 - 10/100/1000	8 - 10/100/1000	8 - 10/100/1000	4 - 10/100/1000	4 - 10/100/1000	4 - 10/100/1000

Firewall/IPsec VPN: Check Point

Table 9: Check Point Products

Check Point Products (continued)

Products	Safe@Office	UTM-1 Edge	UTM-1 130	UTM-1 270	UTM-1 570	UTM-1 1070	UTM-1 2070	UTM-1 3070	IAS M2	IAS M6	IAS M8
Technical Summary (continued)											
Maximum Virtual Interfaces (VLANs)	Yes	32	1024	1024	1024	1024	1024	1024	255	255	255
Number of Expansion Slots	None	None	None	None	None	None	None	None	2	2	4
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput (Mbps)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Features											
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	No information	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
GPRS Transport Protocol (GTP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High-Availability Support	Redundant WAN and dial backup	A/P	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A
IPsec and SSL VPN Services	IPsec	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL
VPN Clustering and Load Balancing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

A = Active, P = Passive.

UTM-1 Edge has eight versions of boxes: X8, X16, X32, and Xu with 8,16, 36, and unlimited users, respectively, and with 1, 10, 15, and 25 remote-access users. The other four are the same but except for wireless: W8, W16, W32, and WU.

Safe@Office comes in four versions: 500, 500W, 500 ADSL, and 500W ADSL, where W indicates a wireless device and ADSL indicates appliances that have an integrated ADSL 2/2+ modem.

Firewall/IPsec VPN: Check Point

Table 9: Check Point Products

Check Point Products

Products	Power-1 5070	Power-1 9070	Power-1 11065	Power-1 11075	Power-1 11085
Technical Summary					
Positioning	Enterprise	Enterprise	Large enterprise and data center	Large enterprise and data center	Large enterprise and data center
Cisco Equivalent	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary					
Maximum Firewall Throughput	9 Gbps	16 Gbps	15 Gbps	20 Gbps	25 Gbps
Maximum Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) VPN Throughput	2.4 Gbps	3.7 Gbps	3.7 Gbps	4 Gbps	4.5 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	No information	No information	No information	No information	No information
Maximum SSL VPN User Sessions	No information	No information	No information	No information	No information
Maximum Connections	1.2 million	1.2 million	1.2 million	1.2 million	1.2 million
Maximum Connections per Second	No information	No information	No information	No information	No information
Packets per Second (64-byte)	No information	No information	No information	No information	No information
Number of Policies Supported	No information	No information	No information	No information	No information
Technical Summary					
Memory	160 GB HD	2X 160 GB HD	2X 250 GB HD	2X 250 GB HD	2X 250 GB HD

Check Point Products

Products	IP295	IP395	IP565	IP695	IP1285	IP2455
Technical Summary						
Positioning	Small and branch office	Small to midsized enterprise and large branch office	Midsized to large enterprise	Midsized to large enterprise and service provider	Large enterprise and service provider	Large enterprise and service provider
Cisco Equivalent	Cisco ASA 5550 and Cisco 3900 Series ISR	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary						
Maximum Firewall Throughput	1.5 Gbps	3 Gbps	7 Gbps	7.2 to 11.7 Gbps	10.3 to 17.5 Gbps	11 to 30 Gbps
Maximum Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) VPN Throughput	1 Gbps	677 Mbps	1.7 Gbps	1.9 to 3.3 Gbps	1.9 to 8.3 Gbps	1.9 to 8.3 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	No information	No information	No information	No information	No information	No information
Maximum SSL VPN User Sessions	No information	No information	No information	No information	No information	No information
Maximum Connections	90,000	1 million	1 million	1 million	1 million	1 million
Maximum Connections per Second	No information	No information	No information	No information	No information	No information
Packets per Second (64-byte)	No information	No information	No information	No information	No information	No information
Number of Policies Supported	No information	No information	No information	No information	No information	No information
Technical Summary						
Memory	1 GB DRAM	1 GB DRAM	1 GB DRAM	2 GB DRAM	4 GB DRAM	4 GB DRAM

Firewall/IPsec VPN: Check Point

Check Point Products (continued)

Products	Power-1 5070	Power-1 9070	Power-1 11065	Power-1 11075	Power-1 11085
Technical Summary (continued)					
Minimum System Flash Memory (MB)	No information	No information	No information	No information	No information
Integrated Ports (maximum listed, not default)	10X 10/100/1000 and optional 10/100/1000 and 10 Gigabit Ethernet modules	14X 10/100/1000, optional 10/100/1000, SFP, and 10 Gigabit Ethernet modules	14X 10/100/1000, optional 10/100/1000, SFP, and 10 Gigabit Ethernet modules	14X 10/100/1000, optional 10/100/1000, SFP, and 10 Gigabit Ethernet modules	14X 10/100/1000, optional 10/100/1000, SFP, and 10 Gigabit Ethernet modules
Maximum Virtual Interfaces (VLANs)	1024	1024	1024	1024	1024
Number of Expansion Slots	1	2	2	2	2
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput (Mbps)	No information	No information	No information	No information	No information
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	Yes
Features					
Application-Layer Security	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	No information	No information	No information	No information	No information
GPRS Transport Protocol (GTP)	Yes	Yes	Yes	Yes	Yes
High-Availability Support	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A
IPsec and Secure Sockets Layer (SSL) VPN Services	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL
VPN Clustering and Load Balancing	Yes	Yes	Yes	Yes	Yes

Products	IP295	IP395	IP565	IP695	IP1285	IP2455
Technical Summary (continued)						
Minimum System Flash Memory (MB)	40 GB HDD or 2 GB flash memory	80 GB HDD or 1 GB flash memory	80 GB HDD or 1 GB flash memory	80 GB HDD or 4 GB flash memory	80 GB HDD or 4 GB flash memory	80 GB HDD or 4 GB flash memory
Integrated Ports (maximum listed, not default)	6X10/100/1000, optional 10/100, 10/100/1000, and SFP modules	4X 10/100/1000, optional 10/100, 10/100/1000, SFP, and T1 WAN modules	4X 10/100/1000, optional 10/100, 10/100/1000, and SFP modules	4X 10/100/1000, optional 10/100, 10/100/1000, SFP, and 10 Gigabit Ethernet modules	4X 10/100/1000, optional 10/100/1000, SFP, and 10 Gigabit Ethernet modules	4X 10/100/1000, optional 10/100/1000, SFP, and 10 Gigabit Ethernet modules
Maximum Virtual Interfaces (VLANs)	1024	1024	1024	1024	1024	1024
Number of Expansion Slots	1 PMC	2 PMC	2 PMC	3 PMC	5 PMC	5 PMC
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput (Mbps)	No information	No information	No information	No information	No information	No information
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	Yes	Yes
Features						
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	No information	No information	No information	No information	No information	No information
GPRS Transport Protocol (GTP)	Yes	Yes	Yes	Yes	Yes	Yes
High-Availability Support	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A
IPsec and Secure Sockets Layer (SSL) VPN Services	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL	IPsec and SSL
VPN Clustering and Load Balancing	Yes	Yes	Yes	Yes	Yes	Yes

PMC = PCI Mezzanine Card, CPCI = Compact PCI, and ADP =Accelerated Data Path.

Firewall/IPsec VPN

Firewall/IPsec VPN: Check Point

D. Check Point Sales Tactics

- Check Point may position its products as security-centric, primarily targeting technical decision makers.
- Check Point generally will promote its SmartCenter, Provider-1, and Eventia management platforms, along with its new Smart-1 management appliances, to provide user-friendly and powerful multidevice management, logging, reporting, and event correlation.
- Check Point is increasingly selling its own private-label appliances, which it uses to migrate Nokia customers and reduce the reliance on Crossbeam in the high-end market.
- Check Point appliance sales now account for approximately 50% of the company's total product sales.
- Check Point released a "new" Software Blade architecture to simplify service deployment and licensing structure, but in reality it is largely a repackaging of its existing security application and management software modules.
- Check Point may propose significant price reductions on its appliances to gain or retain customer accounts.

E. Check Point Weaknesses

- Check Point generally proposes multiple licensing schemes with its product sales.
- Most Check Point high-level OS and application support teams are in Israel, which may present certain difficulties and challenges in dealing with the time zone difference.
- Check Point does not publish connections per second (CPS) performance data for any platforms.
- When unified threat management (UTM) services are turned on, device performance degrades significantly.

NOTES

Firewall/IPsec VPN: Fortinet

II. Fortinet

A. Fortinet Overview

Fortinet, Inc., together with its subsidiaries, provides network security appliances and unified threat management (UTM) network security solutions to enterprises, service providers, and government entities. Its flagship UTM solution consists of the FortiGate appliance product line and FortiGuard security subscription services, which provide various security and networking functions, including firewall, VPN, antivirus, intrusion prevention, web filtering, antispam, and WAN acceleration. Fortinet has operations in the Americas; Europe, the Middle East, and Africa; and the Asia Pacific countries. The company was founded in 2000 and is headquartered in Sunnyvale, California.

B. Fortinet Financial Profile

Table 10: Fortinet Financial Profile

Fortinet Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	211,791	155,366	123,466
Total Cost of Goods Sold (COGS)	65,472	56,652	40,964
Gross Margin (profit)	146,319	98,714	82,502
Sales and Marketing Costs	87,717	72,159	54,056
Research and Development	37,035	27,588	21,446
Administration	16,640	20,544	12,997
Other Expenses	1710	-1,991	-503
Operating Income or Loss	**4927**	**-21,577**	**-5997**
Operating Profit of Loss	9251	-20,061	-4124
Number of Employees	1196		
Fortinet Overall Market Position	5	6	8
Worldwide Network Security Market Share	4%	3%	2%

Firewall/IPsec VPN: Fortinet

C. Fortinet Product Guide

Table 11: Fortinet Products

Fortinet Products								
Products	FG-30B	FG-50B	FG-60B	FG-80C	FG-82C	FG-110C/111C	FG-200A	FG-200B
Positioning	Small office and home office (SOHO) and ROBO	SOHO and ROBO	SOHO and ROBO	SOHO and ROBO	SOHO and ROBO	SOHO and ROBO	Midsized enterprise	Midsized enterprise
Cisco Equivalent	Cisco ASA 5505 and Cisco 860 Series ISR	Cisco ASA 5505 and Cisco 880 Series ISR	Cisco ASA 5505 and Cisco 890 Series ISR	Cisco ASA 5510 and Cisco 1900 Series ISR	Cisco ASA 5510 and Cisco 1900 Series ISR	Cisco ASA 5520 and Cisco 2900 Series ISR	Cisco ASA 5505 and Cisco 890 Series ISR	Cisco ASA 5580-20 and Cisco 3800 Series ISR
Performance Summary								
Maximum Firewall Throughput	30 Mbps	50 Mbps	100 Mbps	350 Mbps	350 Mbps	500 Mbps	150 Mbps	5 Gbps
Maximum 3DES/AES VPN Throughput	5 Mbps	48 Mbps	64 Mbps	80 Mbps	80 Mbps	100 Mbps	70 Mbps	2.5 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	5	20	50	200	200	1500	200	2000
Maximum SSL VPN User Sessions	None	No information	No information	No information	No information	No information	No information	200
Maximum Connections	5000	25,000	70,000	100,000	100,000	400,000	400,000	500,000
Maximum Connections Per Second	1000	2000	3000	5000	5000	10,000	4000	15,000
Packets Per Second (64-byte)	No information	No information	No information	No information	No information	No information	No information	No information
Number of Policies Supported	200	2000	2000	2000	2000	4000	2000	6000
Technical Summary								
Memory (MB)	No information	No information	No information	No information	No information	No information	No information	No information
Minimum System Flash Memory (MB)	No information	No information	No information	No information	No information	No information	No information	No information
Integrated Ports	3X 10/100 LAN and 1X 10/100 WAN	3X LAN and 2X WAN	6X LAN and 2X WAN	6X 10/100 LAN, 2X 10/100/1000 WAN, and 1X 10/100 DMZ	4X 10/100/1000	8X 10/100 LAN and 2X 10/100/1000 WAN	4X 10/100 LAN, 2X 10/100 WAN, and 2X DMZ	8X 10/100 and 8X 10/100/1000
Maximum Virtual Interfaces (VLANs)	255 VLAN per VDOM			255 VLAN per VDOM				
Number of Expansion Slots	None	None	None	None	None	None	None	None
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput	5 Mbps	19 Mbps	20 Mbps	50 Mbps	50 Mbps	65 Mbps	30 Mbps	95 Mbps
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Firewall/IPsec VPN: Fortinet

Table 11: Fortinet Products

Fortinet Products (continued)

Products	FG-30B	FG-50B	FG-60B	FG-80C	FG-82C	FG-110C/111C	FG-200A	FG-200B
Features								
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	0	10 VDOM	10 VDOM	10 VDOM	10 VDOM	10 VDOM	10 VDOM	10 VDOM
GTP (GPRS Transport Protocol)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High Availability Support	None	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/S	A/A and A/P
IPsec and SSL VPN Services	IPsec	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN
VPN Clustering and Load Balancing	No information	No information	No information	No information	No information	No information	No information	No information

A = Active, P = Passive.

Firewall/IPsec VPN: Fortinet

Table 11: Fortinet Products

Fortinet Products (continued)

Products	FG-224B	FG-300A	FG-310B (AMC optional)	FG-311B (AMC optional)	FG-400A	FG-500A	FG-800	FG-1000A	FG-1000AFA2	FG-1240B	FG-3016B	FG-3600A	FG-3810A
Positioning	Midsized enterprise	Midsized enterprise	Small-to-midsized enterprise	Small-to-midsized enterprise	Midsized enterprise	Midsized enterprise	Midsized enterprise	Large enterprise	Large enterprise	Large enterprise	Large enterprise	Large enterprise	Large enterprise
Cisco Equivalent	Cisco ASA 5505 and Cisco 1900 Series ISR	Cisco ASA 5520 and Cisco 2900 Series ISR	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 100 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 100 Series, and 6500/7600 with FWSM	Cisco ASA 5520 and Cisco 2900 Series ISR	and Cisco 2900 Series ISR	Cisco ASA 5550 and Cisco 3900 Series ISR	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary													
Maximum Firewall Throughput	150 Mbps	400 Mbps	8 to 12 Gbps	8 to 12 Gbps	500 Mbps	600 Mbps	1 Gbps	2 Gbps	2 Gbps	40 to 44 Gbps	16 to 20 Gbps	6 to 10 Gbps	7 to 37 Gbps
Maximum 3DES/AES VPN Throughput	70 Mbps	120 Mbps	6 to 9 Gbps	6 to 9 Gbps	140 Mbps	150 Mbps	200 Mbps	600 Mbps	600 Mbps	16 to 18.5 Gbps	12 to 15 Gbps	800 Mbps to 3.8 Gbps	1 to 19 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	200	1500	3000	3000	2000	3000	3000	10,000	10,000	20,000	64,000	64,000	64,000
Maximum SSL VPN User Sessions	No information	No information	No information	No information	No information	No information	No information	No information	No information	1500	No information	No information	No information
Maximum Connections	400,000	400,000	600,000	600,000	400,000	400,000	400,000	600,000	600,000	2 million	1 million	1 million	2 million
Maximum Connections Per Second	4000	10,000	20,000	20,000	10,000	10,000	10,000	15,000	15,000	100,000	25,000	40,000	40,000
Packets Per Second (64-byte)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Number of Policies Supported	2000	5000	8000	8000	5000	8000	20,000	100,000	100,000	100,000	100,000	100,000	100,000
Technical Summary													
Memory (MB)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information

Firewall/IPsec VPN: Fortinet

Table 11: Fortinet Products

Fortinet Products (continued)

Products	FG-224B	FG-300A	FG-310B (AMC optional)	FG-311B (AMC optional)	FG-400A	FG-500A	FG-800	FG-1000A	FG-1000AFA2	FG-1240B	FG-3016B	FG-3600A	FG-3810A
Minimum System Flash Memory (MB)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Integrated Ports	26X 10/100 and 2X 10/100/1000	4X 10/100 and 2X 10/100/1000	10X 10/100/1000	10X 10/100/1000	4X 10/100 and 2X 10/100/1000	8X Fast Ethernet and 2X Gigabit Ethernet	4X 10/100 and 4X 10/100/1000	10X 10/100/1000	10X 10/100/1000 and 2X SFP	16X 10/100/1000 and 24X SFP	2X 10/100/1000 and 16X SFP	8X 10/100/1000 and 2X SFP	8X 10/100/1000 and 2X SFP
Maximum Virtual Interfaces (VLANs)	255 VLAN per VDOM						255 VLAN per VDOM						
Number of Expansion Slots	None	None	1	1	None	None	None	None	None	1	1	1	2 single width and 2 double width
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput	30 Mbps	70 Mbps	160 Mbps	160 Mbps	100 Mbps	120 Mbps	150 Mbps	200 Mbps	200 Mbps	900 Mbps	300 Mbps	400 Mbps	500 Mbps
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Features													
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	10 VDOM	10 VDOM	10 VDOM	10 VDOM	10 VDOM	10 VDOM	10 VDOMs	10 VDOMs	10 VDOMs	25 VDOMs	500 VDOMs	500 VDOMs	500 VDOMs
GPRS Transport Protocol GTP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High-Availability Support	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P
IPsec and SSL VPN Services	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN
VPN Clustering and Load Balancing	No information	No information	No information	No information	No information	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

A = Active, P = Passive.

Firewall/IPsec VPN: Fortinet

Fortinet Products (continued)

Products	FG-5020	FG-5050	FG-5140
Positioning	Large enterprise and MSSP	Large enterprise and MSSP	Large enterprise and MSSP
Cisco Equivalent	Cisco ASA 5580-40, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary			
Maximum Firewall Throughput	Up to 26 Gbps	Up to 65 Gbps	Up to 182 Gbps
Maximum 3DES/AES VPN Throughput	Up to 14 Gbps	Up to 35 Gbps	Up to 98 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	Up to 128,000	Up to 250,000	Up to 700,000
Maximum SSL VPN User Sessions	No information	No information	No information
Maximum Connections	Up to 4 million	Up to 10 million	Up to 28 million
Maximum Connections Per Second	Up to 100,000	Up to 250,000	Up to 700,000
Packets Per Second (64-byte)	No information	No information	No information
Number of Policies Supported	200,000	500,000	1.4 million
Technical Summary			
Memory (MB)	No information	No information	No information
Minimum System Flash Memory (MB)	No information	No information	No information
Integrated Ports	None (chassis)	None (chassis)	None (chassis)
Maximum Virtual Interfaces (VLANs)	255 VLAN per VDOM		
Number of Expansion Slots	2	5	14
Intrusion Prevention	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput	Up to 1 Gbps	Up to 2.5 Gbps	Up to 7 Gbps
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes

Continued on page 39

Fortinet Products (continued)

Products	FG-5020	FG-5050	FG-5140
Features			
Application-Layer Security	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes
Virtual Firewall Instances	Up to 500 VDOMs	Up to 1250 VDOMs	Up to 3500 VDOMs
GPRS Transport Protocol (GTP)	Yes	Yes	Yes
High Availability Support	A/A and A/P	A/A and A/P	A/A and A/P
IPsec and SSL VPN Services	IPsec and SSL VPN	IPsec and SSL VPN	IPsec and SSL VPN
VPN Clustering and Load Balancing	Yes	Yes	Yes

A = Active, P = Passive.

D. Fortinet Sales Tactics

- Fortinet may claim that it is the leading unified threat management (UTM) vendor (referencing IDC reports).
- FortiOS 4.0 adds WAN optimization, application control, SSL inspection, and data loss prevention (DLP) to Fortinet's product offerings.
- Fortinet generally positions UTM content subscription bundles with most appliance offerings.
- Fortinet may position its high-end appliances' throughput performance claims in combination with the potential for other UTM services and a generally low price point in a "getting more for less" package.
- Fortinet generally sells its products and services through resellers.
- Fortinet emphasizes that it has more ICSA certifications than any other security vendor, in addition to key government certifications.

E. Fortinet Weaknesses

- Fortinet's truncated deep inspection intrusion prevention system (IPS) is not as full-featured and does not provide the real-time protection that Cisco® IPS Sensor Software Version 7.0 with Global Correlation does.
- When UTM services are turned on, the device performance degrades significantly. Performance degradation is very dramatic and very unpredictable, even when just two services are enabled, such as IPS and antivirus.
- Fortinet's SSL VPN capabilities are limited. The Cisco ASA Adaptive Security Appliances feature set is much stronger, and the Cisco AnyConnect VPN Client provides greater flexibility in deployment. Fortinet offers clientless SSL VPN only.
- Fortinet bases its data sheet throughput statistics on User Datagram Protocol (UDP) large-packet traffic tests. This type of "bit blaster" test is not as stressful to a stateful firewall as tests using TCP traffic.
- The Advanced Mezzanine Card (AMC), which is used to improve performance of FortiGate, is expensive (approximately US$30,000) and has limitations: for example, it supports only IPv4; the Layer 4 protocol must be UDP, TCP, or Internet Control Message Protocol (ICMP); and it does not support antivirus or IPS inspection.

Firewall/IPsec VPN: Juniper Networks

III. Juniper Networks

A. Juniper Overview

Juniper Networks, Inc. designs, develops, and sells products and services that provide network infrastructure that helps accelerate the deployment of services and applications over a single IP-based network. Its Infrastructure segment provides M-series routers that are used in small and medium-sized core networks, enterprise networks, and in other applications; T-series core routers designed for core IP infrastructures used in the multiservice environment; and E-series products that provide carrier-class routing, broadband subscriber management services, and a range of IP services. This segment also provides MX-series products, which are used to address Ethernet network architectures and services in service provider and enterprise networks; and EX-series Ethernet switches for transporting information in enterprise networks.

The company's Service Layer Technology (SLT) segment offers firewall and VPN systems, and appliances to provide integrated firewall, VPN, and denial-of-service protection capabilities for enterprise environments and service provider network infrastructures. In addition, the SLT segment offers SSL VPN appliances, which are used to secure remote access, extranets, and intranets. This segment also provides intrusion detection and prevention (IDP) appliances for traffic processing, alarm collection, and presentation and forwarding services; application-acceleration products (WX and WXC families) for client-server and web-enabled business applications; and identity and policy control solutions to integrate subscriber privileges, application requirements, and business policies with the IP network infrastructure.

The company also offers technical support and professional services, and a range of education and training programs. Juniper Networks sells its products through direct sales force, distributors, and value-added resellers to global service providers, enterprises, governments, and research and education institutions. The company was founded in 1996 and is headquartered in Sunnyvale, California.

B. Juniper Financial Profile

Table 12: Juniper Financial Profile

Juniper Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	3,572,376	2836.09	2303.58
Total Cost of Goods Sold (COGS)	1,165,966	927.64	754.29
Gross Margin (profit)	2,406,410	1908.45	1549.29
Sales and Marketing Costs	927,777	797.18	685.67
Research and Development	731,151	622.96	480.25
Depreciation and Amortization	No information	85.9	91.82
Administration	No information	No information	No information
Unusual Expenses (income)	13,979	-4.6	1289.32
Other Expenses	38,529	-0.05	0.01
Operating Income or Loss	**694,974**	**407.06**	**-997.78**
Number of Employees	7030	5879	4883
Juniper Overall Market Share Position	2	2	2
Worldwide Network Security Market Share	10%	10%	10%

Firewall/IPsec VPN: Juniper Networks

C. Juniper Product Guide

Table 13: Juniper Products

Juniper Products											
Products	SSG 5 and SSG 5 Wireless	SSG 20 and SSG 20 Wireless	SSG 140	SSG 320M	SSG 350M	SSG 520/ SSG 520M	SSG 550/ SSG 550M	ISG 1000 with Optional IDP	ISG 2000 with Optional IDP	NetScreen-5200	NetScreen-5400
Positioning	Remote office or branch office (ROBO)	ROBO	SMB and midsized business	Regional and branch offices, midsized businesses, and service providers	Regional and Branch Offices, Medium-Sized Businesses, and Service Providers			Large enterprise, data center, and service provider	Large enterprise, data center, and service provider	Data center	Data center
Cisco Equivalent	Cisco ASA 5505 and Cisco 860 or 880 Series ISR	Cisco ASA 5505 and Cisco 880 Series ISR	Cisco ASA 5510 and Cisco 880 Series ISR	Cisco ASA 5520 and Cisco 890 or 1900 Series ISR	Cisco ASA 5540 and Cisco 2900 Series ISR	Cisco ASA 5540 and Cisco 2900 Series ISR	Cisco ASA 5550 and Cisco 3900 Series ISR	Cisco ASA 5580-20, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary											
Maximum Firewall Throughput	160 Mbps	160 Mbps	350 Mbps	450 Mbps	550 Mbps	650 Mbps	1 Gbps	2 Gbps	4 Gbps	10 Gbps	30 Gbps
Maximum 3DES/AES VPN Throughput	40 Mbps	40 Mbps	100 Mbps	175 Mbps	225 Mbps	300 Mbps	500 Mbps	1 Gbps	2 Gbps	5 Gbps	15 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	25 or 40	25 or 40	500	500	500	500	1000	2000	10,000	25,000	25,000
Maximum SSL VPN User Sessions	No	No	No	No	No	No	No	No	No	No	No
Maximum Connections	8000 or 16,000	8000 or 16,000	48,000	64,000	128,000	128,000	256,000	500,000	1 million	1 million	1 million, or 2 million with 2 SPM
Maximum Connections Per Second	2800	2800	8000	8000	12,500	10,000	15,000	20,000	23,000	26,500	26,500
Packets Per Second (64-byte)	30,000	30,000	90,000	175,000	225,000	300,000	600,000	1.5 million	3 million	6 million	18 million
Number of Policies Supported	200	200	1000	2000	2000	4000	4000	10,000	30,000	40,000	40,000
Technical Summary											
Memory (MB)	128 to 256	128 to 256	256 to 512	256 to 1 GB	256 to 1 GB	1 GB	1 GB	No information	No information	No information	No information
Minimum System Flash Memory (MB)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information

Firewall/IPsec VPN: Juniper Networks

Table 13: Juniper Products

Juniper Products (continued)

Products	SSG 5 and SSG 5 Wireless	SSG 20 and SSG 20 Wireless	SSG 140	SSG 320	SSG 350M	SSG 520/ SSG 520M	SSG 550/ SSG 550M	ISG 1000 with Optional IDP	ISG 2000 with Optional IDP	NetScreen-5200	NetScreen-5400
Technical Summary (continued)											
Integrated Ports (maximum listed, not default)	7X 10/100 with factory-configured V.92 or ISDN BRI S/T or RS-232 serial or auxiliary; optional IEEE 802.11a/b/g	5X 10/100 plus 2X I/O slots supporting ADSL 2+, T1, E1, V.92, ISDN BRI S/T, SFP, or serial; optional IEEE 802.11a/b/g	8X 10/100 and 2X 10/100/1000 plus 4X I/O slots supporting T1, E1, ISDN BRI S/T, serial, 10/100/1000, and SFP	4X fixed 10/100/1000 plus 3X I/O slots supporting serial, T1, E1, ADSL/ADSL2/ ADSL2+, G.SHDSL, 8X 10/100/1000, 16X 10/100/1000, and 6X SFP	4X fixed 10/100/1000 plus 5X I/O slots supporting serial, T1, E1, ADSL/ADSL2/ ADSL2+, G.SHDSL, 8X 10/100/1000, 16X 10/100/1000, and 6X SFP	4X fixed 10/100/1000 plus 6X I/O slots supporting serial, T1, E1, DS3, E3, ADSL/ ADSL2/ ADSL2+, G.SHDSL, 10/100, 10/100/1000, and SFP	4X fixed 10/100/1000 plus 6X I/O slots supporting serial, T1, E1, DS3, E3, ADSL/ ADSL2/ ADSL2+, G.SHDSL, 10/100, 10/100/1000, and SFP	Up to 8X mini-GBIC (SX, LX, or TX), up to 8X 10/100/1000, up to 20X 10/100, and up to 2X 10 Gigabit Ethernet	Up to 16X mini-GBIC (SX, LX, or TX), up to 8X 10/100/1000, up to 28X 10/100, and up to 4X 10 gigabit Ethernet	1X expansion slot supporting 2X XFP 10 Gigabit (SR or LR) or 8X Mini-GBIC	3X expansion slots supporting 2X XFP 10 Gigabit (SR or LR) or 8X Mini-GBIC
Maximum Virtual Interfaces (VLANs)	10 base and 50 extended		100	125	125	125	150	4094	4094	4094	4094
Number of Expansion Slots	0	2 I/O	4	3	5	6	6	2 I/O and 1 internal IDP slot	4 I/O and 3 internal IDP slots	1 management and 1 SPM	1 management and 3 SPM
Intrusion Prevention	Yes, D.I.	Yes, D.I.	Yes, D.I.	Yes, D.I.	Yes, D.I.	Yes, D.I.	Yes, D.I.	Yes, D.I. or IDP	Yes, D.I. or IDP	Yes, D.I.	Yes, D.I.
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Features											
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	0	0	0	0	0	0	0	0 default; upgradeable to 50 VSYS	0 default; upgradeable to 250 VSYS	0 default; upgradeable to 500 VSYS	0 default; upgradeable to 500 VSYS
GTP (GPRS Transport Protocol)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High Availability	Dial Backup, A/A and A/P	Dial Backup, A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P
IPsec and SSL VPN Services	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec
VPN Cluster and Loan Balancing	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information

Firewall/IPsec VPN: Juniper Networks

Table 13: Juniper Products

Juniper Products (continued)								
Products	SRX 100	SRX 210	SRX 240	SRX 650	SRX 3400	SRX 3600	SRX 5600	SRX 5800
Positioning	Branch offices	Branch offices	Branch offices	Branch offices	Midsized to large enterprise, public sector, and service provider	Midsized to large enterprise, public sector, and service provider	Large enterprise, public sector, and service provider	Large enterprise, public sector, and service provider
Cisco Equivalent	Cisco ASA 5540 and Cisco 2900 Series ISR	Cisco ASA 5540 and Cisco 2900 Series ISR	Cisco ASA 5550 and Cisco 3900 Series ISR	Cisco ASA 5580-20 and Cisco 3900 Series ISR	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary								
Maximum Firewall Throughput	650 Mbps	750 Mbps	1.5 Gbps	7 Gbps	20 Gbps	30 Gbps	60 Gbps	120 Gbps
Maximum 3DES/AES VPN Throughput	65 Mbps	75 Mbps	250 Mbps	1.5 Gbps	6 Gbps	10 Gbps	15 Gbps	30 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	128	256	1000	3000	5000	5000	5000	5000
Maximum SSL VPN User Sessions	0	0	0	0	0	0	0	0
Maximum Connections	16,000 or 32,000	32,000 or 64,000	64,000 or 128,000	512,000	2.5 million	2.5 million	9 million	10 million
Maximum Connections Per Second	2000	2000	9000	30,000	175,000	175,000	350,000	350,000
Packets Per Second (64-byte)	75,000	80,000	200,000	900,000	3 million	3 million	7 million	15 million
Number of Policies Supported	384	512	4096	8192	40,000	40,000	80,000	80,000
Technical Summary								
Memory (MB)	512 MB to 1 GB	512 MB to 1 GB	512 MB to 1 GB	2GB	No information	No information	No information	No information
Minimum System Flash Memory (GB)	1	1	1	2	No information	No information	No information	No information
Integrated Ports (maximum listed, not default)	8X 10/10	2X 10/100/1000, 6X 10/100, and 1X SRX mini-PIM slot supporting serial, ADSL/ADSL2/ADSL2+,T1,E1, SFP, and 1X Express Card slot for 3G WAN	16X 10/100/1000 and 4X SRX mini-PIM slots supporting serial, ADSL/ADSL2/ADSL2+, T1, E1, and SFP	4X 10/100/1000 and 8X GPIM/XPIM slots supporting 10/100/1000, PoE, SFP, T1, and E1	8X 10/100/1000, 4X SFP, and 4X I/O slots supporting 16X 10/100/1000 copper, 16X Gigabit Ethernet SFP, and 2X 10 Gigabit Ethernet XFP	8X 10/100/1000, 4X SFP, and 4X I/O slots supporting 16X 10/100/1000 copper, 16X Gigabit Ethernet SFP, and 2X 10 Gigabit Ethernet XFP	5X I/O slots supporting 40X Gigabit Ethernet SFP, 4X 10 Gigabit Ethernet XFP (SR or LR), 16X Gigabit Ethernet Flex IOC, and 4X 10 Gigabit Ethernet XFP Flex IOC	11X I/O slots supporting 40X Gigabit Ethernet SFP, 4X 10 Gigabit Ethernet XFP (SR or LR), 16X Gigabit Ethernet Flex IOC, and 4X 10 Gigabit Ethernet XFP Flex IOC
Optional PoE	No	Yes, maximum of 4	Yes, maximum of 16	Yes, maximum of 48	No	No	No	No

Firewall/IPsec VPN: Juniper Networks

Table 13: Juniper Products

Juniper Products (continued)

Products	SRX 100	SRX 210	SRX 240	SRX 650	SRX 3400	SRX 3600	SRX 5600	SRX 5800
Technical Summary (continued)								
Maximum Virtual Interfaces (VLANs)	16	64	512	4096	4096	4096	4096	4096
Number of Expansion Slots	0	1	4	8	4	6	5	11
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	No	No	No	No
Features								
Application-Layer Security	Yes	Yes	Yes	Yes	Limited	Limited	Limited	Limited
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	0	0	0	0	0	0	0	0
GPRS Transport Protocol (GTP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High Availability	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A	A/P and A/A
IPsec and SSL VPN Services	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec
VPN Cluster and Load Balancing	No information	No information	No information	No information	No information	No information	No information	No information

Firewall/IPsec VPN: Juniper Networks

D. Juniper Sales Tactics

- Juniper may claim the SRX 5800 is the “fastest firewall in the world,” but Juniper’s tests use large-packet User Datagram Protocol (UDP) traffic.
- Juniper may claim to be a “leader” in the latest Gartner Magic Quadrant for Enterprise Network Firewalls (second half of 2008 [2H08]).
- Juniper may claim the SRX 3000 and 5000 series provide superior scalability to meet the demands of today’s data center and service provider networks.
- Juniper may target managed security service providers (MSSPs) for either hosted or managed security services, using Network and Security Manager (NSM) and the SRX Series Gateways for the Branch as the service provider’s customer-premises equipment.
- Juniper may position SRX Series Gateways for the Branch products as both secure routers and unified threat management (UTM) content subscription devices against Cisco® products in certain competitive situations.
- Juniper may promote its “One OS” story, yet there are five variants of JUNOS.

E. Juniper Weaknesses

- In JUNOS 10.0, software security processing is not applied to IPv6 packets forwarded by the device.
- When Multiprotocol Label Switching (MPLS) is enabled In JUNOS 10.0, all security features such as security policies, zones, Network Address Translation (NAT), application layer gateways (ALGs), chassis clustering, screens, firewall authentication, and IPsec VPNs are unavailable.
- In JUNOS 10.0, transparent mode does not support NAT, ALG, intrusion detection and prevention (IDP), and IPv6.
- Juniper’s SSG and SRX product lines have no virtual firewall (VSYS) capabilities.
- The SRX series does not send IDP captured packet data to Network and Security Manager (NSM).
- Juniper does not integrate SSL VPN remote-access functions into any products other than the Secure Access product line.
- Juniper has announced that ScreenOS support will end in March 2011, and most Screen OS-based devices cannot run JUNOS.
- When chassis clustering is configured on the SRX, IPv6, IDP, MPLS, multicast, and Layer 2 switching are not supported.
- The SRX series has no security certifications for firewall, remote access VPN, or IPS.

NOTES

Firewall/IPsec VPN: Palo Alto Networks

IV. Palo Alto Networks

A. Palo Alto Networks Overview

Palo Alto Networks, Inc. develops and markets firewalls that enable organizations to gain visibility and control over Internet applications flowing in and out of the networks. The company provides PA-4000 Series firewalls for high-speed Internet gateway deployments within enterprise environments; and PA-2000 Series firewalls for high-speed Internet gateway deployments within large branch offices and medium-sized enterprises. It also offers various network management tools, including Panorama, which provides centralized visibility, control, and management over multiple firewalls; Application Command Center, which provides a visual summary of applications traversing the network; and App-Scope, which gives administrators a comparative view of network activity to help pinpoint erratic behavior. In addition, the company provides a policy editor that allows administrators to create and deploy networks security policies; an application browser, which enables access to a wealth of information on applications, including category, purpose, technology, and behavioral characteristics; and reporting and logging that enable the analysis of security incidents, application usage, and traffic patterns. Its products are used for application visibility and control, real-time threat prevention, security devices consolidation, monitoring and control, and data leakage prevention applications. The company offers its products through channel partners in the United States and internationally. Palo Alto Networks, Inc. was founded in 2005 and is based in Sunnyvale, California.

B. Palo Alto Networks Financial Profile

Table 14: Palo Alto Networks Financial Profile

Palo Alto Networks Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue			
Total Cost of Goods Sold (COGS)			
Gross Margin (profit)			
Sales and Marketing Costs			
Research and Development			
Depreciation and Amortization			
Administration			
Unusual Expenses			
Other Expenses			
Operating Income or Loss			
Number of Employees			
Palo Alto Networks Overall Market Share Position	Company does not report		
Worldwide Network Security Market Share			

Private Company—No Verifiable Detailed Financial Information Available

Firewall/IPsec VPN: Palo Alto Networks

C. Palo Alto Networks Product Guide

Table 15: Palo Alto Networks Products

Palo Alto Networks Products						
Products	PA-500	PA-2020	PA-2050	PA-4020	PA-4050	PA-4060
Positioning	Enterprise branch offices and midsized businesses	Internet gateway	Internet gateway	Internet gateway and data center	Internet gateway and data center	Internet gateway and data center
Cisco Equivalent	Cisco ASA 5510 and Cisco 890 or 1900 Series ISR	Cisco ASA 5540 and Cisco 2900 Series ISR	Cisco ASA 5550 and Cisco 3900 Series ISR	Cisco ASA 5580-20, Cisco ASR 1000 Series, Cisco 3900 Series ISR, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-40, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM
Performance Summary						
Maximum Firewall Throughput	250 Mbps	500 Mbps	1 Gbps	2 Gbps	10 Gbps	10 Gbps
Maximum 3DES/AES VPN Throughput	50 Mbps	200 Mbps	300 Mbps	1 Gbps	2 Gbps	2 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	250	1000	2000	5000	4000	4000
Maximum SSL VPN User Sessions	100	500	1000	5000	10,000	10,000
Maximum Connections	64,000	125,000	250,000	500,000	2 million	2 million
Maximum Connections per Second	7500	15,000	15,000	60,000	60,000	60,000
Packets per Second (64-byte)	No information	No information	No information	No information	No information	No information
Number of Policies Supported	1000	2500	5000	10,000	20,000	20,000
Technical Summary						
Memory	No information	No information	No information	No information	No information	No information
Minimum System Flash Memory	No information	No information	No information	No information	No information	No information
Integrated Ports	8X 10/100/100 and 1X 10/100/1000 management	12X 10/100/1000, 2X SFP Gigabit Ethernet, and 1X 10/100/1000 management	16X 10/100/1000, 4X SFP Gigabit Ethernet, and 1X 10/100/1000 management	16X 10/100/1000, 8X SFP Gigabit Ethernet, 2X 10/100/100 high availability, and 1X 10/100/1000 management	16X 10/100/1000, 8X SFP Gigabit Ethernet, 2X 10/100/100 high availability, and 1X 10/100/1000 management	4X SFP Gigabit Ethernet, 4X 10 Gigabit Ethernet XFP, 2X 10/100/100 high availability, and 1X 10/100/1000 management
Maximum Virtual Interfaces (VLANs)	No information	No information	No information	No information	No information	25 PortShield
Number of Expansion Slots	None	None	None	None	None	No information
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput	100 Mbps	200 Mbps	500 Mbps	2 Gbps	5 Gbps	5 Gbps
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Yes	Yes	Yes	Yes	Yes	Yes

Firewall/IPsec VPN: Palo Alto Networks

Table 15: Palo Alto Networks Products

Palo Alto Networks Products (continued)

Products	PA-500	PA-2020	PA-2050	PA-4020	PA-4050	PA-4060
Features						
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	None	5	5	10	25	25
GPRS Transport Protocol (GTP)	No information	No information	No information	No information	No information	No information
High-Availability Support	A/P	A/P	A/P	A/P	A/P	A/P
IPsec and SSL VPN Services	Both	Both	Both	Both	Both	Both
VPN Clustering and Load Balancing	No information	No information	No information	No information	No information	No information

Firewall/IPsec VPN: Palo Alto Networks

D. Palo Alto Networks Sales Tactics

- Palo Alto may claim it can identify applications across all ports, irrespective of protocol, SSL encryption, or evasive tactic.
- Palo Alto may claim it can provide multigigabit throughput with no performance degradation when deployed inline.
- Palo Alto may claim it can provide policy control based on user identity and/or group membership, not just the IP address.
- Palo Alto may claim it can provide scan application content in real time to prevent threats and data leaks.
- Palo Alto may claim it can provide granular visibility and policy control over application access and functions.
- Palo Alto may claim it can provide not unified threat management (UTM), but a next-generation firewall because it classifies traffic by application, not by port or protocol.
- Palo Alto may claim it can provide superior price-to-performance compared to other high-end firewalls.

E. Palo Alto Networks Weaknesses

- Palo Alto is a privately held company, and therefore the financial and market information that accompanies a publicly traded company is absent.
- Palo Alto launched its product in June 2007, which gives it a limited technical-support track record.
- Palo Alto SSL VPN support was released in June 2009 with limited capabilities compared to the Cisco® ASA 5500 Series Adaptive Security Appliances.
- High-end Palo Alto devices do not have the connections-per-second performance needed for a high-performance firewall.
- Palo Alto does not offer active-active high-availability support.
- Palo Alto does not offer a security information and event management (SIEM) product.
- Palo Alto security features are not as extensive as Cisco's unified computing security features.

NOTES

Firewall/IPsec VPN: SonicWALL

V. SonicWALL

A. SonicWALL Overview

SonicWALL, Inc. designs, develops, manufactures, and sells network security, content security, and business continuity solutions worldwide. The company's products and services provide secure Internet access to both wired and wireless broadband customers, enable Internet-based connectivity for distributed organizations, inspect the content entering and leaving customer networks, protect organizations against inbound and outbound email threats, and provide business continuity in the case of data or connectivity loss.

SonicWALL also offers value-added services for security appliances, including content filtering, anti-spam protection, client antivirus protection, integrated gateway antivirus, anti-spyware, email protection, offsite data backup, and intrusion prevention. In addition, the company licenses software packages, including Global Management System (GMS), Global VPN Client, and email security licenses. The GMS solutions provide network administrators with configuration and management tools to globally define, distribute, enforce, and deploy various security application services and upgrades for its Internet security appliances. The Global VPN Client provides mobile users with a solution for securely accessing the network. Further, SonicWALL Backup and Recovery Offsite Services enable customers to recover data lost in natural disasters, such as floods, fires, and electrical power surges, or from a theft in the business. The company offers solutions for small to medium-sized networks used in enterprises, e-commerce, education, healthcare, and retail/point-of-sale markets. It was formerly known as Sonic Systems and changed its name to SonicWALL, Inc. in August 1999. The company was founded in 1991
and is headquartered in Sunnyvale, California.

B. SonicWALL Financial Profile

Table 16: SonicWALL Financial Profile

SonicWALL Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	218,644	199.2	175.54
Total Cost of Goods Sold (COGS)	66,626	58.68	56.84
Gross Margin (profit)	152,018	140.52	118.7
Sales and Marketing Costs	100,961	99.21	91.58
Research and Development	44,176	39.41	33.67
Depreciation and Amortization	No information	0.71	2.72
Administration	No information	No information	No information
Unusual Expenses (income)	1683	1930	2989
Other Expenses	1114	715	2721
Operating Income or Loss	**4084**	**-751**	**-12,260**
Number of Employees	820	674	436
SonicWALL Overall Market Share Position	8	8	6
Worldwide Network Security Market Share	3%	3%	3%

Firewall/IPsec VPN: SonicWALL

C. SonicWALL Product Guide

Table 17: SonicWALL Products

SonicWALL Products

Products	TZ 180	TZ 100	TZ 200	TZ 210	NSA 240	NSA 2400	NSA 3500	NSA 4500	NSA E5500	NSA E6500	NSA E7500
Positioning	Small, remote, or branch office	Small, remote, or branch office	Small, remote, or branch office	Small, remote, or branch office	Small and midsize enterprise and branch office	Small and midsize enterprise and branch office	Small and midsize enterprise and branch office	Small and midsize enterprise and branch office	Enterprise	Enterprise	Enterprise
Cisco Equivalent	Cisco ASA 5505 and Cisco 890 Series ISR	Cisco ASA 5505 and Cisco 860 Series ISR	Cisco ASA 5505 and Cisco 880 Series ISR	Cisco ASA 5505 and Cisco 890 Series ISR	Cisco ASA 5540 and Cisco 2900 Series ISR	Cisco ASA 5550 and Cisco 2900 Series ISR	Cisco ASA 5550 and Cisco 3900 Series ISR	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000 Series, and 6500/7600 with FWSM	Cisco ASA 5580-20, Cisco 3900 Series ISR, Cisco ASR 1000, and 6500/7600 with FWSM
Performance Summary											
Maximum Firewall Throughput	90 Mbps	100 Mbps	100 Mbps	200 Mbps	600 Mbps	775 Mbps	1.5 Gbps	2.75 Gbps	3.9 Gbps	5 Gbps	5.6 Gbps
Maximum 3DES/AES VPN Throughput	30 Mbps	75 Mbps	75 Mbps	75 Mbps	150 Mbps	300 Mbps	625 Mbps	1 Gbps	1.7 Gbps	2.7 Gbps	3 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	10	5	10	15	25; 50 with stateful high availability and expansion upgrade	75	800	1500	4000	6000	10,000
Maximum SSL VPN User Sessions	0	5	10	10	15	25	30	30	50	50	50
Maximum Connections	6000	6000	8000	10,000	25,000; 35,000 with stateful high-availability and expansion upgrade	48,000	128,000	450,000	600,000	750,000	1 million
Maximum Connections Per Second	250	1000	1000	1500	2000	4000	7000	10,000	15,000	20,000	25,000
Packets Per Second (64-byte)	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Number of Policies Supported	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
Technical Summary											
Memory	128 MB	128 MB	256 MB	256 MB	256 MB	512 MB	512 MB	512 MB	1 GB	1 GB	2 GB
Minimum System Flash Memory	16 MB	16 MB	16 MB	32 MB	32 MB	512 MB	512 MB	512 MB	512 MB CF	512 MB CF	512 MB CF

Firewall/IPsec VPN: SonicWALL

Table 17: SonicWALL Products

SonicWALL Products (continued)

Products	TZ 180	TZ 100	TZ 200	TZ 210	NSA 240	NSA 2400	NSA 3500	NSA 4500	NSA E5500	NSA E6500	NSA E7500
Technical Summary (continued)											
Integrated Ports	7X 10/100	5X 10/100	5X 10/100	2X 10/100/1000 and 5X 10/100	3X Gigabit Ethernet, 6X Fast Ethernet, 1X console interface, and 2X USB ports (future use)	6X Gigabit Ethernet, 1X console interface, and 2X USB ports (future use)	6X Gigabit Ethernet, 1X console interface, and 2 USB ports (future use)	6X Gigabit Ethernet, 1X console interface, and 2X USB ports (future use)	8X Gigabit Ethernet, 1X Gigabit Ethernet high availability, 1X console interface, and 2X USB ports (future use)	8X Gigabit Ethernet, 1X Gigabit Ethernet high availability, 1X console interface, and 2X USB ports (future use)	1X console interface, 4X Gigabit Ethernet, 4X SFP (SX, LX, or TX), 1X Gigabit Ethernet high availability, and 2X USB ports (future use)
Maximum Virtual Interfaces (VLANs)	Yes with SonicOS Enhanced	Yes	Yes	Yes	10; 25 with stateful high availability and expansion upgrade	25	50	200	400	500	512
Number of Expansion Slots	None	None	None	None	No information	No information	No information	No information	No information	No information	No information
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput	10 Mbps	25 Mbps	35 Mbps	50 Mbps	110 Mbps	150 Mbps	240 Mbps	600 Mbps	850 Mbps	1.59 Gbps	1.7 Gbps
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Antivirus and Spyware (optional)				Antivirus, spyware, file blocking, phishing, and URL	Antivirus, spyware, file blocking, phishing, and URL	Antivirus, spyware, file blocking, phishing, and URL	Antivirus, spyware, file blocking, phishing, and URL	Antivirus, spyware, file blocking, phishing, and URL	Antivirus, spyware, file blocking, phishing, and URL	Antivirus, spyware, file blocking, phishing, and URL
Features											
Application-Layer Security	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information	No information
GPRS Transport Protocol (GTP)	No	No	No	No	No	No	No	No	No	No	No
High-Availability Support	No	No	A/P	A/P	Optional A/P with stateful high availability and expansion upgrade	Optional A/P	Optional A/P	A/P	A/P, A/A UTM	A/P, A/A UTM	A/P, A/A UTM
IPsec and SSL VPN Services	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL	IPsec/SSL
VPN Clustering and Load Balancing	Incoming and Outgoing With SonicOS Enhanced				Yes (outgoing with percent-based round-robin and spillover; incoming with round-robin, random distribution, sticky IP, block remap, and symmetrical remap)						
Built-in Wireless	802.11 b/g	802.11 b/g/n			No information						

Firewall/IPsec VPN: SonicWALL

Table 17: SonicWALL Products

SonicWALL Products (continued)

Products	NSA 2400	NSA 3500	NSA 4500	NSA 5000	NSA 5500	NSA E6500	NSA E7500
Positioning	Small and midsize enterprise and branch office	Enterprise	Enterprise	Enterprise	Enterprise	Enterprise	Enterprise
Cisco Equivalent	Cisco 2800 Series and Cisco ASA 5540	Cisco 3800 Series ISR, Cisco ASA 5580-20, and 6500/7600 with FWSM	Cisco 3800 Series ISR, Cisco ASA 5580-20, and 6500/7600 with FWSM	Cisco 3800 Series ISR, Cisco ASA 5580-20, and 6500/7600 with FWSM	Cisco 3800 Series ISR, Cisco ASA 5580-40, and 6500/7600 with FWSM	Cisco 3800 Series ISR, Cisco ASA 5580-40, and 6500/7600 with FWSM	Cisco 3800 Series ISR, Cisco ASA 5580-40, and 6500/7600 with FWSM
Performance Summary							
Maximum Firewall Throughput	450 Mbps	1 Gbps	1.5 Gbps	1.8 Gbps	2 Gbps	3 Gbps	5.5 Gbps
Maximum 3DES/AES VPN Throughput	300 Mbps	625 Mbps	845 Mbps	1.1 Gbps	1.5 Gbps	2.3 Gbps	3 Gbps
Maximum Site-to-Site and Remote-Access VPN User Sessions (tunnels)	75	800	1500	2500	4000	6000	10,000
Maximum SSL VPN User Sessions	No	No	No	No	No	No	No
Maximum Connections	48,000	128,000	450,000	600,000	700,000	750,000	1,000,000
Maximum Connections Per Second	3000	5000	7500	8500	10,000	19,000	25,000
Packets Per Second (64-byte)	No Information	No Information	No Information	No Information	No Information	No Information	No Information
Number of Policies Supported	No Information	No Information	No Information	No Information	No Information	No Information	No Information
Technical Summary							
Memory	256 MB	512 MB	512 MB	1 GB	1 GB	1 GB	2 GB
Minimum System Flash Memory	512 MB	512 MB	512 MB	512 MB	16 MB and 512 MB Compact	512 MB	512 MB
Integrated Ports	6 Gigabit Ethernet, 1 Console Interface, and 2 USB Ports	6 Gigabit Ethernet, 1 Console Interface, and 2 USB Ports	6 Gigabit Ethernet, 1 Console Interface, and 2 USB Ports	6 Gigabit Ethernet, 1 Console Interface, and 2 USB Ports	8 Gigabit Ethernet, 1 Gigabit High Availability, 1 Console Interface, and 2 USB Ports (future use)	8 Gigabit Ethernet, 1 Gigabit High Availability, 1 Console Interface, and 2 USB Ports (future use)	1 Console Interface, 4 Gigabit Ethernet, 4 SFP (SX, LX, or TX), 1 Gigabit High Availability, and 2 USB Ports (future use)
Maximum Virtual Interfaces (VLANs)	128	128	256	256	256	256	512
Number of Expansion Slots	No Information	No Information	No Information	No Information	No Information	No Information	No Information
Intrusion Prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Threat Mitigation Throughput *	50 Mbps	170 Mbps	300 Mbps	350 Mbps	400 Mbps	750 Mbps	1 Gbps
Content Security (antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, and URL filtering)	Antivirus, Spyware, File, Phishing, and URL	Antivirus, Spyware, File, Phishing, and URL	Antivirus, Spyware, File, Phishing, and URL	Antivirus, Spyware, File, Phishing, and URL	Antivirus, Spyware, File, Phishing, and URL	Antivirus, Spyware, File, Phishing, and URL	Antivirus, Spyware, File, Phishing, and URL
Maximum Number of Users for Antivirus, Anti-Spyware, and File Blocking	No Information	No Information	No Information	No Information	No Information	No Information	No Information

* UTM Performance Throughput": UTM performance is based on HTTP tests run on the Spirent Avalanche/Reflector

Firewall/IPsec VPN: SonicWALL

Table 17: SonicWALL Products

SonicWALL Products (continued)

Products	NSA 2400	NSA 3500	NSA 4500	NSA 5000	NSA 5500	NSA E6500	NSA E7500
Features							
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Firewall Instances (virtual IP) (included and maximum)	No Information	No Information	No Information	No Information	No Information	No Information	No Information
GTP and GPRS Inspection	No	No	No	No	No	No	No
High Availability Support	Optional A/P	Optional A/P	A/P	A/P	A/P	A/P	A/P
IPsec and SSL VPN Services	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec	IPsec
VPN Clustering and Load Balancing	Yes (outgoing with percent-based, round-robin and spillover; incoming with round-robin, random distribution, sticky IP, block remap, and symmetrical remap)			Yes (outgoing with percent-based, round-robin and spillover; incoming with round-robin, random distribution, sticky IP, block remap, and symmetrical remap)	No Information	No Information	No Information

Firewall/IPsec VPN: SonicWALL

D. SonicWALL Sales Tactics

- SonicWALL generally focuses on bundling multiple-year unified threat management (UTM) content subscription service contracts with each appliance sale transaction.
- SonicWALL sells almost exclusively through distributors and resellers, which account for approximately 98% of SonicWALL's total revenue.
- SonicWALL generally claims a better price-to-performance point than competitors and then offers its all-in-one-box solution message.
- SonicWALL has offered free upgrades, from SonicOS to Enhanced SonicOS.
- SonicWALL generally has targeted the small and medium-sized business (SMB) market, but it is targeting the enterprise market with the NSA E-Class appliances.

E. SonicWALL Weaknesses

- SonicWALL generally relies on sales to the SMB market for most of its revenue, where gross margins for product transactions are traditionally lower, and price competition more fierce, than in the midsize to large enterprise markets.
- SonicWALL's higher-end appliance products are still relatively new and face many larger and more established competitors.
- SonicWALL sells almost exclusively through distributors and resellers and lacks direct-touch sales capabilities, which may impede its ability to sell to midsize and enterprise markets.
- High-end SonicWALL devices do not have the connections-per-second performance needed for a high-performance firewall.
- SonicWALL's intrusion prevention system (IPS) subscription services offering, which primarily involves specific RFC protocol anomaly detection and regular expression signature matching, is not as full-featured and does not provide the same real-time protection as Cisco® IPS Sensor Software Version 7.0 with Global Correlation.
- SonicWALL does not offer a security information and event management (SIEM) product.

NOTES

NOTES

IDS/IPS

Companies	Sections in Each Company Guide
I. 3Com TippingPoint	A. Company Overview
II. IBM ISS	B. Financial Profile
III. Juniper Networks	C. Product Guide
IV. McAfee	D. Sales Tactics
V. Sourcefire	E. Weaknesses

IDS/IPS: 3Com TippingPoint

I. 3Com TippingPoint

A. 3Com TippingPoint Overview

3Com Corporation provides secure and converged networking solutions that enable customers to manage voice, video, and data in a secure network environment. The company has three global product and solutions brands, including H3C, 3Com, and TippingPoint, which offer networking and security solutions to enterprises large and small. The H3C enterprise networking portfolio includes products that span from the data center to the edge of the network and is targeted at large enterprises. The 3Com family of products offers a price/performance value proposition for the small and medium-size business. Its security brand, TippingPoint, features network-based intrusion prevention systems (IPSs) and network access control (NAC) solutions. It sells its products and services in Europe, the Middle East, Africa, North America, the Asia Pacific, Latin America, and South America. The company was founded in 1979 and is headquartered in Marlborough, Massachusetts.

B. 3Com TippingPoint Financial Profile

Table 18: 3Com TippingPoint Financial Profile

3Com TippingPoint Financial Profile				
	2008	2007	2006	TippingPoint 2008
Dollars in Millions				
Total Revenue	1,316,978	24,462	22,923	No information
Total Cost of Goods Sold (COGS)	565,514	12,735	11,713	No information
Gross Margin (profit)	751,464	11,727	11,210	No information
Sales, General, and Administrative Costs	452,301	5015	5066	No information
Research and Development	179,979	1368	1522	No information
Operating Income or Loss	**100,692**	**6193**	**5696**	**No information**
Operating Profit or Loss	5860	No Information	No Information	300
Number of Employees	4	4	3	4
TippingPoint Network-Based IDS/IPS Market Share Position (based on calendar year revenue)	13%	14%	15%	13%
TippingPoint Network-Based IDS/IPS Market Share (based on calendar year revenue)	14%	15%	14%	No Info

IDS/IPS: 3Com TippingPoint

C. 3Com TippingPoint Product Guide

Table 19: 3Com TippingPoint Products

3Com TippingPoint Products												
Products	TP-10	TP-110	TP-210E	TP-300	TP-600E	TP-1200E	TP-2400E	TP-5000E	TP-650N	TP-1400N	TP-2500N	TP5100N
Cisco Equivalent	Cisco ASA 5510 with AIP10 or Cisco ISR with AIM-IPS	Cisco ASA 5510 with AIP20, Cisco ASA 5520 with AIP10, or Cisco IPS 4240 Sensor	Cisco ASA 5540 with AIP20	Cisco ASA 5540 with AIP20	Cisco ASA 5540 with AIP40 or Cisco IPS 4255 Sensor	Cisco IPS 4260 Sensor	Cisco IPS 4260 Sensor	Cisco IPS 4270-20 Sensor	Cisco ASA 5540 with AIP40 or Cisco IPS 4255 Sensor	Cisco IPS 4260 Sensor	Cisco IPS 4270-20 Sensor	Cisco IPS 4270-20 Sensor
Performance Summary												
Maximum Aggregate Throughput	20 Mbps	100 Mbps	200 Mbps	300 Mbps	600 Mbps	1.2 Gbps	2.0 Gbps	5.0 Gbps	750 Mbps	1.5 Gbps	3 Gbps	5 Gbps
Maximum Number of Concurrent Sessions	250,000	250,000	1,000,000	250,000	2,000,000	2,000,000	2,000,000	2,000,000	6,500,000	6,500,000	10,000,00	10,000,000
Connections per Second	3600	9700	8000	18,500	92,000	215,000	350,000	350,000	115,000	115,000	230,000	230,000
Latency	500 micro seconds	600 micro seconds	600 micro seconds	600 micro seconds	84 micro seconds	84 microseconds	84 micro seconds	84 micro seconds	80 micro seconds	80 micro seconds	80 micro seconds	80 micro seconds
Logging	Yes, through TippingPoint Security Management System (SMS)	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS	Yes, through SMS
Customer Capability to Create Custom Signatures	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrated Security Information and Event Management (SIEM)	No	No	No	No	No	No	No	No	No	No	No	No
High Availability	Active-active (A/A) and active-standby (A/S)	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S
Sensor-to-Management-Server Transport Encryption	Yes, Secure Shell (SSH)	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH	Yes, SSH
Low-Cost Standalone Management and Logging Option	No	No	No	No	No	No	No	No	No	No	No	No
Integrated Management Platform for IPS, Firewall, Secure Sockets Layer (SSL), and IP Security (IPsec) VPN	No	No	No	No	No	No	No	No	No	No	No	No

IDS/IPS: 3Com TippingPoint

Table 19: 3Com TippingPoint Products

3Com TippingPoint Products (continued)

Products	TP-10	TP-110	TP-210E	TP-300	TP-600E	TP-1200E	TP-2400E	TP-5000E	TP-650N	TP-1400N	TP-2500N	TP5100N
Performance Summary (continued)												
Host Intrusion Prevention System (HIPS) Integration and Linkage	No	No	No	No	No	No	No	No	No	No	No	No
OS Fingerprinting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Import of Vulnerability Scanning Data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Session Termination	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hardware Integration with Firewall and VPN Appliances	No	No	No	No	No	No	No	No	No	No	No	No
Protocol, Application, and Statistical Anomaly Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Technical Summary												
Management Platform	TippingPoint SMS		TippingPoint SMS			TippingPoint SMS						
Monitoring and Switched Port Analyzer (SPAN) Ports	4X 10/100 copper	4X 10/100 copper	8X 10/100/1000 copper	8X 10/100/1000 copper	8X 10/100/1000 fiber and copper	8X 10/100/1000 fiber and copper	8X 10/100/1000 fiber and copper	8X 10/100/1000 fiber and copper	20X 10/100/1000 (10X copper, 10X Small Form-Factor Pluggable [SFP])	20X 10/100/1000 (10X copper, 10X SFP)	2X 10 Gigabit Ethernet XFP (modular); 20X 10/100/1000 (10X copper, 10X SFP) (external)	2X 10 Gigabit Ethernet XFP (modular); 20X 10/100/1000 (10X copper, 10X SFP) (external)
Management Interfaces	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial	1X 10/100 and 1X serial
Number of Segments	1	2	5	4	4	4	4	4	10	10	1 (modular), 10 (external)	1 (modular), 10 (external)
Virtual Sensor Support	No	No	No	No	No	No	No	No	No	No	No	No
Size	2 rack unit (RU)	1RU	1RU	1RU	2RU	2RU	2RU	2RU	2RU	2RU	2RU	2RU
Bypass Features	Software	Software	Software	Software	Software	Software	Software	Software	Software	Software	Software	Software
Redundant Power Supplies	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Common Criteria Certification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

IDS/IPS: 3Com TippingPoint

D. 3Com TippingPoint Sales Tactics

- TippingPoint generally positions its products as high-performance, best-of-breed IPS products.
- TippingPoint often uses “speeds and feeds” marketing comparisons in competitive situations, emphasizing its custom application-specific integrated circuit (ASIC) based Threat Suppression Engine (TSE) hardware platform.
- TippingPoint often states that they are in the leaders quadrant in Gartner’s Network IPS Magic Quadrant report. TippngPoint often promote its ICSA and NSS certifications.
- TippingPoint promotes its Zero Day Initiative (ZDI) a program through which the company pays researchers, vendors, and others, a reward for providing TippingPoint with commercial product vulnerabilities.
- TippingPoint (after HP’s proposed acquisition of 3Com) would allow HP to offer next-generation data center security services through their extended product portfolio.

E. 3Com TippingPoint Weaknesses

- 3Com attempted to both spin-off and sell TippingPoint in 2007, creating customer uncertainty as to TippingPoint’s future.
- TippingPoint’s parent company, 3Com, has experienced challenges related to its financial condition, which may negatively affect TippingPoint and its cash requirements.
- TippingPoint has no antivirus, anti-spyware, antispam , and anti-phising (anti-X); SSL-VPN; firewall; or SIEM offerings
- TippingPoint’s brief foray into unified threat management (UTM) product offerings lasted less than 2 years, and those products have been in end-of-life and end-of-support status since November 2007. In addition, TippingPoint has not had any field replacements for those appliances.
- When compared with competitive equivalent offerings, TippingPoint appliances generally have very high list prices, especially for primarily an IPS-specific solution.

NOTES

IDS/IPS: IBM ISS

II. IBM ISS

A. IBM ISS Overview

IBM develops and manufactures IT products and services worldwide. Its Global Technology Services segment offers IT infrastructure and business process services, such as strategic outsourcing, integrated technology, business transformation outsourcing, and maintenance. The company's Global Business Services segment provides professional services and application outsourcing services, including consulting and systems integration, and application management. Its Systems and Technology segment offers computing and storage solutions, including servers, disk and tape storage systems and software, semiconductor technology and products, packaging solutions, engineering and technology services, and retail store solutions. IBM's Software segment primarily offers middleware and OS software comprising WebSphere software for web-enabled applications; information management software for database, content management, information integration, and business intelligence; Tivoli software for infrastructure management, including security and storage management; Lotus software for collaboration, messaging, and social networking; and rational software, a process automation tool. The company's Global Financing segment provides commercial financing to dealers and remarketers of IT products; lease and loan financing to external and internal clients; and sale and lease of used equipment. IBM serves banking, insurance, education, government, healthcare, life sciences, aerospace and defense, automotive, chemical and petroleum, electronics, distribution, telecommunications, media and entertainment, and energy and utilities, as well as small and medium-sized business. The company was formerly known as Computing-Tabulating-Recording Co. and changed its name to International Business Machines Corporation in 1924. IBM was founded in 1910 and is based in Armonk, New York.

ISS, originally founded in 1994 as a security company, and later acquired by IBM in 2006, supplies products and services based on the security intelligence conducted by the ISS X-Force research and development team. In addition to its Atlanta, Georgia headquarters, IBM ISS has operations throughout the Americas, Asia, Australia, Europe, and the Middle East.

B. IBM ISS Financial Profile

Table 20: IBM ISS Financial Profile

IBM ISS Financial Profile				
	2008	2007	2006	ISS 2008
Dollars in Millions				
Total Revenue	103,630,000	98,785	91,423	No information
Total Cost of Goods Sold (COGS)	57,969,000	57,057	53,129	No information
Gross Margin (profit)	45,661,000	41,728	38,294	No information
Sales, General, and Administrative Costs	23,386,000	22,060	20,259	No information
Research and Development	6,337,000	6153	6107	No information
Operating Income or Loss	**17,091,000**	**13,515**	**11,928**	**No information**
Number of Employees	410, 100	386,558	355,766	1250
ISS Network-Based IDS/IPS Market Share Position (based on calendar year revenue)	3	2	2	No information
ISS Network-Based IDS/IPS Market Share (based on calendar year revenue)	16%	16%	18%	No information

IDS/IPS: IBM ISS

C. IBM ISS Product Guide

Table 21: IBM ISS Products

IBM ISS Products							
Products	GX3002	GX4002	GX4004	GX5008	GX5108	GX5208	GX6116
Positioning	Remote office	Remote office	Network perimeter	Network perimeter	Network core	Network core	Network core
Cisco Equivalent	Cisco ASA 5510 with AIP10 or Cisco ISR with AIM-IPS	Cisco ASA 5510 with AIP20, Cisco ASA 5520 with AIP10, or Cisco IPS 4240 Sensor	Cisco ASA 5510 with AIP20, Cisco ASA 5520 with AIP10, or Cisco IPS 4240 Sensor	Cisco ASA 5520 with AIP20 or 40, Cisco ASA 5540 with AIP20, or Cisco IPS 4255 Sensor	Cisco 4260 Sensor	Cisco 4260 Sensor	Cisco 4270 Sensor
Performance Summary							
Maximum Aggregate Throughput/ Inspected Throughput	10 Mbps	200 Mbps	200 Mbps	400 Mbps	1.2 Gbps	2 Gbps	15/6 Gbps
Connections per Second	3750	21,000	21,000	35,000	40,000	60,000	160,000
Latency	< 1 ms	< 150 microsec	< 150 microsec	< 200 microsec	< 200 microsec	< 200 microsec	< 150 microsec
Logging	Yes, through IBM Proventia Management SiteProtector	Yes, through SiteProtector	Yes, through SiteProtector	Yes, through SiteProtector	Yes, through SiteProtector	Yes, through SiteProtector	Yes, through SiteProtector
Customer Capability to Create Custom Signatures	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrated SIEM	No	No	No	No	No	No	No
High Availability	Active-passive (A/P)	A/P	A/P	A/A and A/P	A/A and A/P	A/A and A/P	A/A and A/P
Sensor-to-Management-Server Transport Encryption	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL
Low-Cost Standalone Management and Logging Option	HTTPS	HTTPS	HTTPS	HTTPS	HTTPs	HTTPS	HTTPS
Integrated Management Platform for IPS, Firewall, SSL, and IPsec VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HIPS Integration and Linkage	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OS Fingerprinting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Import of Vulnerability Scanning Data	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Session Termination	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hardware Module Integration with Firewall and VPN Appliances	No	No	No	No	No	No	No
Protocol, Application, and Statistical Anomaly Detection	Yes, with Protocol Analysis Module (PAM)	Yes	Yes	Yes	Yes	Yes	Yes

IDS/IPS: IBM ISS

Table 21: IBM ISS Products

IBM ISS Products (continued)

Products	GX3002	GX4002	GX4004	GX5008	GX5108	GX5208	GX6116
Technical Summary							
Management Platform	IBM Proventia Management SiteProtector			IBM Proventia Management SiteProtector			
Monitoring and SPAN Ports	2 10/100 copper	2 10/100/1000 copper	4 10/100/1000 copper	8X 10/100/1000 copper, or 4X 10/100/1000 copper and 4X SFP and mini–Gigabit Interface Converter (mini-GBIC) ports (1000BASE- TX/SX/LX), or 8X SFP and mini-GBIC ports (1000 TX/SX/LX)	8X 10/100/1000 copper, or 4 10/100/1000 copper and 4 SFP and mini-GBIC ports (1000BASE- TX/SX/LX), or 8X SFP and mini-GBIC ports (1000BASE- TX/SX/LX)	8X 10/100/1000 copper, or 8X SFP and mini-GBIC ports (1000BASE- TX/SX/LX)	16X SFP and mini-GBIC ports (1000BASE-TX/SX/LX)
Management Interfaces	1 10/100 copper and 1 serial	2 10/100/1000 copper and 1 serial	2 10/100/1000 copper and 1 serial	2X 10/100/1000 copper and 1X serial	2X 10/100/1000 copper and 1X serial	2X 10/100/1000 copper and 1X serial	2X 10/100/1000 copper and 1X serial
Total Number of Segments	1	1	2	4	4	4	8
Virtual Sensor Support	Yes, through "protection domains"			Yes, through "protection domains"			
Size	Desk	1RU	1RU	2RU	2RU	2RU	2RU
Bypass Features	Integrated	Integrated	External	External	External	External	External
Redundant Power Supplies	No	No	No	Yes	Yes	Yes	Yes
Common Criteria Certification	Yes	Yes	Yes	Yes	Yes	Yes	Yes

D. IBM ISS Sales Tactics

- IBM ISS generally attempts to position its products as best-in-class intrusion detection/intrusion prevention (IDS/IPS) appliances.
- IBM ISS may attempt to use its IBM Global Services consulting and managed services relationships to gain entry to customers' IDS/IPS opportunities.
- IBM ISS generally positions its X-Force research and development team as a primary advantage and competitive differentiator.
- IBM ISS will use its IBM Proventia Virtualized Network Security Platform to help differentiate its offerings in the Service Provider and Managed Security Services Provider (MSSP) markets.
- IBM ISS will also use its newly announced Proventia Web Application Security, which protects against Web 2.0 related threats.

E. IBM ISS Weaknesses

- IBM ISS generally has had to use an OEM vendor's hardware platform for its appliance product offerings. The GX series is ISS hardware and software. This approach may lead to confusion or delayed response for a customer needing technical assistance center (TAC) support.
- IBM ISS may not release updates fast enough to keep up with the latest vulnerabilities. This could weaken the point it makes about its X-Force being able to provide content updates well before threats occur.
- Primarily, the two new product introductions by IBM ISS since 2007 are the Virtual Proventia (a GX running on VMware) and the Web Application Firewall GX edition.
- The ISS Security group typically tries to sell the product with bundled services. This approach may work in some environments, but not in all.
- The IBM ISS M Series unified threat management (UTM) appliances generally has had weak market acceptance. Generally, most of those appliances' UTM services and functions, except those involving IDS/IPS, are OEM components obtained from third-party vendors.

NOTES

IDS/IPS: Juniper Networks

III. Juniper Networks

A. Juniper Overview

For full Juniper overview see page 40.

B. Juniper Financial Profile

For full Juniper financial data see page 41.

Table 22: Juniper Financial Profile

Juniper Financial Profile			
	2008	2007	2006
Dollars in Millions			
Juniper Network-Based IDS/IPS Market Share Position (based on calendar year revenue)	6	5	5

IDS/IPS: Juniper Networks

C. Juniper Product Guide

Table 23: Juniper Products

Juniper Products

Products	IDP 75	IDP 250	IDP 800	IDP 8200	ISG 1000 with IDP	ISG 2000 with IDP
Positioning	Small office and home office (SOHO) and remote office and branch office (ROBO)	Small and medium-sized business (SMB)	Midmarket	Enterprise	Enterprise	Enterprise
Cisco Equivalent	Cisco ASA 5510 with AIP10 or Cisco ASA 5520 with AIP10	Cisco ASA 5510 with AIP20, Cisco ASA 5520 with AIP20, or Cisco IPS 4240 or 4255 Sensors	Cisco IPS 4260 Sensor	Cisco IPS 4270 Sensor	Cisco ASA 5540 with AIP40 or Cisco IPS 4260 Sensor	Cisco ASA 5540 with AIP40 or Cisco IPS 4270 Sensor
Performance Summary						
Maximum Aggregate Throughput	150 Mbps	300 Mbps	1 Gbps	10 Gbps	1 Gbps	2 Gbps
Maximum Number of Concurrent Sessions	100,000	300,000	1,000,000	5,000,000	500,000	1,000,000
Logging	Using Network and Security Manager (NSM) with Statistical Report Server module option		Using Network and Security Manager (NSM) with Statistical Report Server module option			
Customer Capability to Create Custom Signatures	Yes	Yes	Yes	Yes	Yes	Yes
Integrated SIEM	Yes, through Security Threat Response Manager (SRTM) – OEM from Q1 Labs		Yes, through Security Threat Response Manager (SRTM) – OEM from Q1 Labs			
High Availability	Through clustering only	Through clustering only	Through clustering only	Through clustering only	A/A, A/P, and full-mesh	A/A, A/P, and full-mesh
Connections per Second	No information	No information	No information	No information	20,000	23,000
Sensor-to-Management-Server Transport Encryption	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL
Low-Cost Standalone Management and Logging Option	Yes	Yes	Yes	Yes	Yes	Yes
Integrated Management Platform for IPS, Firewall, SSL, and IPsec VPN	IPS, firewall, and VPN (no SSL VPN)		IPS, firewall, and VPN (no SSL VPN)			
HIPS Integration and Linkage	No	No	No	No	No	No
OS Fingerprinting	No	No	No	No	No	No
Import of Vulnerability Scanning Data	No information	No information	No information	No information	No information	No information
Session Termination	Yes	Yes	Yes	Yes	Yes	Yes
Hardware Module Integration with Firewall and VPN Appliances	No	No	No	No	Yes	Yes
Protocol, Application, and Statistical Anomaly Detection	Yes	Yes	Yes	Yes	Yes	Yes

IDS/IPS: Juniper Networks

Table 23: Juniper Products

Juniper Products (continued)						
Products	IDP 75	IDP 250	IDP 800	IDP 8200	ISG 1000 with IDP	ISG 2000 with IDP
Technical Summary						
Management Platform	NSM, web user interface, and command-line interface (CLI)		NSM, web user interface, and command-line interface (CLI)			
Monitoring and SPAN Ports	2X fixed RJ-45 Ethernet 10/100/1000 with bypass	8X fixed RJ-45 Ethernet 10/100/1000 with bypass	2X fixed RJ-45 Ethernet 10/100/1000 with bypass, and 2X modular I/O slots, with choice of only 2 of the following: 4-port Gigabit Ethernet copper with bypass, and/or 4-port Gigabit Ethernet fiber SFP, and/or 4-port Gigabit Ethernet SX-bypass	4X modular I/O slots: 4-port Gigabit Ethernet copper with bypass, 4-port Gigabit Ethernet fiber SFP, 4-port Gigabit Ethernet SX-bypass, and 2-port 10 Gigabit Ethernet SR-bypass	4X fixed 10/100/1000 ports and 2X expansion slots	4X expansion slots
Management Interfaces	1X RJ-45 Ethernet 10/100/1000	1X RJ-45 Ethernet 10/100/1000	1X RJ-45 Ethernet 10/100/1000	1X RJ-45 Ethernet 10/100/1000	Yes, serial	Yes, serial
Number of Segments	1	4	5	4	3	2
Virtual Sensor Support	No	No	No	No	No	No
Size	1RU	1RU	2RU	2RU	3RU	3RU
Bypass Features	Hardware and software	Hardware and software	Hardware and software	Hardware and software	Hardware and software	Hardware and software
Redundant Power Supplies	No	No	Yes	Yes	No	Yes
Common Criteria Certification	Yes	Yes	Yes	Yes	Yes	Yes

D. Juniper Sales Tactics

- Juniper may attempt to use its installed base of firewalls and VPN products to insert its IDP line of intrusion prevention (IPS) products into customer network security deployments.
- Juniper may attempt to position the IDP line as having tight integration with other Juniper products, although almost none exists between it and the Junos-based products and the Secure Access products.
- Juniper may attempt to position its ISG products with IDP hardware modules as a secondary positioning tactic when its products (for example, when its SSG products, which can offer only Juniper's more truncated form of IPS, deep packet inspection) fail to meet customer IPS expectations.

E. Juniper Weaknesses

- Although Juniper IDP has some integration with its ScreenOS line of products, it has almost none with other Juniper products, including the Junos-based products and the new Secure Access line of products.
- Juniper has had a significant drop in revenue over the last six quarters.
- The Juniper IDP line has no host intrusion prevention system (HIPS) integration or linkage.
- Juniper IDP has no passive OS fingerprinting capabilities.
- Juniper does not support virtual instantiations of IPS, only for IEEE 802.1Q VLAN virtualization.
- Juniper does not support risk ratings or meta-events that would allow a user to create more comprehensive security policies.

IDS/IPS: McAfee

IV. McAfee

A. McAfee Overview

McAfee, Inc. offers security technology to protect systems and networks from known and unknown threats worldwide. The company's system security offerings include endpoint protection for consumer and corporate computer systems; data protection solutions to safeguard vital information residing on various devices; and mobile security solutions to protect mobile operators and their users by safeguarding mobile terminals, applications, and content. Its network security offerings comprise firewall, intrusion detection and prevention, web, email, and data-loss-protection security appliances. McAfee SiteAdvisor protects Internet users from a range of security threats, including spyware and other malicious downloads, spam, and identity theft scams, and it provides customers a search tool bar that eliminates red-rated sites on search engine results. McAfee SECURE standard, an aggregate of industry best practices, provides a level of security that an online merchant would reasonably expect to achieve to protect consumers as they interact with websites and shop online.

McAfee's vulnerability and risk management offerings enable companies to meet security compliance objectives across an entire organization, including identification of security risks, enforcement of security policies, and compliance audits for industry and government security regulations. The company's McAfee NAC solution supports internal security policies by preventing noncompliant personal computers from connecting to the internal network. It has strategic-alliance agreements with HP ProCurve to develop and deliver network security solutions; NTT DoCoMo; Extreme Networks Inc.; BMC Software Inc.; and Verizon Business. The company was formerly known as Network Associates, Inc. and changed its name to McAfee, Inc. in 2004. McAfee was founded in 1989 and is headquartered in Santa Clara, California.

B. McAfee Financial Profile

Table 24: McAfee Financial Profile

McAfee Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	1,600,065	1,308.22	1,145.16
Total Cost of Goods Sold (COGS)	383,528	305.74	246.84
Gross Margin (profit)	1,216,537	1,002.48	898.32
Sales, General, and Administrative Costs	730,728	569.38	536.15
Research and Development	252,020	217.93	193.45
Operating Income or Loss	**189,571**	**159.81**	**139.03**
Number of Employees	5600	4250	3700
McAfee Network-Based IDS/IPS Market Share Position (based on calendar year revenue)	2	3	4
McAfee Network-Based IDS/IPS Market Share (based on calendar year revenue)	20%	16%	16%

IDS/IPS: McAfee

C. McAfee Product Guide

Table 25: McAfee Products

McAfee Products							
Products	M-1250	M-1450	M-2750	M-3050	M-4050	M-6050	M-8000
Positioning	Branch office	Branch office and perimeter	Perimeter	Core	Core	Core	Core
Cisco Equivalent	Cisco ASA 5510 with AIP10	Cisco ASA 5510 with AIP20, Cisco ASA 5520 with AIP10, or Cisco IPS 4240 Sensor	Cisco ASA 5540 with AIP40 or Cisco IPS 4255 Sensor	Cisco 4260 Sensor	Cisco 4260 Sensor	Cisco 4270 Sensor	Cisco 4270 Sensor
Performance Summary							
Maximum Aggregate Throughput	100 Mbps	200 Mbps	600 Mbps	1.5 Gbps	3 Gbps	5 Gbps	10 Gbps
Maximum Number of Concurrent Sessions	40,000	80,000	250,000	750,000	1,500,000	2,000,000	4,000,000
Logging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Customer Capability to Create Custom Signatures	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrated SIEM	No	No	No	No	No	No	No
High Availability	Yes (stateful failover)	Yes (stateful failover)	Yes (stateful failover)	Yes (stateful failover)	Yes (stateful failover)	Yes (stateful failover)	Yes (stateful failover)
Connections per Second	No information	No information	No information	No information	No information	No information	No information
Sensor-to-Management-Server Transport Encryption	SSH	SSH	SSH	SSH	SSH	SSH	SSH
Low-Cost Standalone Management and Logging Option	No	No	No	No	No	No	No
Integrated Management Platform for IPS, Firewall, SSL and IPsec VPN	IPS	No information	SSL	SSL	SSL	SSL	SSL
HIPS Integration and Linkage	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OS Fingerprinting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Import of Vulnerability Scanning Data	Foundstone, Qualys, and Nessus			Foundstone, Qualys, and Nessus			
Session Termination	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hardware Module Integration with Firewall and VPN appliances	No	No	No	No	No	No	No
Protocol, Application, and Statistical Anomaly Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes

IDS/IPS: McAfee

Table 25: McAfee Products

McAfee Products (continued)							
Products	M-1250	M-1450	M-2750	M-3050	M-4050	M-6050	M-8000
Technical Summary							
Management Platform	McAfee Network Security Manager (formerly IntruShield Security Manager)			McAfee Network Security Manager (formerly IntruShield Security Manager)			
Monitoring and SPAN Ports	8X 10/100/1000	8X 10/100/1000	20X 10/100/1000	4X 10/100/1000 and 8X 10 Gigabit Ethernet	4X 10/100/1000 and 8X 10 Gigabit Ethernet	8X 10/100/1000 and 8X 10 Gigabit Ethernet	16X 10/100/1000 and 12X 10 Gigabit Ethernet
Management Interfaces	1X 10/100	1X 10/100	1X 10/100	1X 10/100	1X 10/100	1X 10/100	1X 10/100
Number of Segments	1	2	4	7	3	8	14
Virtual Sensor Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Size	1U	1U	2U	2U	2U	2U	2 x 2U
Bypass Features	Software or hardware	Software or hardware	Software or hardware	Software or hardware	Software or hardware	Software or hardware	Software or hardware
Redundant Power Supplies	No	No	Optional	Optional	Optional	Optional	Optional
Common Criteria Certification	No	No	No	No	No	No	No

D. McAfee Sales Tactics

- McAfee generally promotes its market and brand leadership in sales and antivirus software to the commercial market and positions itself as a market leader in the sale of security products, especially endpoint protection products.
- McAfee generally promotes its vulnerability and compliance product integration marketing message.
- McAfee generally promotes its R&D group, McAfee Labs, and its overall reputation in the antivirus industry.
- McAfee generally attempts to take full advantage of its ePolicy Orchestrator (ePO) installed base, which has a strong, loyal following among desktop and server antivirus administrators.
- McAfee generally attempts to position intruShield products as its high-performance IDS/IPS.

E. McAfee Weaknesses

- McAfee has little integration of its NAC solution (Policy Enforcer) with IntruShield.
- Compared to other IDS/IPS competitors' product offerings, IntruShield products have generally higher list prices.
- McAfee generally has a limited direct salesforce for its IntruShield product line.
- McAfee's Intrushield product line provides only a small percentage of McAfee's overall product and license revenue.

IDS/IPS: Sourcefire

V. Sourcefire

A. Sourcefire Overview

Sourcefire, Inc. provides intelligent cyber security solutions for IT; commercial enterprises, such as healthcare, financial services, manufacturing, energy, education, retail, and telecommunications; and federal, state, and international government organizations. The Sourcefire 3D System comprises multiple Sourcefire hardware and software products that provide a layered approach to network defense, protecting assets before, during, and after an attack. The company also offers Snort, an open source intrusion prevention technology that is incorporated into the intrusion prevention system (IPS) software component of the Sourcefire 3D System; and ClamAV, an open source antivirus and anti-malware project. In addition, it offers various services to aid customers with installing and supporting cyber security solutions, including customer support, education, professional services, the Sourcefire vulnerability research team, and Snort rule subscriptions. The company was founded in 2001 and is headquartered in Columbia, Maryland.

B. Sourcefire Financial Profile

Table 26: Sourcefire Financial Profile

Sourcefire Financial Profile

	2008	2007	2006
Dollars in Millions			
Total Revenue	75,673	55.86	44.93
Total Cost of Goods Sold (COGS)	17,360	12.88	11.07
Gross Margin (profit)	58,313	42.98	33.85
Sales, General, and Administrative Costs	51,882	36.46	25.67
Research and Development	12,620	11.9	8.61
Operating Income or Loss	**-8816**	**-9981**	**-1657**
Number of Employees	295	240	182
Sourcefire Network-Based IDS/IPS Market Share Position (based on calendar year revenue)	5%	6%	6%
Sourcefire Network-Based IDS/IPS Market Share (based on calendar year revenue)	7%	6%	10%

IDS/IPS: Sourcefire

C. Sourcefire Product Guide

Sourcefire Products

Products	3D500	3D1000	3D2000	3D2100	3D2500	3D3500	3D4500	3D6500	3D9900
Positioning	SOHO and ROBO	SOHO and ROBO	SOHO and ROBO	SMB	Midmarket	Midmarket	Enterprise	Enterprise	Enterprise
Cisco Equivalent	Cisco ASA 5510 with AIP10 or Cisco ISR with AIM-IPS	Cisco ASA 5510 with AIP10 or Cisco ISR with AIM-IPS	Cisco ASA 5510 with AIP10	Cisco ASA 5510 with AIP20, Cisco ASA 5520 with AIP10, or Cisco IPS 4240 Sensor	Cisco ASA 5520 with AIP40, Cisco ASA 5540 with AIP20 or 40, or Cisco IPS 4255 Sensor	Cisco 4260 Sensor	Cisco 4260 Sensor	Cisco 4270 Sensor	Cisco 4270 Sensor
Performance Summary									
Maximum Aggregate Throughput	5 Mbps	45 Mbps	100 Mbps	250 Mbps	500 Mbps	1 Gbps	1.5 Gbps	4 Gbps	10 Gbps
Maximum Number of Concurrent Sessions	No information	No information	No information	No information	No information	No information	No information	No information	No information
Typical Latency	< 1 ms	< 1 ms	< 1 ms	< 1 ms	< 1 ms	< 1 ms	< 1 ms	250 microsec	150 microsec
Logging	Yes, through Defense Center	Yes, through Defense Center	Yes, through Defense Center	Yes, through Defense Center	Yes, through Defense Center	Yes, through Defense Center	Yes, through Defense Center	Yes, through Defense Center	Yes, through Defense Center
Customer Capability to Create Custom Signatures	No	No	No	No	No	No	No	No	No
Integrated SIEM	Available through their Sourcefire Defense Center				Available through their Sourcefire Defense Center				
High Availability	Yes, with clustering	Yes, with clustering	Yes, with clustering	Yes, with clustering	Yes, with clustering	Yes, with clustering	Yes, with clustering	Yes, with clustering	Yes, with clustering
Connections per Second	No information	No information	No information	No information	No information	No information	No information	No information	No information
Sensor-to-Management-Server Transport Encryption	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL	SSH and SSL
Low-Cost Standalone Management and Logging Option	No	No	No	No	No	No	No	No	No
Integrated Management Platform for IPS, Firewall, SSL and IPsec VPN	No	No	No	No	No	No	No	No	No
HIPS Integration and Linkage	Yes, with Snort	Yes, with Snort	Yes, with Snort	Yes, with Snort	Yes, with Snort	Yes, with Snort	Yes, with Snort	Yes, with Snort	Yes, with Snort
OS Fingerprinting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Import of Vulnerability Scanning Data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Session Termination	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hardware Module Integration with Firewall and VPN Appliances	No	No	No	No	No	No	No	No	No
Protocol, Application, and Statistical Anomaly Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

IDS/IPS: Sourcefire

Table 27: Sourcefire Products

Sourcefire Products

Products	3D500	3D1000	3D2000	3D2100	3D2500	3D3500	3D4500	3D6500	3D9900
Technical Summary									
Management Platform	Sourcefire Defense Center				Sourcefire Defense Center				
Monitoring and SPAN Ports	4X RJ-45 10/100/1000 copper	4X RJ-45 10/100/1000 copper	4X RJ-45 10/100/1000 copper	4X RJ-45 10/100/1000 copper	8X RJ-45 10/100/1000 copper or 4X RJ-45 10/100/1000 copper and 4X LC 100/1000 fiber	8X RJ-45 10/100/1000 copper with bypass, or 4 copper and 4 LC 100/1000 fiber	8X RJ-45 10/100/1000 copper with bypass, or 4X copper and X LC 100/1000 Fiber	12X RJ-45 10/100/1000 copper with bypass, or 4X 10 Gbps SR, or 4X 10 Gbps LR, or 6X 1 Gbps copper and 2X 10 Gbps SR, or 6X 1 Gbps copper and 2X 10 Gbps LR, or 6X 1 Gbps copper and 4X 1 Gbps fiber	12X RJ-45 10/100/1000 copper with bypass, or 4X 10 Gbps SR
Management Interfaces	1 RJ45 10/100/1000 copper	1X RJ-45 10/100/1000 copper	1X RJ-45 10/100/1000 copper	2X RJ-45 10/100/1000 copper	2X RJ-45 10/100/1000 copper	2X RJ-45 10/100/1000 copper	2X RJ-45 10/100/1000 copper	1X RJ-45 10/100/1000 copper	1X RJ-45 10/100/1000 copper
Number of Segments	2	2	2	2	4	4	4	4	4
Virtual Sensor Support	No	No	No	No	No	No	No	No	No
Size	1RU	1RU	1RU	1RU	1RU	1RU	1RU	2RU	2RU
Bypass Features	No information	No information	No information	No information	Yes, hardware	Yes, hardware	Yes, hardware	Yes, hardware	Yes, hardware
Redundant Power Supplies	No	No	No	No	No information	Yes	Yes	Yes	Yes
Common Criteria Certification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

D. Sourcefire Sales Tactics

- Sourcefire generally attempts to promote the market popularity of open-source Snort and its primary creator, Martin Roesch, for overall IDS market recognition, leadership, and respect.
- Sourcefire may also promote its open-source antivirus acquisition, ClamAV, to gain more credibility in the open-source market.
- Sourcefire generally attempts to promote its OEM partner relationships with hardware platform vendor Crossbeam
- Sourcefire generally positions its integrated RNA branded vulnerability scanning and analysis solution as a primary competitive differentiator.
- Sourcefire generally promotes itself as having focused on a single technology product line, IDS/IPS, and often claims to be a best-in-class IDS/IPS vendor.
- Sourcefire has many high-level U.S federal government customers and may attempt to promote this fact to expand its market presence.
- Sourcefire generally promotes its IPv6 support in its products and the fact that its IDS has obtained Common Criteria EAL-2 certification.

E. Sourcefire Weaknesses

- Sourcefire generally has a single product line with its 3D line of intrusion detection/intrusion prevention (IDS/IPS) products.
- Sourcefire products generally offer few endpoint protection capabilities (beyond Nessus and nMap vulnerability scanning and Snort IDS agent support).
- Sourcefire does not offer a real NAC capability (beyond postadmission scans and quarantines).
- Sourcefire's management platform, Defense Center, is really a standalone management application that manages only Sourcefire's own IDS/IPS and VA products.
- Sourcefire generally relies on OEMs for its appliance hardware platforms.
- Sourcefire's OEM relationship with Crossbeam may be threatened by that vendor's longstanding relationship with Check Point.
- IBM is one of Sourcefire's largest channels, and there could potentially be conflict between IBM's own newly acquired IDS/IPS product line and Sourcefire's, which might hamper Sourcefire's ability to sell through IBM.

NOTES

NAC

Companies	Sections in Each Company Guide
I. Bradford Networks	A. Company Overview
II. Juniper Networks	B. Financial Profile
III. McAfee	C. Product Guide
IV. Symantec	D. Sales Tactics
	E. Weaknesses

NAC: Bradford Networks

I. Bradford Networks

A. Bradford Company Profile

Bradford Networks, founded in 1999, provides customized engineering development services for telecomm equipment manufacturers. Bradford is headquartered in Concord, New Hampshire. Bradford is a privately held company with investment from Windspeed Ventures, whose funds focus on early-stage investments.

Bradford has changed technological focus over the years. In early 2001, Bradford developed a solution to enhance control of network devices. By late 2001, Bradford had a prototype of the product, Campus Manager, a port-based tool to monitor and control network clients and devices. In 2002, Bradford transitioned into a product-focused company, developing, marketing, and selling Campus Manager to educational institutions in the United States and Europe. In January 2007, Bradford introduced NAC Director, a NAC appliance designed for enterprise markets, including healthcare, finance, and government sectors. In April 2008, at the RSA Conference, Bradford introduced its new NAC Director Guest/Contractor Services (GCS) solution for self-service and sponsored guest services.

Bradford has developed reseller networks in both North America and Europe. The company has created a three-tiered channel partner program that includes solution partners who provide sales, deployment, and support; deployment partners who provide installation and integration services; and advisor partners who provide customer referrals.

B. Bradford Financial Profile

Bradford is a privately held company with funding from Windspeed Ventures.

C. Bradford Product Guide

Table 28: Bradford Products

Bradford Products	
Products	Sentry Family NS500, NS1200/8200, NS2200R/NS9200R
Cisco Equivalent	Cisco NAC 3350 Appliance
Identification and Authentication	
Single Sign-On (SSO)	No
IEEE 802.1x Support	Yes
Identification and Authentication of Wireless Devices	Yes
Captive Web Portal Logon	Yes
Authentication by User Name and Organizational Role	Yes
Authentication by Device MAC Address	Yes
Authentication by Device IP Address	Yes
Kerberos Support	Yes
Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), and RADIUS Support	Yes
Posture Assessment	
Agentless and Installed Client	Yes
Client Operating Systems	Mac OS X, Microsoft Windows, and Linux
Browsers	No Information
Pre- and Post-Admission Device Scanning	Yes; endpoint and network based
Registry Entry Scanning	Microsoft Windows only
Detection of Unauthorized Applications	Yes

NAC: Bradford Networks

Table 28: Bradford Products

Bradford Products (continued)	
Products	Sentry Family NS500, NS1200/8200, NS2200R/NS9200R
Posture Assessment (continued)	
Detection of Unauthorized Processes, Services, and Open Ports	Yes
Assessment of Managed and Unmanaged Devices	Yes
Auto-Assessment of Other IP-Based Computing Devices (printers, IP phones, medical equipment, etc.)	No
Other Endpoint Security Software Supported	Yes: Symantec, McAfee, and Trend
Assessment and Policy Enforcement of Guest Users (unmanaged)	Yes, with Dissolvable Agent
Access Control Authorization and Enforcement	
VLAN Network Access Control	Yes
Network Access Control by Subnet	Yes
Layer 3 Device Network Admission Control	Yes
Layer 2 LAN Switch Network Admission Control	Yes
WLAN Access Point Network Admission Control	Yes
Firewall Network Admission Control	No
SSL VPN Gateway Admission Control	Yes
NAC hardware Module for Routers	No
Inline NAC	No
Host and Endpoint Admission Control	Yes
Quarantine and Remediation Services	
Quarantine by VLAN	Yes
Quarantine by Subnet	Yes
Fully Automated Remediation Support	Yes

Table 28: Bradford Products

Bradford Products (continued)	
Products	Sentry Family NS500, NS1200/8200, NS2200R/NS9200R
Quarantine and Remediation Services (continued)	
Directed URL for Updates and Patches	Yes
Built-in Native Host Intrusion Prevention	No
Integration with Security Information and Event Management (SIEM)	No
Management Platform	Bradford Network Security Manager appliance
Technical Summary	
Maximum Number of Concurrent Users	12,000
CPU	2X dual-core Intel Xeon 5150
Hard Drive and Storage Controller	4X 160-GB enterprise SATA drives and RAID-10
High Availability	A/S
Size (chassis height)	1 rack unit (1RU)
Network I/O Ports	GX-A: 2X 10/100/1000; LX-C: 3X 10/100/1000
Redundant Power Supplies	Yes

NAC: Bradford Networks

D. Bradford Sales Tactics

- Bradford positions itself as a low-cost network admission control (NAC) provider. The company typically uses pricing to close the customer deal.
- Bradford targets the higher education market. The company recently started expanding into several other vertical markets.
- Bradford positions its partnerships and integration with Aruba Networks and Packeteer (Blue Coat).

E. Bradford Weaknesses

- The Bradford remediation process potentially requires a lot of manual operations to bring a PC up to standards, which can lead to low efficiency.
- Bradford provides some basic NAC functions but lacks certain essential and important capabilities:
  - No single sign-on (SSO) support
  - Support only for out-of-band (OOB) deployments
  - Only manual remediation offered, and support for anti-spam and antivirus vendors is minimal
  - No Network Address Translation (NAT) support; everything behind a NAT gateway is allowed
  - Limited high-availability support (only a subset of VPN gateways is supported)

NOTES

NAC: Juniper Networks

II. Juniper Networks

A. Juniper Company Profile

For full Juniper company overview see page 40.

B. Juniper Financial Profile

For full Juniper financial data see page 41.

C. Juniper Product Guide

Table 30: Juniper Products

Juniper Products

Products	Juniper Networks Infranet Controller 4500 and Unified Access Control (UAC) Agent	Juniper Networks Infranet Controller 6500 and UAC Agent
Cisco Equivalent	Cisco NAC 3310 Appliance	Cisco NAC 3350 Appliance
Identification and Authentication		
Single Sign-On (SSO)	Yes	Yes
IEEE 802.1x Support	Yes	Yes
Identification and Authentication of Wireless Devices	Yes	Yes
Captive Web Portal Logon	Yes	Yes
Authentication by User Name and Organizational Role	Yes	Yes
Authentication by Device MAC Address	Yes	Yes
Authentication by Device IP Address	Yes	Yes
Kerberos Support	Yes	Yes
Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), and RADIUS Support	Yes	Yes
Posture Assessment		
Agentless and Installed Client	Yes	Yes
Client Operating Systems	Microsoft Windows, Mac OS X, Linux, and Solaris	Microsoft Windows, Mac OS X, Linux, and Solaris
Browsers	Internet Explorer and Firefox	Internet Explorer and Firefox
Pre- and Post-Admission Device Scanning	Yes	Yes

Table 30: Juniper Products

Juniper Products (continued)

Products	Juniper Networks Infranet Controller 4500 and Unified Access Control (UAC) Agent	Juniper Networks Infranet Controller 6500 and UAC Agent
Posture Assessment (continued)		
Registry Entry Scanning	Yes	Yes
Detection of Unauthorized Applications	No	No
Detection of Unauthorized Processes, Services, and Open Ports	Yes	Yes
Assessment of Managed and Unmanaged Devices	Yes	Yes
Auto-Assessment of Other IP-Based Computing Devices (printers, IP phones, medical equipment, etc.)	Yes	Yes
Other Endpoint Security Software Supported	Personal firewall, antivirus, and malicious-code protection	
Assessment and Policy Enforcement of Guest Users (unmanaged)	Yes	Yes
Access Control Authorization and Enforcement		
VLAN Network Access Control	Yes	Yes
Network Access Control by Subnet	Yes	Yes
Layer 3 Device Network Admission Control	Yes	Yes
Layer 2 LAN Switch Network Admission Control	Yes	Yes
WLAN Access Point Network Admission Control	Yes	Yes
Firewall Network Admission Control	Yes, Juniper firewall	Yes, Juniper firewall
SSL VPN Gateway Admission Control	No	No
NAC Hardware Module for Routers	No	No
Inline NAC	Yes	Yes
Host and Endpoint Admission Control	Yes	Yes

NAC: Juniper Networks

Table 30: Juniper Products

Juniper Products (continued)		
Products	Juniper Networks Infranet Controller 4500 and Unified Access Control (UAC) Agent	Juniper Networks Infranet Controller 6500 and UAC Agent
Quarantine and Remediation Services		
Quarantine by VLAN	Yes	Yes
Quarantine by Subnet	Yes	Yes
Fully Automated Remediation Support	Yes	Yes
Directed URL for Updates and Patches	Yes	Yes
Built-in Native Host Intrusion Prevention	No	No
Integration with SIEM	Yes	Yes
Management Platform	Infranet Controller Access Management System	
Technical Summary		
Maximum Number of Concurrent Users	5000	15,000 or 30,000
CPU	No information	No information
Hard Drive and Storage Controller	Yes, hard drive	Mirrored RAID hard drive (optional)
High Availability	Cluster pairs	Multiunit clustering, hot-swappable redundant power supplies, cooling fans, and mirrored RAID hard disks
Size (chassis height)	1RU	2RU
Network I/O Ports	2X RJ-45 10/100/1000	4X RJ-45 10/100/1000
Redundant Power Supplies	No	Redundant hot-swappable power supplies

D. Juniper Sales Tactics

- Juniper emphasizes its integration story: its Infranet Controller as the policy management server, its firewall and VPN appliances and EX-series switches as the enforcement points, and its acquisition of Funk Software's Radius and IEEE 802.1x products.
- Juniper often attempts to portray its solution as an open, standards-based approach, even though Juniper itself uses proprietary implementations.
- Juniper sometimes claims more than it can deliver. For instance, Juniper claims that its Unified Access Control (UAC) solution can provide granular application access control. What it actually provides is IP address–based network access control, not application-level access control.
- Juniper markets its support for Microsoft Network Access Protection (NAP) through Trusted Network Connect (TNC) extensions.
- Juniper markets its UAC 3.0 FIPS 140-2 certification.

E. Juniper Weaknesses

- Juniper's license is restrictive. If a user logs in at two different connections, that counts as two seats instead of one.
- Juniper supports only limited use cases. It does not support routers as an enforcement device. Similarly, it needs an inline firewall for wireless coverage. Juniper's non–IEEE 802.1x implementation is supported only by its own inline firewalls.
- If the enforcement point needs to be close to the client side, many firewalls must be deployed inline.
- Juniper does not have full network admission control (NAC) lifecycle support. For instance, Juniper does not provide out-of-the-box capabilities to manage nonauthenticating devices (IP phones, printers, etc.). Its autoremediation capability is limited to basic functions.
- Host assessment with UAC's Java-based agent (Mac OS, Linux, or Solaris) is very limited.
- User requirements for remediation and posture compliance are totally manual and poorly documented.

NAC: McAfee

III. McAfee

A. McAfee Company Profile

For full McAfee company profile see page 94.

B. McAfee Financial Profile

For full McAfee financial profile see page 95.

C. McAfee Product Guide

Table 31: McAfee Products

McAfee Products	
Products	McAfee NAC Unified Secure Access (N-450)
Cisco Equivalent	Cisco NAC 3350 Appliance
Identification and Authentication	
Single Sign-On (SSO)	No
IEEE 802.1x Support	No
Identification and Authentication of Wireless Devices	Yes
Captive Web Portal Logon	No
Authentication by User Name and Organizational Role	No
Authentication by Device MAC Address	Yes
Authentication by Device IP Address	Yes
Kerberos Support	No
Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), and RADIUS Support	Yes
Posture Assessment	
Agentless and Installed Client	Yes, Microsoft Windows only
Client Operating Systems	Microsoft Windows only
Browsers	Internet Explorer and Firefox
Pre- and Post-Admission Device Scanning	Yes
Registry Entry Scanning	No specific registry keys or files

Table 31: McAfee Products

McAfee Products (continued)	
Products	McAfee NAC Unified Secure Access (N-450)
Posture Assessment (continued)	
Detection of Unauthorized Applications	Yes
Detection of Unauthorized Processes, Services, and Open Ports	Microsoft Windows only; cannot detect processes
Assessment of Managed and Unmanaged Devices	Yes
Auto-Assessment of Other IP-Based Computing Devices (printers, IP phones, medical equipment, etc.)	No
Other Endpoint Security Software Supported	Personal firewall, antivirus, and malicious-code protection
Assessment and Policy Enforcement of Guest Users (unmanaged)	Yes
Access Control Authorization and Enforcement	
VLAN Network Access Control	Yes
Network Access Control by Subnet	No
Layer 3 Device Network Admission Control	Yes
Layer 2 LAN Switch Network Admission Control	Yes
WLAN Access Point Network Admission Control	Yes
Firewall Network Admission Control	No
SSL VPN Gateway Admission Control	Yes
NAC Hardware Module for Routers	No
Inline NAC	Yes
Host and Endpoint Admission Control	Yes
Quarantine and Remediation Services	
Quarantine by VLAN	Yes
Quarantine by Subnet	Yes
Fully Automated Remediation Support	Yes
Directed URL for Updates and Patches	Yes
Built-in Native Host Intrusion Prevention	Yes
Integration with SIEM	Yes, through third-party product
Management Platform	McAfee ePolicy Orchestrator (ePO)

NAC: McAfee

Table 31: McAfee Products

McAfee Products (continued)	
Products	McAfee NAC Unified Secure Access (N-450)
Technical Summary	
Maximum Number of Concurrent Users	5000 concurrent
CPU	Intel Pentium compatible; 450 MHz or higher
Hard Drive and Storage Controller	No information
High Availability	Yes
Size (chassis height)	2RU
Network I/O Ports	10 inline segments
Redundant Power Supplies	No information
Throughput	2 Gbps

D. McAfee Sales Tactics

- McAfee typically sells its network admission control (NAC) solution by approaching a customer who already uses a McAfee antivirus product or McAfee ePolicy Orchestrator (ePO).
- McAfee emphasizes the ease of deployment of its NAC product.
- McAfee attempts to divert the conversation toward the number of agents on the desktop and how McAfee can achieve the same results with just a single agent. The reality is that customers deploy NAC because they cannot rely on the endpoint and its agent to police itself. The intelligence and enforcement needs to reside on the network.

E. McAfee Weaknesses

- McAfee's NAC function is an extension of its ePO endpoint security suite. NAC policy enforcement options are limited to either the endpoint agent itself or selected switches. No Layer 3, wireless, or VPN support is provided.
- McAfee does not offer authentication or user identity support, IEEE 802.1x support, or Microsoft Active Directory integration.
- McAfee does not support guest users or unmanaged assets.

NOTES

NAC

NAC: Symantec

IV. Symantec

A. Symantec Company Profile

Symantec was founded in 1982 and is headquartered in Cupertino, California, with its main manufacturing facility in Dublin, Ireland. Symantec acquired the Norton product line in 1990 from Peter Norton Computing, Inc. In July 2005, Symantec completed its merger with VERITAS Software, one of the 10 largest software companies in the world. Symantec also has acquired a number of companies in recent years, including Sygate in August 2005 for its access control technology, WholeSecurity in September 2005 for its zero-day attack technology, IMlogic in January 2006, and Altaris in January 2007 for its IT management software.

Symantec's generally accepted accounting principles (GAAP) revenue for FY07 (period ending March 31, 2007) was US$5.19 billion. Symantec employs approximately 17,100 people. Symantec maintains five operating segments: Enterprise Security, Enterprise Administration, Consumer Products, Services, and Other. The Enterprise Security segment focuses on providing Internet security technology, global response, and the services necessary for organizations to manage their information security needs. The Enterprise Administration segment offers products for IT department efficiency. The Consumer Products segment focuses on products for individual users, home offices, and small businesses. The Services segment provides information security solutions that incorporate technology, security expertise, and global resources. The Other segment is composed of products that have reached or are nearing the end of their lifecycle.

B. Symantec Financial Profile

Table 32: Symantec Financial Profile

Symantec Financial Profile			
	2009	2008	2007
Dollars in Millions			
Total Revenue	6,149.85	5,874.42	5,199.37
Total Cost of Goods Sold (COGS)	1,226.93	1,220.33	1,215.83
Gross Margin (profit)	4,922.93	4,654.09	3,983.54
Sales, General, and Administrative Costs	2,728.79	2,762.91	2,324.43
Research and Development	879.7	895.24	866.88
Operating Income or Loss	**-6469.91**	**660.78**	**519.74**
Number of Employees	17,426	No Information	No Information
Symantec NAC Market Share Position (based on calendar year revenue)	No Information	No Information	No Information
Symantec NAC Market Share	No Information	No Information	No Information

C. Symantec Product Guide

Table 33: Symantec Products

Symantec Products			
Products	Symantec Network Access Control Enforcer 6100 Series DHCP Enforcer and SNAC Client*	Symantec Network Access Control Enforcer 6100 Series LAN Enforcer and SNAC Client*	Symantec Network Access Control Enforcer 6100 Series Gateway Enforcer and SNAC Client*
Cisco Equivalent	Cisco NAC 3350 Appliance	Cisco NAC 3350 Appliance	Cisco NAC 3350 Appliance
Identification and Authentication			
Single Sign-On (SSO)	Yes	Yes	Yes
IEEE 802.1x Support	No	Yes	No
Identification and Authentication of Wireless Devices	Yes	Yes	Yes
Captive Web Portal Logon	Yes	Yes	Yes
Authentication by User Name and Organizational Role	Yes	Yes	Yes
Authentication by Device MAC Address	Yes	Yes	Yes
Authentication by Device IP Address	Yes	Yes	Yes
Kerberos Support	No	No	No
Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), and RADIUS Support	Yes	Yes	Yes
Posture Assessment			
Agentless and Installed Client	Yes	Yes	Yes
Client Operating Systems	Mac OS X, Microsoft Windows, and Linux; persistent in Windows only		
Browsers	Internet Explorer and Firefox		
Pre- and Post-Admission Device Scanning	Yes	Yes	Yes
Registry Entry Scanning	Yes	Yes	Yes
Detection of Unauthorized Applications	Yes	Yes	Yes
Detection of Unauthorized Processes, Services, and Open Ports	Yes	Yes	Yes

NAC: Symantec

Table 33: Symantec Products

Symantec Products (continued)			
Products	Symantec Network Access Control Enforcer 6100 Series DHCP Enforcer and SNAC Client*	Symantec Network Access Control Enforcer 6100 Series LAN Enforcer and SNAC Client*	Symantec Network Access Control Enforcer 6100 Series Gateway Enforcer and SNAC Client*
Posture Assessment (continued)			
Assessment of Managed and Unmanaged Devices	Yes	Yes	Yes
Auto-Assessment of Other IP-Based Computing Devices (printers, IP phones, medical equipment, etc.)	Yes, requires SNAC scanner	Yes, requires SNAC scanner	Yes, requires SNAC scanner
Other Endpoint Security Software Supported	Personal firewall, antivirus, and malicious-code protection	Personal firewall, antivirus, and malicious-code protection	Personal firewall, antivirus, and malicious-code protection
Assessment and Policy Enforcement of Guest Users (unmanaged)	Yes, Linux and UNIX; requires SNAC scanner	Yes, Linux and UNIX; requires SNAC scanner	Yes, Linux and UNIX; requires SNAC scanner
Access Control Authorization and Enforcement			
VLAN Network Access Control	No	Yes	Yes
Network Access Control by Subnet	Yes	No	Yes
Layer 3 Device Network Admission Control	Yes	No	No
Layer 2 LAN Switch Network Admission Control	No	Yes	No
WLAN Access Point Network Admission Control	Yes	Yes	No
Firewall Network Admission Control	No	No	No
SSL VPN Gateway Admission Control	Yes; requires Symantec On-Demand Server and Agent		
NAC Hardware Module for Routers	No	No	No
Inline NAC	No	No	Yes
Host and Endpoint Admission Control	Yes	Yes	Yes
Quarantine and Remediation Services			
Quarantine by VLAN	No	Yes	No
Quarantine by Subnet	Yes	No	Yes
Fully Automated Remediation Support	Yes	Yes	Yes
Directed URL for Updates and Patches	Yes	Yes	Yes
Built-in Native Host Intrusion Prevention	Yes	Yes	Yes
Integration with SIEM	No	No	No
Management Platform	Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager

Table 33: Symantec Products

Symantec Products (continued)			
Products	Symantec Network Access Control Enforcer 6100 Series DHCP Enforcer and SNAC Client*	Symantec Network Access Control Enforcer 6100 Series LAN Enforcer and SNAC Client*	Symantec Network Access Control Enforcer 6100 Series Gateway Enforcer and SNAC Client*
Technical Summary			
Maximum Number of Concurrent Users	No information	No information	No information
CPU	2.8-GHz Intel Pentium 4 processor	2.8-GHz Intel Pentium 4 processor	2.8-GHz Intel Pentium 4 processor
Hard Drive and Storage Controller	160-GB SATA	160-GB SATA	160-GB SATA
High Availability	Yes; A/S failover	Yes; A/S failover	Yes; A/S failover
Size (chassis height)	1RU	1RU	1RU
Network I/O Ports	2X dual-port 10/100/1000	2X dual-port 10/100/1000	2X dual-port 10/100/1000
Redundant Power Supplies	No	No	No

*The three Symantec 6100 Series Enforcer appliances are also offered as software-only products. In addition, DHCP Enforcer is offered as a plug-in to a Microsoft Dynamic Host Configuration Protocol (DHCP) server.

D. Symantec Sales Tactics

- Symantec typically uses its antivirus software installed base to promote network admission control (NAC) sales.
- Symantec may claim that its products are simple to deploy.
- Symantec often diverts the conversation toward the number of agents on the desktop and how Symantec can achieve the same results with just a single agent. In reality, customers typically deploy NAC because they cannot rely on the endpoint and its agent to police itself. The intelligence and enforcement needs to reside on the network.

E. Symantec Weaknesses

- The company has only limited security and NAC offerings for enterprise customers.
- The Symantec security offering is largely focused on endpoints. Symantec Endpoint Protection 11 implements a common agent architecture for malicious code protection, intrusion prevention, and NAC. Such a “fat client” approach severely affects the performance of the endpoints and may not address unmanaged assets.
- Symantec has a complicated mix of enforcement points. Products require different devices for in-band (Gateway Enforcer) and out-of-band (LAN Enforcer) support.
- Symantec cannot make use of the existing infrastructure (such as routers and switches) for policy enforcement.

NOTES

SSL VPN

Companies	Sections in Each Company Guide
I. Check Point	A. Company Overview
II. Citrix	B. Financial Profile
III. F5	C. Product Guide
IV. Juniper Networks	D. Sales Tactics
V. SonicWALL	E. Weaknesses

SSL VPN: Check Point

I. Check Point

A. Check Point Overview

For full Check Point overview see page 16.

B. Check Point Financial Profile

For full Check Point financial data see page 17.

Table 34: Check Point Financial Profile

Check Point Financial Profile			
	2008	2007	2006
Dollars in Millions			
Worldwide SSL VPN Gateway Market Share Position	5	5	5
Worldwide SSL VPN Gateway Market Share	8%	6%	7%

C. Check Point Product Guide

Table 35 Check Point Products

Check Point Products			
Products	Connectra 270	Connectra 3070	Connectra 9072
Cisco Equivalent	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5580 or 5540
Features and Functions			
Maximum Number of Simultaneous VPN Users	100	1000	10,000
Secure Sockets Layer (SSL) VPN Sessions per Second	No information	No information	No information
SSL Clientless Access (browsers and microbrowsers)	Internet Explorer version 5.5 or later, Firefox, Safari, and Netscape		
Clientless Network Resource Support	Integrity Clientless Security and Integrity Secure Workspace for Connectra (Windows only)		
Support for IP Security (IPsec) and SSL VPN Clients	Yes	Yes	Yes
Pre-Connection Endpoint Posture Assessment	Yes	Yes	Yes
Application-Aware Traffic Inspection	Yes	Yes	Yes
Keystroke Logger Protection	Yes	Yes	Yes
Single Sign-On (SSO) for Web Interface	Yes	Yes	Yes
Integrated Network Firewall and Intrusion Prevention System (IPS)	SmartDefense on Connectra appliances; SmartDefense with SSL Network Extender on VPN-1 and UTM-1	SmartDefense on Connectra appliances; SmartDefense with SSL Network Extender on VPN-1 and UTM-1	SmartDefense on Connectra appliances; SmartDefense with SSL Network Extender on VPN-1 and UTM-1
Integrated High Availability	Active-active (A/A) and active-standby (A/S)	A/A and A/S	A/A and A/S
Internal Load Balancing	Yes	Yes	Yes
End-of-Session Data Cleanup	Yes	Yes	Yes
Datagram Transport Layer Security (DTLS) Support for SSL Client	No	No	No
Customizable Web Portals	Yes	Yes	Yes
Guest Permissions	Yes	Yes	Yes

SSL VPN: Check Point

Table 35: Check Point Products

Check Point Products (continued)

Products	Connectra 270	Connectra 3070	Connectra 9072
Features and Functions (continued)			
Native Application Client	Yes, Endpoint Connect for IPsec VPN; Network Extender for SSL	Yes, Endpoint Connect for IPsec VPN; Network Extender for SSL	Yes, Endpoint Connect for IPsec VPN; Network Extender for SSL
Web-Based and Command-Line Interface (CLI) Management Support	No	No	No
VLAN Support	Yes, 256	Yes, 256	Yes, 256
Idle Session Timeout Termination	Yes	Yes	Yes
Split-Tunneling Support	Yes	Yes	Yes
SSL Session Persistence	No	No	No
Logging and Reporting	Yes; requires Eventia Analyzer and Eventia Reporter	Yes; requires Eventia Analyzer and Eventia Reporter	Yes; requires Eventia Analyzer and Eventia Reporter
Multi-Factor Authentication Support	Active Directory, internal database, client certificates, LDAP, RADIUS, RSA SecurID, and ActivIdentity	Active Directory, internal database, client certificates, LDAP, RADIUS, RSA SecurID, and ActivIdentity	Active Directory, internal database, client certificates, LDAP, RADIUS, RSA SecurID, and ActivIdentity
RADIUS and Lightweight Directory Access Protocol (LDAP) Support	Yes	Yes	Yes
Technical Summary			
Management Platform	SmartCenter or Provider-1	SmartCenter or Provider-1	SmartCenter or Provider-1
Client Operating Systems Supported	Linux, Macintosh (including Intel-based), and Windows 2000 and XP (Vista supported in Network Extender)	Linux, Macintosh (including Intel-based), and Windows 2000 and XP (Vista supported in Network Extender)	Linux, Macintosh (including Intel-based), and Windows 2000 and XP (Vista supported in Network Extender)
Size (chassis height)	1 rack unit (1RU)	1RU	2RU
Interface Ports	4X copper Gigabit Ethernet	10X copper Gigabit Ethernet	Fixed: 10X copper Gigabit Ethernet; Optional: 4X Gigabit Ethernet copper; 4X Gigabit Ethernet fiber LR (single mode); 4X Gigabit Ethernet fiber SR (multimode)
Redundant Power Supplies	No	No	Yes
FIPS-140-2 Certification	No	No	No
Common Criteria Certification	No	No	No

D. Check Point Sales Tactics

- Check Point may attempt to position its Connectra SSL VPN products as natural adjuncts to Check Point customers' existing VPN-1 and Power-1 deployments, particularly when the customer is investigating moving from an existing IPsec VPN remote access model to one using SSL VPN remote access technologies.
- Check Point may promote the integrated support of its Connectra appliances with its NGX R70 product suite, including its primary management platforms, SmartCenter and Provider-1, and Eventia.
- Check Point may also promote its web browser plug-in software, SSL Network Extender, which enables clientless SSL VPN functions without deployment of the Connectra appliance. However, for midsize to large enterprise deployments, Check Point generally will position its Connectra appliances for any scalable SSL VPN remote access solution.

E. Check Point Weaknesses

- Connectra is a remote access VPN product only. It has no firewall or site-to-site VPN capabilities as part of the Connectra appliance itself. Other separate appliances are required for these functions.
- Check Point has no true IPS integration with its SSL VPN product offerings. It does have a truncated form of IPS it calls SmartDefense, but its true IPS product offerings are its IPS-1 product line (formerly NFR), which has no integration with its flagship NGX R70, Connectra, or SmartCenter and Provider-1 management platforms.
- Two separate clients are required to support both IPsec (Endpoint Connect) and SSL (Network Extender).
- Check Point Connectra uses Check Point Integrity for its Endpoint Protection and Secure Workspace functions. Windows is the only OS supported by Integrity, and Internet Explorer the only browser.

SSL VPN: Citrix

II. Citrix

A. Citrix Overview

Citrix Systems, Inc., a publicly held company headquartered in Ft. Lauderdale, Florida, designs, develops, markets, sells, and supports multiple products in the Application Delivery Infrastructure. Its product family for all its infrastructure solutions is Citrix Delivery Center. Products in this family include solutions for application, server, and desktop virtualization; web application optimization; application performance monitoring; branch-office and WAN application delivery optimization; SSL VPN gateways; and IP telephony. Citrix also offers GoTo services, such as GoToMyPC, GoToMeeting, GoToAssist, GoToWebinar, and all their variants, collectively called Online Services, through its Online Services Division. It organizes its products into four principal groups: Delivery Systems, Virtualization and Management Systems, and Online Services and Technical Services. The Access Gateway SSL VPN products are part of the Delivery Systems group. On October 19, 2007, Citrix acquired XenSource, Inc.

B. Citrix Financial Profile

Table 36: Citrix Financial Profile

Citrix Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	1,583,354,000	1,391,942,000	1,134,319,000
Total Cost of Goods Sold (COGS)	175,132,000	137,607,000	98,698,000
Gross Margin (profit)	92.61% (5-year average)		
Sales, General, and Administrative Costs	926,249,000	819,638,000	659,012,000
Research and Development	288,109,000	205,103,000	155,331,000
Operating Income or Loss	**170,001,000**	**202,407,000**	**203,344,000**
Operating Profit or Loss	178,276,000	214,483,000	182,997,000
Number of Employees	5040	4620	3742
Overall Market Share Position	2	2	3
Worldwide Network Security Market Share	21%	16%	15%

SSL VPN: Citrix

C. Citrix Product Guide

Table 37: Citrix Products

Citrix Products													
Products	Access Gateway Standard and Advanced Editions 2010	Access Gateway Enterprise Edition 7000	Access Gateway Enterprise Edition 9010	Access Gateway Enterprise Edition 10010	MPX 17000	MPX 1500	MPX 12500	MPX 10500	MPX 9500	9010 FIPS	MPX 7500	MPX 5500	VPX 10/ 200/1000
Cisco Equivalent	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580	Cisco ASA 5580	Cisco ASA 5580	Cisco ASA 5580	Cisco ASA 5580	Cisco ASA 5580	Cisco ASA 5550	Cisco ASA 5580	Cisco ASA 5550	Cisco ASA 5520 / 5510
Features and Functions													
Maximum Number of Simultaneous VPN Users	500	2500	5000	10,000	10,000	10,000	10,000	10,000	10,000	5000	10,000	5000	Up to 300
SSL VPN Sessions per Second	No information	4400	4400	8800	80,000	60,000	48,000	24,000	16,000	4400	8000	4000	Up to 500
SSL Clientless Access (browsers and microbrowsers)	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari	Internet Explorer, Firefox, and Safari
Clientless Network Resource Support	Layer 3 tunneling only	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server	Files, web, and presentation server
Support for IP Security (IPsec) and SSL VPN Clients	No	No	No	No	No	No	No	No	No	No	No	No	No
Pre-Connection Endpoint Posture Assessment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Application-Aware Traffic Inspection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Keystroke Logger Protection	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software	Yes; requires third-party software
Single Sign-On (SSO) for Web Interface	Yes; Citrix Password Manager (Advanced Edition only)	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager	Yes; Citrix Password Manager

SSL VPN: Citrix

Table 37: Citrix Products

Citrix Products (continued)													
Products	Access Gateway Standard and Advanced Editions 2010	Access Gateway Enterprise Edition 7000	Access Gateway Enterprise Edition 9010	Access Gateway Enterprise Edition 10010	MPX 17000	MPX 1500	MPX 12500	MPX 10500	MPX 9500	9010 FIPS	MPX 7500	MPX 5500	VPX 10/ 200/1000
Features and Functions (continued)													
Integrated Network Firewall and Intrusion Prevention System (IPS)	No	No	No	No	No	No	No	No	No	No	No	No	No
Integrated High Availability	No	Active-standby (A/S)	A/S	A/S	A/S	A/S	A/S	A/S	A/S	A/S	A/S	A/S	A/S
Internal Load Balancing	No	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware	Yes, on NetScaler hardware
End-of-Session Data Cleanup	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Datagram Transport Layer Security (DTLS) Support for SSL Client	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Customizable Web Portals	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Guest Permissions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Native Application Client	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Web-Based and Command-Line Interface (CLI) Management Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VLAN Support	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number

SSL VPN: Citrix

Table 37: Citrix Products

Citrix Products (continued)

Products	Access Gateway Standard and Advanced Editions 2010	Access Gateway Enterprise Edition 7000	Access Gateway Enterprise Edition 9010	Access Gateway Enterprise Edition 10010	MPX 17000	MPX 1500	MPX 12500	MPX 10500	MPX 9500	9010 FIPS	MPX 7500	MPX 5500	VPX 10/ 200/1000
Features and Functions (continued)													
Idle Session Timeout Termination	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Split-Tunneling Support	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SSL Session Persistence	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Logging and Reporting	Limited (Advanced Edition only)	Yes, though Citrix Command Control (CCC)	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC	Yes, through CCC
Multi-Factor Authentication Support	Yes (limited)	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards	Variety of biometrics, certificates, tokens, and smartcards
RADIUS and Lightweight Directory Access Protocol (LDAP) Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Technical Summary													
Management Platform	CCC						CCC						
Client Operating Systems Supported	Windows 2000, XP, and Vista and Linux	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux and Mac OS X	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux and Mac OS X	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux and Mac OS X	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7	Windows 2000, XP, Vista, and CE; Linux; and Java-based client for Linux, Mac OS X, and Windows 7
Size (chassis height)	1RU	1RU	2RU	2RU	2RU	2RU	2RU	2RU	2RU	2RU			

SSL VPN: Citrix

Table 37: Citrix Products

Citrix Products (continued)

Products	Access Gateway Standard and Advanced Editions 2010	Access Gateway Enterprise Edition 7000	Access Gateway Enterprise Edition 9010	Access Gateway Enterprise Edition 10010	MPX 17000	MPX 1500	MPX 12500	MPX 10500	MPX 9500	9010 FIPS	MPX 7500	MPX 5500	VPX 10/ 200/1000
Technical Summary (continued)													
Interface Ports	1X serial, 2X 10/100 LAN ports, and 1X USB"	6X 10/100 and 2X 10/100/1000"	4X 10/100/ 1000 and 1X 10/100/ 1000	8 ports in one of two configurations: 4X 10/ 100/1000 and 4X Gigabit Ethernet fiber Small Form-Factor Pluggable (SFP), or 4X 10/100/1000 and 4X Gigabit Ethernet copper SFP; 1X 10/100 (management)	4X 10GBASE-X XFP or 2X 10GBASE-X XFP and 8X 10/100/ 1000 BASE-T	4X 10GBASE-X XFP or 2X 10GBASE-X XFP and 8X 10/100/ 1000 BASE-T	8X 10/100/1000 BASE-T and 8X 1000BASE-X SFP	8X 10/100/1000 BASE-T and 8X 1000BASE-X SFP	8X 10/100/1000 BASE-T	4X 10/ 100/1000 and 1X 10/100/ 1000	8X 10/ 100/1000 BASE-T	4X 10/ 100/1000 BASE-T"	Dependent on server platform chosen
Redundant Power Supplies	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes - optional	Yes	Yes - optional	No	Dependent on server platform chosen
Federal Information Processing Standard (FIPS) 140-2 Certification	No	No	Yes, in FIPS version (hardware and software)	No	No	No	No	No	No	Yes (hardware and software)	No	No	No
Common Criteria Certification	No	No	No	No	No	No	No	No	No	No	No	No	No

SSL VPN: Citrix

D. Citrix Sales Tactics

- Citrix often attempts to use its older installed base of Presentation Server customers to gain access to SSL VPN opportunities.
- Citrix generally emphasizes Access Gateway's SSL VPN integration with Citrix Presentation Sever and Independent Computing Architecture (ICA).
- Although Citrix Presentation Server Platinum Edition includes SSL VPN software (called Secure Gateway), for the more full-featured and scalable SSL VPN functions Citrix may persuade customers to upgrade to the dedicated Access Gateway SSL VPN platform.
- Citrix often approaches a customer's application delivery technology and business decision makers (TDMs and BDMs) rather than decision makers in security or networking for participation in those customers' SSL VPN remote access opportunities.

E. Citrix Weaknesses

- Citrix does not support the breadth of native client and clientless access methods that Cisco does.
- Citrix does not support integrated network firewall, IPsec VPN, and intrusion prevention (IPS) functions.
- The Citrix management platform, Command Central, cannot manage the same breadth of security products and technologies as the Cisco Security Manager and Security Monitoring, Analysis, and Response System (MARS) management suite.
- Citrix has no support for the DTLS standard.

NOTES

SSL VPN: F5

III. F5

A. F5 Overview

F5 Networks, Inc. provides technology that optimizes the delivery of network-based applications, as well as the security, performance, and availability of servers, data storage devices, and other network resources. Its products include BIG-IP, an application delivery controller; VIPRION, a chassis-based application delivery controller; FirePass, which provides SSL VPN access for remote users of IP networks, and applications connected to those networks from any standard web browser on any device; and Application Security Manager, a web application firewall that provides application-layer protection against generalized and targeted attacks. The company also offers WebAccelerator, which speeds web transactions by individual network object requests, connections, and end-to-end transactions; WANJet, which accelerates file transfers, email, data replication, and other applications over IP networks; and Enterprise Manager, which allows customers to discover and view products in a single window.

In addition, F5's ARX product family offers enterprise-class intelligent file virtualization devices, which simplify the management of file storage environments; a Data Manager that gathers file storage statistics and provides graphical reporting and trending functions; and iControl, which allows customers and independent software vendors to modify programs. Further, the company offers services, such as consulting, training, installation, maintenance, and other technical support services. It primarily serves technology, telecommunications, financial services, transportation, education, and manufacturing and healthcare industries, as well as government customers. The company markets its products and services through distributors, value-added resellers, and systems integrators. It sells its products and services in the Americas, Europe, the Middle East, Africa, Japan, and the Asia Pacific. F5 Networks, Inc. was founded in 1996 and is headquartered in Seattle, Washington.

B. F5 Financial Profile

Table 38: F5 Financial Profile

F5 Financial Profile

	2009	2008	2007
Dollars in Millions			
Total Revenue	653.08	650.17	525.67
Total Cost of Goods Sold (COGS)	142.73	149.02	118.32
Gross Margin (profit)	510.36	501.36	407.34
Sales, General, and Administrative Costs	280.44	293.18	224.81
Research and Development	103.67	103.40	69.03
Operating Income or Loss	**121.92**	**99.31**	**99.50**
Number of Employees	1646	No information	792
Worldwide SSL VPN Gateway Market Share Position	4	4	3
Worldwide SSL VPN Gateway Market Share	10%	11%	15%

C. F5 Product Guide

Table 39: F5 Products

F5 Products

Products	FirePass 1200	FirePass 4100	FirePass 4300
Cisco Equivalent	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540 or 5550
Features and Functions			
Maximum Number of Simultaneous VPN Users	100	500	2000
SSL VPN Sessions per Second	Not listed	Not listed	Not listed
SSL Clientless Access (browsers and microbrowsers)	Internet Explorer, Firefox, Safari, Netscape Navigator, and Openwave WAP browser	Internet Explorer, Firefox, Safari, Netscape Navigator, and Openwave WAP browser	Internet Explorer, Firefox, Safari, Netscape Navigator, and Openwave WAP browser
Clientless Network Resource Support	Yes	Yes	Yes
Support for IP Security (IPsec) and SSL VPN Clients	No	No	No
Pre-Connection Endpoint Posture Assessment	Yes	Yes	Yes
Application-Aware Traffic Inspection	Yes	Yes	Yes
Keystroke Logger Protection	Yes; secure login	Yes; secure login	Yes; secure login
Single Sign-On (SSO) for Web Interface	Yes	Yes	Yes
Integrated Network Firewall and Intrusion Prevention System (IPS)	Yes; for Windows 2000 and XP users when using the Full Network Access feature		
Integrated High Availability	Paired Failover	Paired failover and clustering using the F5 BIG-IP GTM and LTM devices for FirePass 4100 and 4300	
Internal Load Balancing	No	Yes	Yes
End-of-Session Data Cleanup	Yes; for Windows platform only		
Datagram Transport Layer Security (DTLS) Support for SSL Client	No	No	No
Customizable Web Portals	Can customize end-user GUI		
Guest Permissions	No	No	No
Native Application Client	Yes	Yes	Yes

SSL VPN: F5

Table 39: F5 Products

F5 Products (continued)			
Products	FirePass 1200	FirePass 4100	FirePass 4300
Features and Functions (continued)			
Web-Based and Command-Line Interface (CLI) Management Support	Yes, both	Yes, both	Yes, both
VLAN Support	Yes; no information on maximum number	Yes; no information on maximum number	Yes; no information on maximum number
Idle Session Timeout Termination	Yes	Yes	Yes
Split-Tunneling Support	Yes	Yes	Yes
SSL Session Persistence	Yes	Yes	Yes
Logging and Reporting	Yes	Yes	Yes
Multi-Factor Authentication Support	RADIUS, Active Directory, RSA 2-Factor, LDAP authentication methods, basic and form-based HTTP authentication, identity management servers (such as Netegrity), and Windows domain servers		
RADIUS and Lightweight Directory Access Protocol (LDAP) Support	Yes	Yes	Yes
Technical Summary			
Management Platform	BIG-IP GTM and LTM (global and local traffic management)		
Client Operating Systems Supported	Windows (2000, Me, XP, and Vista), Mac OS X, Linux, and Windows Mobile 5 and 6 pocket PC and smartphone		
Size (chassis height)	1 rack unit (RU)	2RU	2RU
Interface Ports	2X 10/100 LAN Ports	4X 10/100/1000 LAN ports	4X 10/100/1000 LAN ports and 2X 1-Gbps fiber SFP ports
Redundant Power Supplies	No	Optional	No
Federal Information Processing Standard (FIPS) 140-2 Certification	Yes	Yes	Yes
Common Criteria Certification	No	No	No

D. F5 Sales Tactics

- F5 generally attempts to use its BIG-IP application acceleration and optimization solutions with large data center customers to also sell its SSL VPN products.
- Since F5 has no IPsec VPN offering, it may target existing IPsec installations for conversion to its own remote access solution offering, including FirePass SSL VPN.
- F5 often targets customers with large older mainframe applications, positioning the application "webification" capabilities of BIG-IP and the securing of those webified applications with FirePass SSL VPN.

E. F5 Weaknesses

- Generally, F5 has two fundamental product offerings: application and content acceleration and optimization, and SSL VPN (with FirePass).
- F5's SSL VPN product offerings (FirePass appliances) are only adjuncts to the primary F5 solution offering: BIG-IP.
- Except in its SSL VPN product offerings, F5 is generally not considered a recognized security vendor.
- Top-of-the-line FirePass 4300 can support up to only 2000 concurrent users per appliance. Cisco ASA 5580-40 can support up to 10,000 concurrent users per appliance.
- Client-side cache cleaning is available only for Windows users. No cache cleaning mechanism is available for non-Windows platforms.
- F5's iRules engine can degrade performance.
- F5 may be experiencing difficulty in crossing over from the application optimization to the security market space. Its market share position has been relatively flat or declining over the past several quarters.
- F5 has limited channel reach and limited worldwide field support.

SSL VPN: Juniper Networks

III. Juniper Networks

A. Juniper Overview

For full Juniper Network overview see page page 40.

B. Juniper Financial Profile

For full Juniper financial data see page page 41.

Table 40: Juniper Financial Profile

Juniper Financial Profile	2008	2007	2006
Dollars in Millions			
Worldwide SSL VPN Gateway Market Share Position	1	1	1
Worldwide SSL VPN Gateway Market Share	28%	26%	28%

C. Juniper Product Guide

Table 41: Juniper Products

Juniper Products				
Products	SA 700	SA 2500	SA 4500	SA 6500
Cisco Equivalent	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5540	Cisco ASA 5580
Features and Functions				
Maximum Number of Simultaneous VPN Users	10 to 25	100	1000	10,000
Secure Sockets Layer (SSL) VPN Sessions per Second	No information	No information	No information	No information
SSL Clientless Access (browsers and microbrowsers)	Internet Explorer, Firefox, and Safari			
Clientless Network Resource Support	With additional license	Yes	Yes	Yes
Support for IP Security (IPsec) and SSL VPN Clients	No	No	No	No
Pre-Connection Endpoint Posture Assessment	Yes	Yes	Yes	Yes
Application-Aware Traffic Inspection	No information	Yes	Yes	Yes
Keystroke Logger Protection	No information	Yes	Yes	Yes
Single Sign-On (SSO) for Web Interface	No information	Yes	Yes	Yes
Integrated Network Firewall and Intrusion Prevention System (IPS)	No	No	No	No
Integrated High Availability	No information	With clustering software: active-standby (A/S), active-active (A/A), and stateful peering	With clustering software: A/S, A/A, and stateful peering	With clustering software: A/S, A/A, and stateful peering
Internal Load Balancing	No; requires external load balancer			
End-of-Session Data Clean-Up	Yes	Yes	Yes	Yes
Datagram Transport Layer Security (DTLS) Support for SSL Client	No	Yes	Yes	Yes
Customizable Web Portals	No	Yes	Yes	Yes
Guest Permissions	No	Yes	Yes	Yes
Native Application Client	Network Connect SSL			

SSL VPN: Juniper Networks

Table 41: Juniper Products

Juniper Products (continued)				
Products	SA 700	SA 2500	SA 4500	SA 6500
Features and Functions (continued)				
Web-Based and Command-Line Interface (CLI) Management Support	Yes (both)	Yes (both)	Yes (both)	Yes (both)
VLAN Support	Yes; no information on maximum number	240	240	240
Idle Session Timeout Termination	Yes	Yes	Yes	Yes
Split-Tunneling Support	Yes	Yes	Yes	Yes
SSL Session Persistence	Yes	Yes	Yes	Yes
Logging and Reporting	Yes	Yes	Yes	Yes
Multi-Factor Authentication Support	RADIUS, LDAP, Public Key Infrastructure (PKI), Active Directory, RSA SecurID, and BioPassword	RADIUS, LDAP, PKI, Active Directory, RSA SecurID, and BioPassword	RADIUS, LDAP, PKI, Active Directory, RSA SecurID, and BioPassword	RADIUS, LDAP, PKI, Active Directory, RSA SecurID, and BioPassword
RADIUS and LDAP Support	Yes	Yes	Yes	Yes
Technical Summary				
Management Platform	Secure Access Central Manager; also integration with Network and Security Manager			
Client Operating Systems Supported	Windows, Mac OS X, Linux, and mobile devices	Windows, Mac OS X, Linux, and mobile devices	Windows, Mac OS X, Linux, and mobile devices	Windows, Mac OS X, Linux, and mobile devices
Size (chassis height)	1 rack unit (RU)	1RU	1RU	2RU
Interface Ports	2X RJ-45 10/100	2X RJ-45 Ethernet 10/100/1000 full or half-duplex (auto-negotiation); Management: n/a; Console: 1X RJ-45 serial console port	2X RJ-45 Ethernet 10/100/1000 Console: 1X RJ-45 serial console port	4X RJ-45 10/100/1000; optional 4-port Small Form-Factor Pluggable (SFP) Gigabit Ethernet; 1X RJ-45 10/100/1000 management
Redundant Power Supplies	No	No	No	Yes
Federal Information Processing Standard (FIPS) 140-2 Certification	No	No	Yes, on FIPS version	Yes, on FIPS version (but reduces maximum number of users from 10,000 to 3500)
Common Criteria Certification	No	No	No	No

D. Juniper Sales Tactics

- Juniper generally claims to be the market leader in SSL VPN products.
- Juniper may promote its optional In Case of Emergency (ICE) service-level agreement (SLA) license as a differentiator.
- Juniper generally promotes these additional, optional Secure Access software license upgrades: Enhanced Endpoint Security, Secure Meeting, High Availability, and Instant Virtual Systems.
- Juniper may claim to have both IPsec and SSL VPN support in the Secure Access product line (see the "Juniper Weaknesses" section).
- Juniper may imply that Secure Access has tight integration with the other Juniper products.

E. Juniper Weaknesses

- Little integration has been achieved between the Secure Access (formerly Neoteris) product platform and Juniper's FW/IPsec product platforms (ScreenOS and SRX for Junos product lines).
- Juniper's self-proclaimed IPsec-like implementation, included in the Secure Access platform, has no support for either Authentication Header (AH) or Internet Key Exchange (IKE). It is not interoperable with standards-based IPsec implementations.
- Juniper's Secure Access offerings can be more expensive than comparable Cisco ASA SSL VPN offerings.
- Site-to-site VPN tunneling is not available on the Juniper SA Series.
- To achieve high availability for the Secure Access products, both clustering software and an external load balancer are required.
- The DTLS standard is not supported.

NOTES

SSL VPN: SonicWALL

V. SonicWALL

A. SonicWALL Overview

For full SonicWALL overview see page 60.

B. SonicWALL Financial Profile

For full SonicWALL financial data see page 61.

Table 42: SonicWALL Financial Profile

SonicWALL Financial Profile			
	2008	2007	2006
Dollars in Millions			
Worldwide SSL VPN Gateway Market Share Position	7	8	7
Worldwide SSL VPN Gateway Market Share	4%	5%	3%

SSL VPN: SonicWALL

C. Product Guide: SonicWALL

Table 43: SonicWALL Products

SonicWALL Products						
	SSL VPN Series			Aventail E-Class		
Products	SSL-VPN 200	SRA 4200	SSL-VPN 4000	EX-750	EX-6000	EX-7000
Cisco Equivalent	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5510	Cisco ASA 5510	Cisco ASA 5510 or ASA 5520	Cisco ASA 5550
Features and Functions						
Maximum Number of Simultaneous VPN Users	10	50	200	50	250	2000
Secure Sockets Layer (SSL) VPN Sessions per Second	No information	No information	No information	No information	No information	No information
SSL Clientless Access (browsers and microbrowsers)	Microsoft Internet Explorer and Mozilla Firefox			All Windows, Macintosh, and Linux browser platforms using currently supported Java or ActiveX agents for Citrix or Windows Terminal Services		
Clientless Network Resource Support	Yes, SonicWALL Virtual Assistant	Yes, SonicWALL Virtual Assistant	Yes, SonicWALL Virtual Assistant	Yes	Yes	Yes
Support for IP Security (IPsec) and SSL VPN Clients	No	No	No	No	No	No
Pre-Connection Endpoint Posture Assessment	No	No	No	Yes (End Point Control [EPC] combines pre-authentication interrogation to confirm endpoint criteria such as antivirus updates)	Yes	Yes
Application-Aware Traffic Inspection	No	No	No	Yes	Yes	Yes
Keystroke Logger Protection	Yes	Yes	Yes	Yes	Yes	Yes
Single Sign-On (SSO) for Web Interface	No	No	No	Yes	Yes	Yes
Integrated Network Firewall and Intrusion Prevention System (IPS)	No	No	No	No	No	No
Integrated High Availability	No	No	No	No information	Active-active (A/A)	A/A and clustering
Internal Load Balancing	No	No	No	No information	Yes	Yes
End-of-Session Data Cleanup	Optional	Optional	Optional	Cache Control	Cache Control	Cache Control
Datagram Transport Layer Security (DTLS) Support for SSL Client	No	No	No	No	No	No
Customizable Web Portals	Yes	Yes	Yes	Yes	Yes	Yes
Guest Permissions	No	No	No	No	No	No
Native Application Client	No	No	No	Connect Tunnel client and Native Access Modules	Connect Tunnel client and Native Access Modules	Connect Tunnel client and Native Access Modules
Web-Based and Command-Line Interface (CLI) Management Support	Yes	Yes	Yes	No	No	No
VLAN Support	No	No	No	No	No	No

SSL VPN: SonicWALL

Table 43: SonicWALL Products

SonicWALL Products (continued)						
	SSL VPN Series			Aventail E-Class		
Products	SSL-VPN 200	SRA 4200	SSL-VPN 4000	EX-750	EX-6000	EX-7000
Features and Functions (continued)						
Idle Session Timeout Termination	Yes	Yes	Yes	No	No	No
Split-Tunneling Support	No	No	No	Yes	Yes	Yes
SSL Session Persistence	No	No	No	Yes	Yes	Yes
Logging and Reporting	Yes	Yes	Yes	Yes	Yes	Yes
Multi-Factor Authentication Support	Tokenless two-factor authentication, Vasco one-time passwords, internal user database, RADIUS, LDAP, Microsoft Active Directory, and Windows NT Domain	Tokenless two-factor authentication, RSA, Vasco one-time passwords, internal user database, RADIUS, LDAP, Microsoft Active Directory, and Windows NT Domain	Tokenless two-factor authentication, RSA, Vasco one-time passwords, internal user database, RADIUS, LDAP, Microsoft Active Directory, and Windows NT Domain	Server-side digital certificates, username and password, client-side digital certificates, RSA SecurID and other one-time password tokens, and dual and stacked authentication		
RADIUS and LDAP Support	Yes	Yes	Yes	Yes	Yes	Yes
Technical Summary						
Management Platform	SonicWALL Global Management System (GMS)			SonicWALL Aventail Management Console (AMC)		
Client Operating Systems Supported	Windows 2000, 2003, XP, and Vista (32- and 64-bit)			Windows, Linux, Mac OS X, and mobile devices		
Size (chassis height)	1 rack unit (RU)	1RU	1RU	1RU	1RU	1RU
Interface Ports	5X 10/100 Ethernet	4X 10/100 Ethernet and 1X serial port	6X 10/100 Ethernet and 1X serial port	2X 10/100BASE-T Ethernet	2X 10/100 and 1X 1000BASE-T Ethernet, 2X USB ports, and 1X serial bus connection (DB9)	6X 10/100/1000BASE-T Ethernet
Redundant Power Supplies	No	No	No	No	No	No
FIPS-140-2 Certification	No	No	No	No	No	No
Common Criteria Certification	No	No	No	No	No	No

SSL VPN: SonicWALL

D. SonicWALL Sales Tactics

- SonicWALL has traditionally been a security vendor in the small and medium-sized business (SMB) market. Nearly all its products are sold through channels.
- SonicWALL now has two SSL VPN product lines: its older product line and the products it obtained from its acquisition of Aventail. The older SonicWALL SSL VPN products generally are positioned for the SMB market, and the Aventail products are positioned for midsized to large enterprises; for the latter, SonicWALL may promote the Aventail feature that allows administrators to remotely revoke a mobile client's digital certificate if a user's mobile device is lost or stolen.
- SonicWALL may promote its SSL VPN portfolio of supported mobile client devices as a primary differentiator.

E. SonicWALL Weaknesses

- SonicWALL's SSL VPN products and functions are not integrated into any of the other SonicWALL unified threat management (UTM) appliances.
- Because of SonicWALL's two disparate SSL VPN product lines and management platforms, market overlap and customer confusion may occur.
- SonicWALL's top-of-the-line SSL VPN appliance (Aventail EX-7000) has a capacity of only 2000 concurrent users. The Cisco ASA 5580-40 allows up to 10,000 concurrent users.
- Because of SonicWALL's traditional focus on the SMB market and customers, the company may face difficulties in selling the Aventail SSL VPN products to midsized and large enterprise customers.

NOTES

NOTES

Email Messaging Security

Companies	Sections in Each Company Guide
I. Barracuda Networks	A. Company Overview
II. Google Apps and Postini	B. Financial Profile
III. Microsoft Forefront	C. Product Guide
IV. McAfee	D. Sales Tactics
V. Symantec	E. Weaknesses

Email Messaging Security: Barracuda Networks

I. Barracuda Networks

A. Barracuda Overview

Barracuda Networks provides firewalls that protect enterprises from email spam, viruses, and spyware. Barracuda serves small, midsized, and large businesses in industries such as financial services, manufacturing, technology, consumer goods, utilities, and retail. Barracuda Networks also provides professional services such as support, consulting, and implementation. Barracuda Networks was founded in 2002, and is headquartered in Campbell, CA.

B. Barracuda Networks Financial Profile

Not available: Private company

C. Barracuda Product Guide

Table 44: Barracuda Products

Barracuda Products		
Competitors	Barracuda Spam Firewall	Cisco IronPort C-Series and X-Series
Email Reputation		
Reputation Filters	Yes[1]	Yes
Organizations and Sources Providing Information to Reputation Service	More than 70,000	More than 100,000
Rate-Limiting of Suspected Spam Senders	Yes	Yes
Percentage of Incoming Email Blocked by Reputation (at the connection level)	No information	90+%
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	Yes, based on open source	Yes
Antivirus Scan Engine	Yes, based on open source	Yes
Fully Integrated On-Device Scan Engines	Yes	Yes
Virus Outbreak Filters (or equivalent)	Limited	Yes
Data Loss Prevention (DLP) Features		
Integrated DLP Scanning Capabilities	No	Yes, including remediation
Number of File Types Supported for Embedded Scanning	No information	More than 400
Support for Smart Identifiers (credit card numbers, social security numbers [SSNs], etc.)	No information	Yes
Email Encryption		
Fully Integrated Email Encryption	No. TLS only	Yes
No Additional Software Required on End-User Systems for Encryption	No information	Yes
Managed Key Storage and Recovery Service	No information	Yes, Cisco Registered Envelope Service
Platform Features		
Bounce Verification Filters	Yes	Yes
Outbound Email Scanning	Add-on[2]	Yes
Support for Filtering Policies Based on Lightweight Directory Access Protocol (LDAP) Group	Limited	Yes

[1] Limited to blacklists, honeypots, and their appliances.
[2] Requires Barracuda Spam Firewall-Outbound option.

Email Messaging Security: Barracuda Networks

Table 44: Barracuda Products

Barracuda Products (continued)		
Competitors	Barracuda Spam Firewall	Cisco IronPort C-Series and X-Series
Custom Purpose-Built Operating System	No, based on Postfix and Linux	Yes
Multicore Chip Support	No information	Yes, throughput scales as cores are added
Email Authentication Support	Domain Keys Identified Mail (DKIM), Sender Policy Framework (SPF), and Sender ID Framework (SIDF)	DKIM, SPF, and SIDF
Obscene-Image Blocking	Yes	Yes
High-Performance, Custom Media Terminal Adapter (MTA)	No, based on Postfix	Yes

Table 45: Barracuda Hardware Specifications

Barracuda Hardware Specifications								
Products	100	200	300	400	600	800	900	1000
Suggested Capacity	1 to 50 users	51 to 500 users	300 to 1000 users	1000 to 5000 users	3000 to 10,000 users	8000 to 22,000 users	15,000 to 30,000 users	25,000 to 100,000 users
Form Factor	1RU	1RU	1RU	1RU	1RU	2RU	2RU	2RU
RAM	No information	No information	No information	No information	No information	No information	No information	No information
Processor	No information	No information	No information	No information	No information	No information	No information	No information
Disk	No information	No information	No information	No information	No information	No information	No information	No information
RAID	No information	No information	No information	Yes	Yes	Yes	Yes	Yes
Power Supply	Single	Single	Single	Single	Single	Redundant	Redundant	Redundant
Interfaces	1X 100 MB	1X 100 MB	1X 100 MB	1X 100 MB	2X Gigabit Ethernet	2X Gigabit Ethernet	2X Gigabit Ethernet	2X Gigabit Ethernet

Contents based on publicly available information current as of Dec 2009.

Barracuda Hardware Specifications (continued)				
Products	IronPort C160	IronPort C360	IronPort C660	IronPort X1060
Suggested Capacity	100 to 1000 users	1000 to 10,000 users	10,000 or more users	Carrier or ISP
Form Factor	1RU	2RU	2RU	2RU
RAM	4 GB	4 GB	4 GB	4 GB
Processor	1X single core	1X dual core	2X dual core	2X quad core
Disk	2X 250 GB	2X 300 GB	4X 300 GB	6X 300 GB
RAID	RAID 1	RAID 1	RAID 10	RAID 10
Power Supply	Single	Redundant	Redundant	Redundant
Interfaces	2X Gigabit Ethernet	3X Gigabit Ethernet	3X Gigabit Ethernet	3X Gigabit Ethernet and 2X+M286 fiber-optic

Email Messaging Security: Barracuda Networks

D. Barracuda Sales Tactics

- Barracuda competes on low pricing rather than overall total cost of ownership (TCO) or product quality and effectiveness. With Cisco IronPort, customers receive excellent spam capture rates, fewer false positives, exceptional performance, higher availability, and innovative cutting-edge technology. The overall savings in operating expenditures (OpEx) can outweigh the difference in capital expenses (CapEx) due to price, thereby reducing the overall TCO.
- Barracuda may suggest the level of performance provided by Cisco IronPort is not required for small and medium-sized businesses (SMBs). However, spam volumes have doubled each year between 2006 and 2008. Cisco IronPort appliances can scale to handle the future volume of mail, will not need additional appliances as quickly, and help ensure a high quality of service to all email users, even during significant spam outbreaks.
- Barracuda may suggest that Cisco IronPort is focused on large enterprises and Internet service providers (ISPs). The Cisco IronPort vision is to offer an enterprise-class solution for all customers. Product bundles for the Cisco IronPort C160 appliances are designed for SMBs.

E. Barracuda Spam Firewall Weaknesses

- Barracuda uses the open source SpamAssassin engine, which spammers may have the capability to reverse engineer to bypass its detection. Barracuda requires administrators to constantly modify and add new scanning rules to catch spam that the Barracuda engine may miss, which leads to higher overall TCO and more time spent managing equipment.
- Barracuda supports basic real-time black lists (RBLs), but only limited reputation service and throttling.
- Barracuda solutions may not be able to scale to handle tens of thousands of connections, so more devices may be required to handle the same amount of mail, increasing the administrative burden and the overall TCO.
- Barracuda offers relatively basic attachment blocking and keyword scanning.
- For the most part, Barracuda appliances can handle only a fraction of the mail that Cisco IronPort can.

NOTES

Email Messaging Security: Google Apps and Postini

II. Google Apps and Postini

A. Google Company Overview

Google Inc. maintains an index of websites and other online content for users, advertisers, Google network members, and other content providers. Its automated search technology helps users instantly access relevant information from its online index. The company provides targeted advertising and Internet search solutions, as well as intranet solutions via an enterprise search appliance. Its products and services include Google.com for search and personalization, which provides Google Web Search, Google Image Search, Google Book Search, Google Scholar, Google Finance, Google News, Google Video, Google Blog Search, iGoogle and Personalized Search, Google Product Search, Google Custom Search, Google Base, and Google Webmaster Tools.

The company also offers Google Docs, Google Calendar, Gmail, Google Groups, Google Reader, orkut, Blogger, Google Sites, and YouTube. In addition, it offers Google Toolbar, Google Chrome, Google Pack, Picasa, and Google Desktop for users. The Google GEO product line comprises Google Earth, Google Maps, and Google Sketchup and Sketchup Pro, as well as Google Checkout, an online shopping service. Further, the company provides the Google Mobile product line for users to search and view the mobile web, the Google index, and maps and satellite imagery; and Google Labs, a test bed for engineers and Google users. Additionally, it offers Google AdWords, an auction-based advertising program; the Google AdSense program for content owners; and a Display advertising program that delivers branded display advertising services. The company also offers a Google Enterprise product line comprising Google Apps, which provides hosted communication and collaboration tools for businesses, schools, and nonprofit organizations; and Google Mini and Google Search Appliance products for small and medium-sized businesses. Google, Inc. was founded in 1998 and is headquartered in Mountain View, California.

B. Google Financial Profile

http://finance.yahoo.com/q/pr?s=GOOG

Table 46: Google Financial Profile

Google Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	21,795,550	16,593,986	10,604,917
Cost of Revenue	8,621,506	6,649,085	4,225,027
Gross Profit	13,174,044	9,944,901	6,379,890
Research Development	2,793,192	2,119,985	1,228,589
Selling General and Administrative	3,748,883	2,740,516	1,601,305
Operating Income or Loss	**6,631,969**	**5,084,400**	**3,549,996**
Number of Employees	19,665	19,156	No information

C. Google Product Guide

Table 47: Google Products

Google Products		
Competitors	Google Apps and Postini	Cisco IronPort Hosted and Hybrid Hosted Email Security Services
Email Reputation		
Email Reputation Filters	No information[3]	Yes
Organizations and Sources Providing Information to Reputation Service	No information	More than 100,000
Rate-Limiting of Suspected Spam Senders	No information	Yes
Percentage of Incoming Email Blocked by Reputation (at the connection level)	No information	More than 90%
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	Yes	Yes
Antivirus Scan Engine	Yes	Yes
Fully Integrated On-Device Scan Engines	Not applicable[4]	Yes
Virus Outbreak Filters (or equivalent)	No	Yes
Data Loss Prevention (DLP) Features		
Integrated DLP Scanning Capabilities	Limited	Yes, including remediation
Number of File Types Supported for Embedded Scanning	No information	More than 400
Support for Smart Identifiers (credit card numbers, social security numbers [SSNs], etc.)	Yes	Yes
Email Encryption		
Fully Integrated Email Encryption	No, transport layer security (TLS) only[5]	Yes
No Additional Software Required on End-User Systems for Encryption	No information	Yes
Managed Key Storage and Recovery Service	No information	Yes, Cisco Registered Envelope Service

[3] Google Apps does not disclose whether this type of service is provided.
[4] Scanning is performed within the hosted service.
[5] Other options are available to provide encryption.

Email Messaging Security: Google Apps and Postini

Table 47: Google Products

Google Products (continued)		
Competitors	Google Apps and Postini	Cisco IronPort Hosted and Hybrid Hosted Email Security Services
Platform Features		
Bounce Verification Filters	No	Yes
Outbound Email Scanning	Yes[6]	Yes
Support for Filtering Policies Based on Lightweight Directory Access Protocol (LDAP) Group	Limited	Yes, using Cisco IronPort Hybrid Hosted solution
Custom Purpose-Built Operating System	No information	Yes
Multicore Chip Support	No information	Yes
Email Authentication Support	DKIM, SPF, and SIDF	DKIM, SPF, and SIDF
Obscene-Image Blocking	No	Yes
High-Performance, Custom Media Terminal Adapter (MTA)	No information	Yes

6: Add-on feature at additional cost.

Table 48: Google Hardware Specifications

Google Hardware Specifications		
Products	Google and Postini Service	Cisco IronPort Hosted and Hybrid Hosted Email Security Services
Suggested Capacity	No information	1000 or more users
Uptime Guarantee (SLA)	99.9%	99.999%
Form Factor	No information	Appliance based
Shared Infrastructure	Yes. All users on shared system share the same fate	No. No shared-fate issues
Co-Management of Solution	No	Yes
Message Tracking	Must open a case with support	Customer has direct access to message tracking features
Image Analysis	No	Yes
Outbound Message Filtering	In cloud	On customer premises using Cisco IronPort Hybrid Hosted solution

D. Google Sales Tactics

- Google Apps has been discounted in comparison to the previous pricing for Postini. However, for organizations to get the features they want most, they often must pay the higher pricing, thereby nullifying the discount.
- Competing against third-party filtering services like Postini, also referred to as outsourcers, hosted services, or managed service providers (MSPs), offers a different challenge than competing against traditional software or appliance vendors:
  - A Google Apps or Postini customer running Microsoft Exchange will still require an onsite Mail Transfer Agent (MTA) to receive email.
  - The decision to outsource email filtering is sometimes made at the CIO level and pushed downward, with little or no consideration of the technical feasibility of implementation.
  - Third-party filtering services stress the importance of their service-level agreements (SLAs) more than technical features. Lack of technical features makes the TCO much higher in the long run.
- The decision to choose a third-party filter is often made after dealing with a poorly performing email security product. Google may incorrectly try to position Cisco IronPort in this group. Cisco IronPort appliances are easy to use and are not prone to the same shortfalls as other email appliances.

E. Google Weaknesses

- Google Apps and Postini rely on user white lists to keep from losing important email rather than maintaining a low false positive rate.
- Google Apps filters perform basic reputation filtering at their gateways (using Postini Threat Identification Network [PTIN]), but their network visibility is limited to their customer base, whereas Cisco IronPort SenderBase sees more than 25% of all email traffic.
- Google Apps filters offer few capabilities for recipient validation and DHAP control. Some customers have seen up to 80% of all email delivered from third parties as addressed to invalid recipients, which can cause significant overhead for back-end groupware servers.
- If a single Google Apps email customer is subject to a denial-of-service (DoS) attack, all customers are affected.
- Customers suffer from shared fate outages – If maintenance fails, incorrect settings get applied, or users get blackslisted, then all users on the shared systems are affected.
- If an email is lost or blocked by filters then customers must open a case and wait for support to track messages. Customers have co-management of Cisco IronPort Hosted Services which gives them direct access to message tracking features and no waiting.
- Google Apps provides virus protection through multiple reactive antivirus engines, but does not offer a preventive solution like Cisco IronPort Virus Outbreak Filters.
- Google Apps does not support bounce verification.
- Google Apps provides basic content security capabilities similar to those of Cisco IronPort, but it may be difficult or impossible to apply different content policies to different user groups.
- Google Apps management tools take care of only email filtering, archiving, and encryption. Administrators still need to manage local SMTP infrastructure gateways.

Email Messaging Security: Microsoft Forefront

III. Microsoft Forefront

A. Microsoft Company Overview

Microsoft Corporation, incorporated in 1981 and located in Redmond, Washington, develops, manufactures, licenses, and supports a range of software products for computing devices. The company's software products include operating systems for servers, PCs, and intelligent devices; server applications for distributed computing environments; information worker productivity applications; business solution applications; high-performance computing applications; and software development tools.

The server and tools segment also provides training and certification to developers and IT professionals for Microsoft's server and client platform products. The server and tools segment includes the enterprise partner group, which is responsible for sales, partner management, and partner programs for medium-sized and large organizations; and the public-sector sales and marketing department. Microsoft's products in the server and tools segment include the Windows Server operating system, Microsoft SQL Server, Microsoft Enterprise Services, product support services, Visual Studio, System Center products, Forefront Security products, Biz Talk Server, Microsoft Developer Network (MSDN), and TechNet.

B. Microsoft Financial Profile

Table 49: Microsoft Financial Profile

Microsoft Financial Profile

	2009	2008	2007
Dollars in Millions			
Total Revenue	58,437,000	60,420,00	51,122,000
Cost of Revenue	12,155,000	11,598,000	10,693,000
Gross Profit	46,282,000	46,282,000	40,429,000
Research Development	9,010,000	8,164,000	7,121,000
Selling General and Administrative	16,579,000	18,166,000	14,784,000
Operating Income or Loss	**20,363,000**	**22,492,000**	**18,524,000**
Number of Employees	93,000	79,000	No information

C. Microsoft Product Guide

Table 50: Microsoft Products

Microsoft Products

Competitors	Microsoft Forefront	Cisco IronPort Hosted and Hybrid Hosted Email Security Services
Email Reputation		
Email Reputation Filters	Add-on feature; only in edge transport role	Yes
Organizations and Sources Providing Information to Reputation Service	Unspecified	More than 100,000
Rate-Limiting of Suspected Spam Senders	No[7]	Yes
Percentage of Incoming Email Blocked by Reputation (at the connection level)	Unspecified	90+%
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	Yes	Yes
Antivirus Scan Engine	Yes	Yes
Fully Integrated On-Device Scan Engines	Non-native; requires handoff to licensed scanner	Yes
Virus Outbreak Filters (or equivalent)	Limited[8]	Yes
Data Loss Prevention (DLP) Features		
Integrated DLP Scanning Capabilities	No	Yes, including remediation
Number of File Types Supported for Embedded Scanning	No information	More than 400
Support for Smart Identifiers (credit card numbers, social security numbers [SSNs], etc.)	No information	Yes
Email Encryption		
Fully Integrated Email Encryption	No[9]	Yes
No Additional Software Required on End-User Systems for Encryption	Only with zero download messenger	Yes
Managed Key Storage and Recovery Service	Yes, with key limitations	Yes, Cisco Registered Envelope Service; no key limitations

[7] In Microsoft Exchange edge role.

[8] Microsoft states that these filters should be used only in a major emergency because of the effect on performance.

[9] Microsoft uses the original equipment manufacturer (OEM) Voltage product for encryption and provides this product through the Frontbridge service.

Email Messaging Security: Microsoft Forefront

Table 50: Microsoft Products

Microsoft Products (continued)		
Competitors	Microsoft Forefront	Cisco IronPort Hosted and Hybrid Hosted Email Security Services
Platform Features		
Bounce Verification Filters	No	Yes
Outbound Email Scanning	No[10]	Yes
Support for Filtering Policies Based on Lightweight Directory Access Protocol (LDAP) Group	Yes	Yes
Custom Purpose-Built Operating System	No	Yes
Multicore Chip Support	Yes	Yes
Email Authentication Support	SPF and SIDF	DKIM, SPF, and SIDF
Obscene-Image Blocking	No	Yes
High-Performance, Custom Media Terminal Adapter (MTA)	Limited; non-email-specific OS	Yes

[10] Outbound scanning is provided in the Microsoft Exchange hub transport role.

Table 51: Microsoft Hardware Specifications

Microsoft Hardware Specifications		
Products	Forefront	Cisco IronPort Hosted and Hybrid Hosted Email Security Services
Suggested Capacity	No information	1000 or more
Uptime Guarantee (SLA)	99.999%	99.999%
Form Factor	No information	Appliance based
Shared Infrastructure	Yes. All users on shared system share the same fate	No. No shared-fate issues
Co-Management of Solution	No	Yes
Message Tracking	Customer has direct access to message tracking features	Customer has direct access to message tracking features
Image Analysis	No	Yes
Outbound Message Filtering	In cloud	On customer premises using Cisco IronPort Hybrid Hosted solution

Contents based on publicly available information current as of December 2009.

D. Microsoft Sales Tactics

- Microsoft will often offer a bundled licensing deal that is fairly low in initial cost. However, given the number of servers required to obtain the same level of protection as a Cisco IronPort C-Series solution and the added burden of administration and weak spam catch rates, the post-implementation cost can be significantly more.
- Microsoft may suggest that it is better to have a single vendor for all email infrastructure needs. However, a potential customer that understands the need for best-in-class products for critical services like email, will see through this approach. Because the Microsoft email security model is relatively new in the market, and has been brought together as a result of various acquisitions, the overall service may be segmented and unrefined, possibly requiring several years to mature and prove its value.

E. Microsoft Weaknesses

- In various press reviews and third-party tests, Microsoft's spam catch rate is exceedingly low (around 80%). Furthermore, the false-positive rate is often around 100 times that of Cisco IronPort.
- Microsoft provides virus protection through multiple reactive antivirus engines, but does not offer a preventive solution like Cisco IronPort Virus Outbreak Filters.
- Microsoft does not support bounce verification.
- The Microsoft offering is pieced together from various acquisitions and may contain different types of user interfaces and use inconsistent nomenclature. Thus, the Microsoft product line was not originally designed as a complete, fully integrated solution.
- Third-party testing has shown the Microsoft offering to have a high level of false positives, which can result in more administrator intervention to maintain end-user email. If customers desire a DLP solution to filter outbound emails then they will still need an IronPort solution. Hybrid Hosted services from Cisco IronPort can be positioned to take care of both outsourced email needs and outbound DLP requirements.

Email Messaging Security: McAfee

IV. McAfee

A. McAfee Company Overview

For full McAfee company overview see page 94.

B. McAfee Financial Profile

For full McAfee financial data see page 95.

Table 52: McAfee Financial Profile

McAfee Financial Profile			
	2008	2007	2006
Dollars in Millions			
Total Revenue	1,600,065	1,308,220	1,145,158
Cost of Revenue	383,528	305,744	246,840
Gross Profit	1,216,537	1,002,476	898,318
Research Development	252,020	217,934	193,447
Selling General and Administrative	730,728	569,384	536,148
Operating Income or Loss	**189,571**	**159,813**	**139,028**
Number of Employees	5600		

C. McAfee Product Guide

Table 53: McAfee Products

McAfee Products		
Competitors	McAfee Email Gateway (Formerly IronMail)	Cisco IronPort C-Series
Email Reputation		
Email Reputation Filters	No, requires additional edge appliance	Yes
Organizations and Sources Providing Information to Reputation Service	Fewer than 8000	More than 100,000
Rate-Limiting of Suspected Spam Senders	No	Yes
Percentage of Incoming Email Blocked by Reputation (at the connection level)	50%	90+%
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	No information	Yes
Antivirus Scan Engine	Yes	Yes
Fully Integrated On-Device Scan Engines	Yes	Yes
Virus Outbreak Filters (or equivalent)	Limited; often requires administrator intervention	Yes
Data Loss Prevention (DLP) Features		
Integrated DLP Scanning Capabilities	Some	Yes, including remediation
Number of File Types Supported for Embedded Scanning	Approximately 60	More than 400
Support for Smart Identifiers (credit card numbers, social security numbers [SSNs], etc.)	Limited; dictionary or custom only	Yes
Email Encryption		
Fully Integrated Email Encryption	Yes, using SMIME or Pretty Good Privacy (PGP)	Yes
No Additional Software Required on End-User Systems for Encryption	No, requires client software	Yes
Managed Key Storage and Recovery Service	No information	Yes, Cisco Registered Envelope Service

Email Messaging Security: McAfee

Table 53: McAfee Computing Products

McAfee Products (continued)

Competitors	McAfee Email Gateway (formerly IronMail)	Cisco IronPort C-Series
Platform Features		
Bounce Verification Filters	No	Yes
Outbound Email Scanning	Yes	Yes
Support for Filtering Policies Based on Lightweight Directory Access Protocol (LDAP) Group	Yes	Yes
Custom Purpose-Built Operating System	Yes	Yes
Multicore Chip Support	Yes	Yes
Email Authentication Support	DKIM, SPF, and SIDF	DKIM, SPF, and SIDF
Obscene-Image Blocking	Yes	Yes
High-Performance, Custom Media Terminal Adapter (MTA)	Limited; requires edge device for high-traffic sites	Yes

Table 54: McAfee Computing Hardware Specifications

McAfee Hardware Specifications

Products	S10	S120	EG-5000	EG-5500
Suggested Capacity	No information	No information	No information	No information
Form Factor	1RU	1RU	1RU	2RU
RAM	2 GB	4 GB	6 GB	12 GB
Processor	1X single core	1X Core2Duo	1X quad core	2X quad core
Disk	1X 160 GB	1X 160 GB	1X 300 GB	1X 800 GB
RAID	None	RAID 1	RAID 1	RAID 10
Power Supply	Single	Single	Redundant	Redundant
Interfaces	2X Gigabit Ethernet	2X Gigabit Ethernet	4X Gigabit Ethernet	4X Gigabit Ethernet

McAfee Hardware Specifications

Products	IronPort C160	IronPort C360	IronPort C660	IronPort X1060
Suggested Capacity	100 to 1000 users	1000 to 10,000 users	10,000 or more users	Carrier or ISP
Form Factor	1RU	2RU	2RU	2RU
RAM	4 GB	4 GB	4 GB	4 GB
Processor	1X single core	1X dual core	2X dual core	2X quad core
Disk	2X 250 GB	2X 300 GB	4X 300 GB	6X 300 GB
RAID	RAID 1	RAID 1	RAID 10	RAID 10
Power Supply	Single	Redundant	Redundant	Redundant
Interfaces	2X Gigabit Ethernet	3X Gigabit Ethernet	3X Gigabit Ethernet	3X Gigabit Ethernet and 2X fiber-optic

Contents based on publicly available information current as of December 2009.

Email Messaging Security: McAfee

D. Mcafee Sales Tactics

- McAfee may claim that TrustedSource is more effective than Cisco IronPort SenderBase as a reputation system. See the statistics on reputation effectiveness listed earlier. Furthermore, Cisco IronPort has many reference customers who have moved from the McAfee Secure Mail/ McAfee Email Security Gateway to Cisco IronPort. Show examples of approved customer references to prospects to let them know who has moved to Cisco IronPort.
- McAfee may heavily discount products to close the deal, especially in accounts where they are the incumbent anti-virus provider. However, more Email Security Gateway devices are often needed to transfer the same amount of email as Cisco IronPort. Furthermore, the customer may have to purchase the edge device if they want to use the reputation service offered by McAfee. Suggest that the customer test both products with heavy email volumes. This test may make clear that Cisco IronPort has the superior performance, and save the customer the costs of future appliances, email delays, and other scalability problems.
- Ask potential customers if they have compared Cisco IronPort support to that of McAfee. Cisco IronPort provides exceptional support and takes pride in the quality of our support.

E. McAfee Weaknesses

- McAfee's customers may spend much time working around inaccurate spam filters of Email Security Gateway's and still lose important business messages
- The TrustedSource reputation filtering system is much smaller and can be much less effective than the industry-leading Cisco IronPort SenderBase. Furthermore, customers often find that only 50% of incoming spam is blocked by reputation compared to 90+% by Cisco IronPort.
- Email Security Gateway can validate recipients against LDAP, but cannot rate limit the attackers.
- Email Security Gateway outbreak protection often requires direct administrator intervention and manual updates.
- Email Security Gateway appliances can handle only a fraction of the mail that Cisco IronPort can; therefore, more appliances are needed to handle the same email volume.

NOTES

Email Messaging Security: Symantec

V. Symantec

A. Symantec Company Overview

For full Symantec overview see page 122.

B. Symantec Financial Profile

For full Symantec financial data see page 122.

C. Symantec Product Guide

Table 55: Symantec Products

Symantec Products

Competitors	Symantec Brightmail 8300 Series	Cisco IronPort C-Series
Email Reputation		
Email Reputation Filters	Limited; tracks only local data[11]	Yes
Organizations and Sources Providing Information to Reputation Service	Single appliance (no global reputation)	More than 100,000
Rate-Limiting of Suspected Spam Senders	No	Yes
Percentage of Incoming Email Blocked by Reputation (at the connection level)	Unspecified	90+%
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	Yes	Yes
Antivirus Scan Engine	Yes	Yes
Fully Integrated On-Device Scan Engines	Yes	Yes
Virus Outbreak Filters (or equivalent)	Limited	Yes
Data Loss Prevention (DLP) Features		
Integrated DLP Scanning Capabilities	Yes	Yes
Number of File Types Supported for Embedded Scanning	No information	More than 400
Support for Smart Identifiers (credit card numbers, social security numbers [SSNs], etc.)	Yes	Yes
Email Encryption		
Fully Integrated Email Encryption	TLS only	Yes
No Additional Software Required on End-User Systems for Encryption	No information	Yes
Managed Key Storage and Recovery Service	No information	Yes, Cisco Registered Envelope Service

[11] 11: Provides limited reputation service and applies only rate limiting.

Table 55: Symantec Products

Symantec Products (continued)

Competitors	Symantec Brightmail 8300 Series	Cisco IronPort C-Series
Platform Features		
Bounce Verification Filters	Yes	Yes
Outbound Email Scanning	Yes	Yes
Support for Filtering Policies Based on Lightweight Directory Access Protocol (LDAP) Group	Yes	Yes
Custom Purpose-Built Operating System	No, based on Linux	Yes
Multicore Chip Support	Yes	Yes
Email Authentication Support	No information	DKIM, SPF, and SIDF
Obscene-Image Blocking	No	Yes
High-Performance, Custom Media Terminal Adapter (MTA)	No, based on Postfix	Yes

Table 56: Symantec Hardware Specifications

Symantec Hardware Specifications

Products	Brightmail Gateway 8340	Brightmail Gateway 8360	Brightmail Gateway 8380	IronPort C160	IronPort C360	IronPort C660	IronPort X1060
Suggested Capacity	Up to 1000 users	No information	No information	100 to 1000 users	1000 to 10,000 users	10,000 or more users	Carrier or ISP
Form Factor	1RU	1RU	2RU	1RU	2RU	2RU	2RU
RAM	2 GB	4 GB	4 GB	4 GB	4 GB	4 GB	4 GB
Processor	1X single core	2X multicore	2X multicore	1X single core	1X dual core	2X dual core	2X quad core
Disk	2X 80 GB	2X 146 GB	6X 300 GB	2X 250 GB	2X 300 GB	4X 300 GB	6X 300 GB
RAID	RAID 1	RAID 1	RAID 10	RAID 1	RAID 1	RAID 10	RAID 10
Power Supply	Single	Redundant	Redundant	Single	Redundant	Redundant	Redundant
Interfaces	2X Gigabit Ethernet	2X Gigabit Ethernet	3X Gigabit Ethernet	2X Gigabit Ethernet	3X Gigabit Ethernet	3X Gigabit Ethernet	3X Gigabit Ethernet and 2X fiber-optic

Contents based on publicly available information current as of December 2009.

Email Messaging Security: Symantec

D. Symantec Sales Tactics

- Symantec may claim that Local Reputation is an effective reputation system and compare it to Cisco IronPort SenderBase. The Local Reputation system is limited to spam seen before on that single appliance and does not provide the global knowledge of spam senders that Cisco IronPort SenderBase does.
- Symantec has no throttling capabilities; only blacklist-style block and accept decisions are allowed, creating high false-positive rates for email from Internet Service Providers (ISPs) and large web email providers.
- Symantec offers hardware at a deep discount to lock in long-term subscription pricing, especially in accounts in which they are the incumbent antivirus vender. The company has also been known to dramatically discount Brightmail and offers package pricing for sites that deploy Brightmail at the gateway and Symantec AntiVirus at all levels. However, customers are still choosing Cisco IronPort because of its technical superiority.

E. Symantec Weaknesses

- Symantec's spam detection network and rule-writing operations often take 24 hours or more to respond to new spam outbreaks, allowing large amounts of unwanted messages (particularly new varieties of image spam) to leak through the Brightmail filters.
- Symantec uses Linux and Postfix, which cannot scale to tens of thousands of connections.
- Symantec's latest release has zero-day virus protection, but it is based on the Symantec AntiVirus probe network and does not offer true defense-in-depth.
- Symantec's cluster management function only replicates provisioning data and cannot actually manage remote appliances as is possible with the Cisco IronPort C-Series.

NOTES

NOTES

Web/URL Filtering

Companies	Sections in Each Company Guide
I. Barracuda Networks	A. Company Overview
II. Blue Coat Systems	B. Financial Profile
III. Finjan	C. Product Guide
IV. McAfee	D. Sales Tactics
V. Websense	E. Weaknesses

Web/URL Filtering: Barracuda Networks

I. Barracuda Networks

A. Barracuda Overview

For full Barracuda overview see page 162.

B. Barracuda Financial Profile

For full Barracuda financial data see page 162.

C. Barracuda Product Guide

Table 57: Barracuda Products

Barracuda Products

Competitors	Barracuda	Cisco IronPort S-Series
Web Reputation		
Web Reputation System and Filters	No	Yes
Global Threat Correlation System Powered by Web, Email, and Intrusion Prevention System (IPS)	Email and web only	Yes
Daily Threat Data Volume	50,000	500 GB
Web 2.0 Exploit Filtering	No	Yes
Internal Bot and Zombie Detection	Limited	Yes
URL Outbreak Protection	No	Yes
Administrator-Defined Policy Based on Risk Level	No	Yes
Flexibility to Use Web Reputation in Other Policy Areas, Such as HTTPS Decrypt Decision	No	Yes
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	Yes	Yes
Antivirus Scan Engine	Yes	Yes
Fully Integrated On-Device Scan Engines	Yes	Yes
Parallel Multiscaning Engine	No	Yes
Stream Scanning	No	Yes
Outbound Malware Phone-Home Detection on All Ports	HTTP only	All 65,535 ports
Suspect User Agent Detection	No	Yes
HTTPS Secure Sockets Layer (SSL) Content Inspection	No	Yes

Barracuda Products (continued)

Competitors	Barracuda	Cisco IronPort S-Series
Acceptable Use Policy Enforcement		
URL Filtering	Yes	Yes
Real-Time Content Analysis Engine	No	Yes
Instant Messaging (IM) and Peer-to-Peer (P2P)	Yes	Yes
Data Security		
Integrated Data Security Policy Enforcement	No	Yes
Outbound Content Controls	No	Yes
Offbox Interoperability with Data Loss Prevention (DLP) Vendors	No	Yes
Platform Features		
Integrated Threat Reporting and Alerting	Yes	Yes
Custom Purpose-Built Operating System	Modified Linux	Yes
Proxy Performance Configuration Features	Yes	Yes
Native HTTPS	No	Yes
Native FTP	No	Yes
Deployment Modes		
Explicit Forward Mode	Yes	Yes
Transparent Mode (Web Cache Communications Protocol [WCCP])	Yes	Yes
Physical Inline, Bridge, and Passthrough Mode	Yes	No

Web/URL Filtering: Barracuda Networks

Table 58: Barracuda Hardware Specifications

Barracuda Hardware Specifications							
Products	610	810	910	1010	IronPort S160	IronPort S360	IronPort S660
Suggested Capacity[1]	1500 users	3000 users	4500 users	12,000 users	1000 users	5000 users	More than 5000 users
Form Factor	1 rack unit (RU)	2RU	2RU	Unspecified	1RU	2RU	2RU
RAM	Unspecified	Unspecified	Unspecified	Unspecified	4 GB	4 GB	8 GB
Processor	Unspecified	Unspecified	Unspecified	Unspecified	1X2 (1 dual core) Pentium	1X4 (1 quad core) Xeons	2X4 (2 quad cores) Xeons
Disk	Unspecified	Unspecified	Unspecified	Unspecified	500 GB	1.2 TB	1.8 TB
RAID	Yes	Yes	Yes	Yes	No	Yes	Yes
Redundant Power Supply	No	Yes	Yes	Yes	No	Yes	Yes
Interfaces	2X Gigabit Ethernet	2X Gigabit Ethernet	2X Gigabit Ethernet	2X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet

1: Specifications subject to change.
Contents based on publicly available information current as of September 2009.

D. Barracuda Sales Tactics

- Barracuda uses mass marketing (often at airports) as one primary form of marketing. This approach can result in strong name recognition without much understanding of the underlying product. Respond to this by pointing out the overall total cost of ownership (TCO) of a Cisco IronPort™ S-Series solution compared to the Barracuda solution. The Cisco IronPort S-Series is a top-of-the-line, best-in-class security appliance, thus reducing the residual costs of cleanup, support calls, and maintenance.
- If a customer is evaluating both Cisco IronPort and Barracuda solutions, recommend that the customer run the evaluation appliances in parallel to see that the Cisco IronPort solution reports on spyware and virus traffic that the Barracuda device does not catch. Focus on reliability, efficacy, and performance and the fact that the Cisco IronPort S-Series contains best-in-class scanners for spyware (Webroot) and all other malware (McAfee).
- Barracuda pricing often appeals to price-sensitive customers. However, the customer may not consider the residual costs of downtime, slow performance, missed malware detection, and cleanup.
- With legitimate sites being compromised and serving malware, customers need a web reputation service. Explain how Cisco IronPort Web Reputation can protect the customer from this new threat as well as from malicious websites hosted on botnets and second-generation phishing attacks.
- With the proliferation of Web 2.0 blogs and social networking sites, customers need to take quick, easy steps to enforce common-sense data security policies to prevent data leakage. Explain how Cisco IronPort data security policies can be created for outbound traffic on HTTP, HTTPS, and FTP. For enterprises that have already invested in special-purpose DLP systems, the Cisco IronPort S-Series offers an option to interoperate with DLP vendors via the Internet Content Adaptation Protocol (ICAP). This enables deep content inspection for regulatory compliance and intellectual property protection, incident severity definition, case management, and performance optimization.

E. Barracuda Weaknesses

- Barracuda offers no granular URL threat database like the Cisco IronPort Reputation Filters.
- Unlike the Cisco IronPort S-Series, Barracuda solutions cannot scan inside HTTPS, SSL, and native FTP connections for malware.
- Barracuda's spyware signatures are sometimes developed by open source volunteers on the Internet and can be delayed and inaccurate. Cisco IronPort provides two best-in-class malware scanners.
- Barracuda's web proxy is not designed for high loads. The company has not built a custom file system or networking system like the Cisco IronPort S-Series in order to handle massive data throughput and a large number of simultaneous connections. Thus, the Barracuda web filter can introduce noticeable latency into the end-user web experience.

Web/URL Filtering: Blue Coat Systems

II. Blue Coat Systems

A. Blue Coat Company Overview

Blue Coat Systems, Inc. engages in the design, development, and sale of proxy appliances and related software and services that optimize and secure the delivery of business applications and other information to distributed users over a WAN or the public Internet/web. Its secure web gateway products include the ProxySG appliance to provide virus scanning and to give the IT administrator visibility into and control of enterprise web communications; the ProxyAV family of web antivirus appliances for enterprises to scan for viruses, worms, spyware, and Trojans at the Internet gateway; and WebFilter, a content filtering database to protect enterprise and service provider users and networks from Internet threats and inappropriate content and traffic.

The company's WAN optimization products include ProxySG client software, which serves as the foundation for secure web gateway products and WAN optimization offerings; ProxyRA appliances to enable authorized mobile users to securely connect to a corporate network through a mobile client device; reporter software to collect transaction log data; and a director appliance to manage an enterprise's Blue Coat ProxySG appliances. Its application performance monitoring products include the PacketShaper appliance to provide granular visibility into network utilization and application performance; PolicyCenter software to enable IT administrators to manage the configuration, policy management, software distribution, and adaptive response tracking of various PacketShaper appliances; and IntelligenceCenter software to provide application performance monitoring for PacketShaper appliances deployed in various enterprises. The company was formerly known as CacheFlow, Inc. and changed its name to Blue Coat Systems, Inc. in August 2002. Blue Coat Systems, Inc. was founded in 1996 and is headquartered in Sunnyvale, California.

B. Blue Coat Financial Profile

Table 59: Blue Coat Financial Profile

Blue Coat Financial Profile

	2008	2007	2006
Dollars in Millions			
Total Revenue	444.75	177,700	141,722
Cost of Revenue	131.14	45,748	43,048
Gross Profit	313.61	131,952	98,674
Research Development	76.68	39,882	26,785
Selling General and Administrative	226.15	101,155	66,422
Operating Income or Loss	**311.04**	**-9685**	**1509**
Number of Employees	1481	708	No Info

C. Blue Coat Product Guide

Table 60: Blue Coat Products

Blue Coat Products

Competitors	Blue Coat	Cisco IronPort S-Series
Web Reputation		
Web Reputation System and Filters	No[2]	Yes
Global Threat Correlation System Powered by Web, Email, and Intrusion Prevention System (IPS)	No	Yes
Daily Threat Data Volume	WebPulse analyzes 150 million URLs per day[3]	500 GB
Web 2.0 Exploit Filtering	Limited; available through URL categories only	Yes
Internal Bot and Zombie Detection	Limited; available through URL categories only	Yes
URL Outbreak Protection	No	Yes
Administrator-Defined Policy Based on Risk Level	No	Yes
Flexibility to Use Web Reputation in Other Policy Areas, Such as HTTPS Decrypt Decision	No	Yes
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	No; requires ProxyAV[4]	Yes
Antivirus Scan Engine	No; requires ProxyAV	Yes
Fully Integrated On-Device Scan Engines	No; requires ProxyAV	Yes
Parallel Multiscaning Engine	No	Yes
Stream Scanning	No	Yes
Outbound Malware Phone-Home Detection on All Ports	No	All 65,535 ports
Suspect User Agent Detection	Some	Yes
HTTPS Secure Sockets Layer (SSL) Content Inspection	Yes	Yes
Acceptable Use Policy Enforcement		
URL Filtering	Yes	Yes
Real-Time Content Analysis Engine	Yes, off-box	Yes
Instant Messaging (IM) and Peer-to-Peer (P2P)	Yes	Yes

Web/URL Filtering: Blue Coat Systems

Table 60: Blue Coat Products

Blue Coat Products (continued)		
Competitors	Blue Coat	Cisco IronPort S-Series
Data Security		
Integrated Data Security Policy Enforcement	No	Yes
Outbound Content Controls	Yes	Yes
Offbox Interoperability with Data Loss Prevention (DLP) Vendors	Yes	Yes
Platform Features		
Integrated Threat Reporting and Alerting	Yes	Yes
Custom Purpose-Built Operating System	Yes	Yes
Proxy Performance Configuration Features	Yes	Yes
Native HTTPS	Yes	Yes
Native FTP	Yes	Yes
Deployment Modes		
Explicit Forward Mode	Yes	Yes
Transparent Mode (Web Cache Communications Protocol [WCCP])	Yes	Yes
Physical Inline, Bridge, and Passthrough Mode	Yes	No

2 Blue Coat claims that WebPulse is the dynamic real-time rating (DRTR) engine used for categorization of its URL filters.
3: The volume reported represents all URL categorization activities, not exclusive to security categories.
4: Malware scanning: Blue Coat SG appliances require an add-on antivirus appliance to conduct malware scanning. Malware scanning is handed off through the Internet Content AdaptationProtocol (ICAP), which can seriously affect performance.

Table 61: Blue Coat Hardware Specifications

Blue Coat Hardware Specifications					
Products	SG 810-25	SG 8100-30	IronPort S160	IronPort S360	IronPort S660
Suggested Capacity[5]	No information	No information	1000 users	5000 users	More than 5000 users
Form Factor	2 rack units (RU)	4RU	1RU	2RU	2RU
RAM	6 GB	16 GB	4 GB	4 GB	8 GB
Processor	Unspecified	Unspecified	1X2 (1 dual core) Pentium	1X4 (1 quad core) Xeons	2X4 (2 quad cores) Xeons
Disk	4X 300 GB	8X 300 GB	500 GB	1.2 TB	1.8 TB
RAID	Unspecified	Unspecified	No	Yes	Yes
Redundant Power Supply	Unspecified	Unspecified	No	Yes	Yes
Interfaces	Various	Various	6X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet

5: Specifications subject to change. The Cisco IronPort S100 is available for remote and branch offices.
Contents based on publicly available information current as of Oct 2009.

D. Blue Coat Sales Tactics

- Blue Coat may claim that the Cisco IronPort™ S-Series does not provide caching or performance-enhancing features. The Cisco IronPort AsyncOS operating system is specifically designed as a high-performance caching proxy. The cache-specific file system is designed to provide top performance during caching operations. The Cisco IronPort S-Series also organizes web objects on disk so that related items from the same page are stored close to each other on disk, resulting in very high performance when reading cached web pages.
- Blue Coat may attempt to shift focus from security to WAN optimization. Possibly because of previous failures in the security market (the Spyware Interceptor product that was pulled from the market) and the limited investment in new security technologies such as reputation systems and high-performance scanning, Blue Coat has decided to refocus on WAN optimization. Therefore, the company may attempt to shift its focus away from security and place it on optimization.
- With the proliferation of Web 2.0 blogs and social networking sites, customers need to take quick, easy steps to enforce common-sense data security policies to prevent data leakage. Explain how Cisco IronPort data security policies can be created for outbound traffic on HTTP, HTTPS, and FTP. For enterprises that have already invested in special-purpose DLP systems, the Cisco IronPort S-Series offers an option to interoperate with DLP vendors via ICAP. This enables deep content inspection for regulatory compliance and intellectual property protection, incident severity definition, case management, and performance optimization.

E. Blue Coat Weaknesses

- Blue Coat pulled its antispyware product from the marketplace, and its proxy platform lacks deep content scanning for spyware signatures and has no Layer 4 traffic monitor (L4TM).
- Blue Coat offers numerous old-style reactive URL filtering databases but has no preventive reputation filters such as those provided by Cisco IronPort.
- Blue Coat offers antivirus scanning only through a high-latency off-device antivirus appliance using ICAP. It provides no capabilities for deep content scanning for spyware signatures.
- Blue Coat does not watch outbound network traffic to determine which desktop machines might be infected with spyware.
- Unlike the Cisco IronPort S-Series, the Blue Coat solution doesn't offer on-box data security policies to prevent data leakage.

Web/URL Filtering: Finjan

III. Finjan

A. Finjan Company Overview

Finjan provides network security appliances and related software to protect enterprise data and web-based content. Finjan's security products protect against spyware, phishing, Trojans, malware, and viruses. Finjan's Vital Security appliance line includes models tailored to customers ranging in size from small businesses to large enterprises. Finjan also provides tiered technical support plans. Finjan was founded in 1996.

Press Release November 3, 2009: M86 Security, a global provider of web and messaging security products, today announced the acquisition of Finjan, a leading provider of secure web gateway solutions for the enterprise market. This acquisition adds Finjan's line of enterprise-class secure web gateway and software-as-a-service (SaaS)-based solutions to M86 Security's portfolio of email and web security solutions and significantly enhances the company's malware detection technology.

Under the terms of the agreement, M86 acquires Finjan's global operations, products, and technology, which merge into M86 Security effective immediately. The company will maintain a development center and operations in Netanya, Israel. M86 will also merge Finjan's security labs, Malicious Code Research Center, into M86 Security Labs, forming a comprehensive email and web threat research organization. As part of the agreement, M86 Security acquires a license to Finjan's patents.

M86 Security was formed by the November 2008 merger of Marshal and 8e6 Technologies. Finjan is the company's second acquisition in the last six months, following the March 2009 acquisition of behavioral malware detection company Avinti, Inc. The acquisition grows M86 Security's employee base to just more than 300 employees.

B. Finjan Financial Profile

Not available: Private company

C. Finjan Product Guide

Finjan Products

Competitors	M86 (Finjan)	Cisco IronPort S-Series
Web Reputation		
Web Reputation System and Filters	No	Yes
Global Threat Correlation System Powered by Web, Email, and Intrusion Prevention System (IPS)	No	Yes
Daily Threat Data Volume	No information	500 GB
Web 2.0 Exploit Filtering	No	Yes
Internal Bot and Zombie Detection	No	Yes
URL Outbreak Protection	No	Yes
Administrator-Defined Policy Based on Risk Level	No	Yes
Flexibility to Use Web Reputation in Other Policy Areas, Such as HTTPS Decrypt Decision	No	Yes

Table 62: Finjan Products

Finjan Products (continued)

Competitors	M86 (Finjan)	Cisco IronPort S-Series
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	No	Yes
Antivirus Scan Engine	Yes	Yes
Fully Integrated On-Device Scan Engines	Yes	Yes
Parallel Multiscaning Engine	No	Yes
Stream Scanning	No	Yes
Outbound Malware Phone-Home Detection on All Ports	Limited	All 65,535 ports
Suspect User Agent Detection	No	Yes
HTTPS Secure Sockets Layer (SSL) Content Inspection	Yes	Yes
Acceptable Use Policy Enforcement		
URL Filtering	Yes	Yes
Real-Time Content Analysis Engine	No	Yes
Instant Messaging (IM) and Peer-to-Peer (P2P)	Yes	Yes
Data Security		
Integrated Data Security Policy Enforcement	Yes	Yes
Outbound Content Controls	Yes	Yes
Offbox Interoperability with Data Loss Prevention (DLP) Vendors	Yes	Yes
Platform Features		
Integrated Threat Reporting and Alerting	Yes	Yes
Custom Purpose-Built Operating System	No	Yes
Proxy Performance Configuration Features	Some (varies by mode)	Yes
Native HTTPS	Yes	Yes
Native FTP	Yes	Yes
Deployment Modes		
Explicit Forward Mode	Yes	Yes
Transparent Mode (Web Cache Communications Protocol [WCCP])	Yes	Yes
Physical Inline, Bridge, and Passthrough Mode	Yes	No

Web/URL Filtering: Finjan

Table 63: Finjan Hardware Specifications

Finjan Hardware Specifications						
Products	NG-1100	NG-5100	NG-8100	IronPort S160	IronPort S360	IronPort S660
Suggested Capacity[6]	Up to 1000 users	1000 users	Up to 5000 users	1000 users	5000 users	More than 5000 users
Form Factor	1 rack unit (RU)	2 RU	No information	1RU	2RU	2RU
RAM	2 GB	4 GB	4 GB	4 GB	4 GB	8 GB
Processor	Dual-core Xeon E3120, 3.16 GHz	2X Intel Xeon quad-core E5506, 2.13 GHz	2X Intel Xeon quad-core E5506	1X2 (1 dual core) Pentium	1X4 (1 quad core) Xeons	2X4 (2 quad cores) Xeons
Disk	1X 160 GB SATA	2X 146 GB SAS	2X 146 GB SAS	500 GB	1.2 TB	1.8 TB
RAID	No information	Yes	No information	No	Yes	Yes
Redundant Power Supply	No information	No information	Yes	No	Yes	Yes
Interfaces	4X Gigabit Ethernet	4X Gigabit Ethernet	4X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet

[6]; Specifications subject to change.
Contents based on publicly available information current as of November 2009.

D. Finjan Sales Tactics

- Finjan may attempt to sell based on behavioral malware detection. Finjan uses application behavior to identify malware. This technology may effect performance, have a high false-positive rate, and significantly increase latency during Web browsing. Explain how Cisco IronPort developed concurrent multi-scanning to address these concerns and help ensure a high level of performance even during scanning.
- Finjan does not provide a Web reputation service and may deflect this by promoting its behavioral features. Explain the power of Cisco IronPort Web Reputation. With legitimate sites being compromised and serving malware, customers need Web reputation protection. Explain how Cisco IronPort Web Reputation can protect the customer from this new threat as well as from malicious Websites hosted on botnets and second-generation phishing attacks.
- Finjan will explain its behavioral technology and compare it to scanning and blocking. Behavioral protection currently belongs on the endpoint; it cannot perform and scale to be suitable on the gateway. Suggest that the customer test both Finjan and Cisco IronPort products with normal traffic loads or compare the latency statistics during fully burdened operation. This will make the superior performance of Cisco IronPort clear and save the customer from the costs of future appliances, Web browsing delays, and other scalability problems.

E. Finjan Weaknesses

- ICAP introduces a very high latency into the end-user's Web transaction because objects have to be read from the Internet, fed over the ICAP connection, and then finally transmitted to the end-user's Web browser. The Cisco IronPort approach adds just a few milliseconds of overhead to the scanning of large objects, while Finjan's approach can double or even triple transport time for the end user.
- The Finjan appliance uses behavioral detection techniques for much of its anti-spyware protection. This type of feature does not belong on a gateway device given the amount of traffic it must handle. This type of protection functions much better in an end-user desktop location since it must be continually monitored and often requires changes to reduce false positives or ask for user decisions.
- Finjan devices are not designed to scale like Cisco IronPort appliances. They implement costly and often ineffective behavioral technologies and require ICAP to provide a full solution. Some Finjan features come from the company's end-user products when, in fact, they really do not belong on gateway devices. Customers will experience these problems as a lack of performance and high latency on the appliance.

Web/URL Filtering: McAfee

IV. McAfee

A. McAfee Company Overview

For full McAfee overview see page 92.

B. McAfee Financial Profile

For full McAfee financial data see page 93.

C. McAfee Product Guide

Table 64: McAfee Computing Products

McAfee Products

Competitors	McAfee Web Gateway (formerly Webwasher)	Cisco IronPort S-Series
Web Reputation		
Web Reputation System and Filters	Yes	Yes
Global Threat Correlation System Powered by Web, Email, and Intrusion Prevention System (IPS)	Web and email only	Yes
Daily Threat Data Volume	No information	500 GB
Web 2.0 Exploit Filtering	No	
Internal Bot and Zombie Detection	Limited	Yes
URL Outbreak Protection	No	Yes
Administrator-Defined Policy Based on Risk Level	Yes	Yes
Flexibility to Use Web Reputation in Other Policy Areas, Such as HTTPS Decrypt Decision	No	Yes
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	No	Yes
Antivirus Scan Engine	Yes	Yes
Fully Integrated On-Device Scan Engines	Yes	Yes
Parallel Multiscaning Engine	No	Yes
Stream Scanning	Yes	Yes
Outbound Malware Phone-Home Detection on All Ports	No	All 65,535 ports
Suspect User Agent Detection	No	Yes
HTTPS Secure Sockets Layer (SSL) Content Inspection	Yes	Yes

McAfee Products (continued)

Competitors	McAfee Web Gateway (formerly Webwasher)	Cisco IronPort S-Series
Acceptable Use Policy Enforcement		
URL Filtering	Yes	Yes
Real-Time Content Analysis Engine	Limited	Yes
Instant Messaging (IM) and Peer-to-Peer (P2P)	Yes[7]	Yes
Data Security		
Integrated Data Security Policy Enforcement	Yes	Yes
Outbound Content Controls	Yes	Yes
Offbox Interoperability with Data Loss Prevention (DLP) Vendors	Yes	Yes
Platform Features		
Integrated Threat Reporting and Alerting	Yes	Yes
Custom Purpose-Built Operating System	Yes	Yes
Proxy Performance Configuration Features	No	Yes
Native HTTPS	Yes	Yes
Native FTP	Yes	Yes
Deployment Modes		
Explicit Forward Mode	Yes	Yes
Transparent Mode (Web Cache Communications Protocol [WCCP])	Yes	Yes
Physical Inline, Bridge, and Passthrough Mode	Yes	No

[7] Requires a separate IM appliance.

Web/URL Filtering: McAfee

Table 65 McAfee Hardware Specifications

McAfee Hardware Specifications							
Products	WW500E	WW1100E	WG-5000	WG-5500	IronPort S160	IronPort S360	IronPort S660
Suggested Capacity[8]	Up to 5000 users	Up to 10,000 users	No information	No information	1000 users	5000 users	More than 5000 users
Form Factor	1 rack unit (RU)	1RU	1RU	2RU	1RU	2RU	2RU
RAM	2 GB	2 GB	6 GB	12 GB	4 GB	4 GB	8 GB
Processor	Intel Celeron 440, 2 GHz	Intel Core2Duo E4500, 2.2 GHz	1X4 (1 quad core) Xeons	2X4 (2 quad cores) Xeons	1X2 (1 dual core) Pentium	1X4 (1 quad core) Xeons	2X4 (2 quad cores) Xeons
Disk	160 GB	2X 160 GB	2X 300 GB	6X 300 GB	500 GB	1.2 TB	1.8 TB
RAID	No information	No information	RAID 1	RAID 10	No	Yes	Yes
Power Supply	No	No	Yes	Yes	No	Yes	Yes
Interfaces	2X Gigabit Ethernet	4X Gigabit Ethernet	4X Gigabit Ethernet	4X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet

[8] Specifications subject to change.

Contents based on publicly available information current as of October 2009.

D. McAfee Sales Tactics

- McAfee may claim that TrustedSource is more effective than Cisco IronPort™ SenderBase® as a reputation system. However, Cisco IronPort has many reference customers who have moved from Secure Mail (now Email Security Gateway) to Cisco IronPort. Show examples of approved customer references to prospects to let them know who is moving to Cisco IronPort.
- McAfee may heavily discount the Web Gateway product, while at the same time bundling additional products (such as email security and IPS) for cost as an incentive to close the deal.
- Cisco IronPort provides exceptional support and takes pride in the quality of this support.

E. McAfee Weaknesses

- McAfee Web Gateway (formerly Webwasher) is mainly concerned with viruses coming into the network through downloaded code. Although it does watch outbound network traffic to determine which desktop machines might be infected with spyware, the detection is based on various properties (write to local file system and write to registry) that can be obfuscated or hidden. There is no specific antispyware signature database, so detection may fail or, worse, create a large number of false positives.
- McAfee Web Gateway provides support for multiple antivirus scanning engines; however, there is no specific malware engine (for detecting spyware, Trojans, keyloggers, and so on). Instead, administrators rely on proactive protection filtering.
- McAfee Web Gateway proactive protection features are potentially difficult to understand and provide many settings that can be insufficient for today's rich web applications. It relies on URL categorization identification, which may lead to both false positives and missed detections (through malware obfuscation).
- McAfee Web Gateway runs multiple antivirus engines in series. End users may complain because the resulting antivirus scanning can be slow.
- The McAfee Web Gateway management interface can be extremely complex; an administrator may have to navigate to multiple screens to configure a single policy.
- Users of McAfee Web Gateway may see false positives and performance effects, depending on the features enabled and the configuration. It includes some older and outdated features such as banner-ad blocking and manually created bad-cookie lists.

Web/URL Filtering: Websense, Inc.

V. Websense, Inc.

A. Websense Company Overview

Websense, Inc. provides integrated web, data, and email security solutions. The company offers web filtering and security, data loss prevention (DLP), and email anti-spam and security solutions that protect organizations' employees and critical business data from external web-based and email-based attacks, as well as from internal employee-generated threats, such as employee errors or malfeasance. Its portfolio of web filtering, web security, DLP, and email anti-spam and messaging security software allows organizations to prevent access to undesirable and dangerous elements on the web, such as websites that contain inappropriate content or sites that download viruses, spyware, keyloggers, and malicious code; identify and remove malicious applications from incoming web traffic; filter spam out of incoming email traffic; filter viruses and other malicious attachments from email and instant messages; manage the use of non-web Internet traffic, such as peer-to-peer communications and instant messaging; prevent the unauthorized use and loss of sensitive data, such as customer or employee information; and control misuse of an organization's valuable computing resources, including unauthorized downloading of high-bandwidth content.

The company's customers use its software products to provide a secure and productive computing environment for employees, business partners, and customers. It sells to customers primarily in the United States, Canada, Europe, Asia, Australia, and Latin America. The company was formerly known as NetPartners Internet Solutions, Inc. and changed its name to Websense, Inc. to reflect the shift in its business focus to web filtering solutions. Websense, Inc. was founded in 1994 and is headquartered in San Diego, California.

B. Websense Financial Profile

Table 66: Websense Financial Profile

Websense Financial Profile

	2008	2007	2006
Dollars in Millions			
Total Revenue	288.27	211,665	178,814
Cost of Revenue	48.16	29,080	15,274
Gross Profit	240.11	182,585	163,540
Research Development	53.27	39,681	22,663
Selling General and Administrative	220.71	159,056	101,414
Operating Income or Loss	**-33.87**	**-17,422**	**39,463**
Number of Employees	1375	1180	No Info

C. Websense Product Guide

Table 67: Websense Products

Websense Products

Competitors	Websense	Cisco IronPort S-Series
Web Reputation		
Web Reputation System and Filters	No[9]	Yes
Global Threat Correlation System Powered by Web, Email, and Intrusion Prevention System (IPS)	No	Yes
Daily Threat Data Volume	50 million URLs per day	500 GB
Web 2.0 Exploit Filtering	Limited; available through URL filtering categories only	Yes
Internal Bot and Zombie Detection	No	Yes
URL Outbreak Protection	Limited; available through URL filtering categories only	Yes
Administrator-Defined Policy Based on Risk Level	No	Yes
Flexibility to Use Web Reputation in Other Policy Areas, Such as HTTPS Decrypt Decision	No	Yes
Antivirus and Anti-Malware Protection		
Anti-Malware Scan Engine	No	Yes
Antivirus Scan Engine	No	Yes
Fully Integrated On-Device Scan Engines	No	Yes
Parallel Multiscaning Engine	No	Yes
Stream Scanning	No	Yes
Outbound Malware Phone-Home Detection on All Ports	No	All 65,535 ports
Suspect User Agent Detection	No	Yes
HTTPS Secure Sockets Layer (SSL) Content Inspection	Yes	Yes
Acceptable Use Policy Enforcement		
URL Filtering	Yes	Yes
Real-Time Content Analysis Engine	Limited; appliance only	Yes
Instant Messaging (IM) and Peer-to-Peer (P2P)	Yes	Yes
Data Security		
Integrated Data Security Policy Enforcement	No; requires Websense data security suite	Yes
Outbound Content Controls	No; requires Websense data security suite	Yes
Offbox Interoperability with Data Loss Prevention (DLP) Vendors	Yes	Yes

Web/URL Filtering: Websense, Inc.

Table 67: Websense Products

Websense Products (continued)		
Competitors	Websense	Cisco IronPort S-Series
Platform Features		
Integrated Threat Reporting and Alerting	Yes	Yes
Custom Purpose-Built Operating System	No; Linux	Yes
Proxy Performance Configuration Features	Yes	Yes
Native HTTPS	Yes	Yes
Native FTP	No	Yes
Deployment Modes		
Explicit Forward Mode	Yes	Yes
Transparent Mode (Web Cache Communications Protocol [WCCP])	Yes	Yes
Physical Inline, Bridge, and Passthrough Mode	Yes	No

9: Websense claims that ThreatSeeker is a reputation system, but it is not; it is a website crawling technology.

Table 68: Websense Hardware Specifications

Websense Hardware Specifications					
Products	Websense Web Security	Websense V10000	IronPort S160	IronPort S360	IronPort S660
Suggested Capacity[10]	No information	10,000 users	1000 users	5000 users	More than 5000 users
Form Factor	Various[11]	1 rack unit (RU)	1RU	2RU	2RU
RAM	No information	16 GB	4 GB	4 GB	8 GB
Processor	No information	2X quad-core Intel Xeons (3.0 GHz processors with 2X 6 MB cache)	1X2 (1 dual core) Pentium	1X4 (1 quad core) Xeons	2X4 (2 quad cores) Xeons
Disk	No information	4X 146 GB	500 GB	1.2 TB	1.8 TB
RAID	No information	Yes	No	Yes	Yes
Redundant Power Supply	No information	Yes	No	Yes	Yes
Interfaces	No information	6 X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet	6X Gigabit Ethernet

10: Specifications subject to change.

11: Because Websense is deployed using off-the-shelf operating systems, it provides only minimum system requirements, and the hardware is supplied by the purchaser.

D. Websense Sales Tactics

- Websense may attempt to shift focus from security to acceptable use policy (AUP) enforcement. Many Websense customers have deployed the product for human resources policy enforcement or employee monitoring, potentially because the product does not provide the security features common in most proxies today. Accordingly, Websense may attempt to shift focus away from security. Cisco IronPort™ provides the same type of AUP enforcement, along with all the security features.
- Websense may attempt to sell based on its URL databases and ThreatSeeker network. Websense claims to have recently added web reputation protection to its list of features, potentially in response to other companies' addition of this feature. Websense claims that its ThreatSeeker technology provides web reputation protection, but this is a crawler technology, not a machine learning system with a global threat correlation like the Cisco IronPort SensorBase™.

Suggest the following to counter proposals:

- Focus on security: Websense was originally designed for AUP enforcement and employee monitoring. Ask potential customers if they want a product that does more than URL filtering and provides comprehensive scanning on incoming files, looks for spyware phone-home attempts by previously infected machines, and was built from the start with security as the primary goal.
- Explain the power of Cisco IronPort Web Reputation: With legitimate sites being compromised and serving malware, the usefulness of URL categorization and blacklists is in question; this is Websense's primary business. Explain how Cisco IronPort Web Reputation can protect the customer from this new threat, as well as from malicious websites hosted on botnets and second-generation phishing attacks.
- Provide references: Cisco IronPort has many reference customers who have moved from Websense to Cisco IronPort. Show examples of these customers to prospects to let them know who is moving to Cisco IronPort.
- With the proliferation of Web 2.0 blogs and social networking sites, customers need to take quick, easy steps to enforce common-sense data security policies to prevent data leakage. Explain how Cisco IronPort data security policies can be created for outbound traffic on HTTP, HTTPS, and FTP. For enterprises that have already invested in special-purpose DLP systems, the Cisco IronPort S-Series offers an option to interoperate with DLP vendors via ICAP. This enables deep content inspection for regulatory compliance and intellectual property protection, incident severity definition, case management, and performance optimization.

E. Websense Weaknesses

- Websense offers only a URL database of sites that have been known to host malware in the past. It does no deep content scanning and has no capability to scan for phone-home activity over any protocol other than HTTP.
- The Websense URL databases and ThreatSeeker solution are reactive, similar to old-style blacklists in Simple Mail Transfer Protocol (SMTP). Cisco IronPort Web Reputation is preventive and provides an excellent outer layer of protection on top of the Cisco best-in-class malware signatures.
- Not having a signature-based scanning system for web traffic is like not having antivirus protection for email: You are leaving yourself open to the most virulent threats. Furthermore, Websense admits that its products are not designed to provide antivirus or antispyware protection:

  > *Websense Enterprise and Websense Web Security Suite are not antivirus software applications; however, they can limit the file name extensions that users may download.*

- Websense does not watch outbound network traffic to determine which desktop machines might be infected with spyware. The Cisco IronPort Layer 4 traffic monitor (L4TM) feature provides this visibility into previously compromised internal systems.

NOTES

Conclusion

Why Work With Cisco?

Cisco Offers Business and Technical Value

Cisco offers value beyond any particular router, switch, firewall, intrusion prevention system (IPS), VPN, email and web reputation solution, content filtering solution, or other security application or appliance. Cisco is the security market leader and has the broadest portfolio of security products, services, and solutions. Cisco can provide a complete solution of critical product and service elements, as desired by customers. By working with Cisco, customers and partners can find practical ways to more effectively utilize and secure their networks to further their business goals.

The Cisco® Secure Borderless Networks approach results from extensive interaction with customers and understanding the challenges they face. It demonstrates how Cisco adds value in addition to providing high-function, high-performance networking solutions. Further examples include Cisco Security Intelligence Operations and the Partner Ecosystem.

Cisco Secure Borderless Network

Cisco's Secure Borderless Networks presents a true architectural approach to security. By integrating security into all parts of the network, Cisco simplifies the task of meeting today's security requirements, regardless of application or service. The Cisco Secure Borderless Networks combines flexibility while maintaining control, providing integrated and pervasive security. The architecture's proactive intelligence extends security to the right people, devices, and locations—ultimately enabling businesses to build solutions that keep their entire organization secure and ready to meet business objectives.

Cisco provides expanded capabilities that enables IT and security professionals to more easily extend the right security to their workforce while still controlling risk and meeting compliance objectives. Moreover, it can help businesses increase productivity by enabling adoption of new business models such as software as a service (SaaS)—without compromising security.

For end users, the Cisco Secure Borderless Networks architecture provides flexibility in where, when, and how they can access information. End users enjoy a secure, "always-on" experience with their devices of choice. They don't have to worry about getting connected—instead, it just works.

Conclusion

Cisco Innovation

Cisco has long provided technology innovation and leadership, developing leading-edge features that others brand as proprietary. Cisco has a long history of working proactively with peers and competitors to incorporate these innovations as standards.

The following examples highlight the ways in which Cisco is leading security industry innovation.

Cisco Secure Borderless Networks Innovations

- Cisco pioneered early work on firewall, IPsec VPN, and IPS technologies.
- Cisco was the first network technology provider to support content security in the network switching and routing fabric, and Cisco IronPort® was the first to integrate data-loss prevention capabilities for data in motion.
- Cisco has visibility into 30% of the world's email traffic for computing reputation index information, with more than 110 attributes.
- Cisco leads the field in the blending of technologies: for instance, adding intrusion prevention for endpoints using behavioral technologies, adding reputation analysis to intrusion prevention, adding Secure Sockets Layer (SSL) VPN for remote access, launching Cisco® Network Admission Control (NAC) to control endpoint access, and recently announcing Cisco TrustSec, further demonstrating innovation in the area of network security.
- Cisco has been publicly acknowledged for creating the NAC concept and the NAC market.
- Cisco developed TrustSec, a new architecture plus a set of products and technologies, which allows enterprise networks to transition from disjointed policies to converged policies with pervasive integrity and confidentiality. Ultimately, Cisco TrustSec transforms a topology-aware network into one that is role-aware.
- Cisco IronPort has the world's first and largest email and web traffic monitoring system. The SenderBase® database collects data from more than 100,000 networks worldwide, 10 times more than competing reputation monitoring systems.
- Content security innovations include the Cisco ACE application control engine for performing content inspection, the similarly capable Cisco Catalyst® 6500 Supervisor Engine 3 PISA, integration of content security technologies into the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Integrated Services Routers, and additional IronPort enhancements for web and email content security capabilities.
- Cisco changed the endpoint security landscape through integrated zero-day (behavior-based) threat and data-loss protection.
- The intelligence arm of Cisco Security Intelligence Operations includes the world's largest real-time threat monitoring network: the Cisco SensorBase™ network. Its sources include:
  - More than 700,000 (and growing) globally deployed Cisco security devices collecting threat information
  - Cisco IntelliShield, a historical threat database of 40,000 vulnerabilities and 3300 IPS signatures
  - More than 600 third-party threat intelligence sources, which track over 500 third-party data feeds and 100 security news feeds 24 hours a day

Cisco Borderless Networks Innovations

- Cisco employees chair 20 IETF working groups in various networking areas, turning innovations into standards.
- More than 100 Cisco employees have written Internet drafts and RFCs.
- Cisco IOS® Software unifies all Cisco switches, routers, and other equipment, providing a solid foundation for Internet applications, helping companies extend common services and interfaces across the entire network, and reducing training and administrative costs.
- Cisco management software supports remote monitoring, configuration, fault detection, and troubleshooting. A complete line of tools simplifies and automates the delivery of intelligent services throughout the network, whatever the organization's size.
- Cisco routers provide world-class, innovative VPN capabilities, including Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport VPN, and Easy VPN.
- Cisco worked actively with many companies to develop the initial Fast Ethernet specification, eventually adopted by IEEE as the 802.3u standard.
- Cisco began shipping pre-standard Power over Ethernet (PoE) in mid 2000. This became the basis for the ratification of standards-based PoE (IEEE 802.3af) in late 2003.
- Cisco pioneered many IEEE 802.xx protocols; Multiple Instance Spanning Tree (MIST) was a key source used by the creators of the IEEE 802.1s specification. Spanning Tree Protocol fast enhancements provided the basis for IEEE 802.1w (Rapid Spanning Tree Protocol). Inter-Switch Link (ISL) was the basis for IEEE 802.1Q VLANs.
- Cisco developed Layer 2 Forwarding (L2F), and a Microsoft consortium developed the Point-to-Point Tunneling Protocol (PPTP). Cisco cooperated actively with the Microsoft consortium and helped develop a new standard, Layer 2 Tunneling Protocol (L2TP), which took the best ideas from both groups.
- Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP) later formed the basis for Open Shortest Path First (OSPF).

Cisco actively participates in almost every group concerned with networking standards. This participation helps ensure that Cisco products remain current and compatible with standards. Cisco customers can deploy Cisco devices without concern about incompatibility. By focusing on standards, Cisco also quickly brings to market products that meet customer needs. The emphasis on standards addresses the needs of a broad market, giving customers more choices in how they solve their networking problems and tailor their networks to meet specific business objectives.

Conclusion

Broad Innovations

- Cisco actively looks for new opportunities to grow and serve its customers through internal development, acquisition, or a combination of both, taking the most effective approach possible.
- Cisco is committed to innovation and R&D is a core component of our corporate culture. Cisco spends nearly US$5.2 billion a year in R&D, making us one of the top R&D spenders in the world. When looking at R&D as a percentage of revenue, Cisco matches or exceeds industry peers and secures our commitment to innovation.
- Cisco files over 700 patents annually and over 5000 have been issued.
- Cisco has the largest networking support staff in the world, with five Cisco Technical Assistance Centers (TACs) and more than 1300 support engineers devoted to network support and problem resolution.

Our market accomplishments have demonstrated our network security leadership. Cisco maintains the number-one share of the network security market. Cisco has more than a 20% share of the worldwide email security market, more than 500,000 integrated services router bundles shipped, IPS revenue exceeding US$100 million, and more than 1.5 million Cisco PIX® and ASA network security appliances shipped to date. Cisco is committed to customer and partner success. That commitment plus consistent product development, market commitment, and technical focus are crucial factors in Cisco growth. Cisco is proud of its success and looks forward to a bright future working with its partners and customers.

Cisco Secure Borderless Networks

Cisco® Secure Borderless Networks enables today's workforce to stay productive, while controlling cost and complexity. This comprehensive architectural approach integrates security into the distributed network. Through flexible solutions, integrated and pervasive security, and proactive intelligence, the Cisco Secure Borderless Networks extends security to the right people, devices, and locations. This architecture enables customers to build solutions that keep their organizations secure, and positions them to meet continuously evolving business and security challenges.

Overview

The Cisco Secure Borderless Networks has three primary characteristics:

- Flexibility—Cisco Secure Borderless Networks takes the fundamental concepts of security, threat control, data protection, and secure connectivity and extends them to the distributed workforce. This gives companies and their employees flexibility and freedom of choice to improve their business processes, without sacrificing control over policies and risk management.
- Integrated and pervasive security—To simplify deployment and support the right security solutions for various business needs, Cisco Secure Borderless Networks delivers functionality through different form factors. With the network as the platform, businesses can use integrated network security products, standalone appliances, fully hosted or hybrid-hosted offerings, or security software as a solution (SaaS) to build a wide range of security solutions. To help maximize the value of customers' security investments, Cisco builds ecosystem partnerships and offers professional services, creating one of the most complete offerings in the marketplace.
- Proactive intelligence—Cisco Security Intelligence Operations (SIO) combines with pervasive threat telemetry to establish an advanced threat-control infrastructure that provides threat identification, reputation-based analysis, and mitigation to achieve the highest possible level of security for Cisco customers.

Why?

Organizations need to defend themselves against threats, protect valuable data and resources, and implement the necessary controls for regulatory compliance. However, the distributed workforce—and the borderless network that is used to support it—require a new security strategy to deal with:

- Enabling collaboration—Organizations are adopting new applications for integrated voice, video, and conferencing services. These applications need to be secured to protect against vulnerabilities, mitigate risks, and maintain availability.
- The "consumerization" of IT—The popularity of mobile computing devices in the consumer market has helped these devices make their way to corporate networks. While it presents flexibility for the end user, security and IT organizations need to consider how to secure the connectivity of these devices, as well as how to extend the right security services and policies to protect them.

Conclusion

- Software as a service (SaaS) delivery models—Pushing more applications and services into the "cloud" can provide tremendous operational benefits, but organizations need assurance that their data is still protected when it is off the enterprise network, and a level of confidence that their security has not been compromised.

As security risks have evolved, so have organizations' approaches to them. Whereas information security was once a technology issue, today it is a business issue, representing a significant cost and operational challenge, but a fundamental business enabler as well. More and more organizations are implementing formal programs to reduce IT risk, especially security and compliance risks. As regulatory compliance becomes a core requirement for organizations in more industries, businesses must develop new capabilities for controlling the kinds of information traversing their networks, the way that information is used, and who can access the information. Organizations not only face the challenge of becoming compliant, but also of remaining compliant as the network evolves with business needs.

Cisco Secure Borderless Networks is an architecture that integrates security into the network to address today's security requirements. This approach delivers flexibility, integrated and pervasive coverage, and proactive intelligence to extend security to the right people, devices, and locations. This helps organizations meet evolving security requirements that enable the distributed workforce to stay productive, while controlling cost and complexity.

Cisco Security Services and Support

Cisco® Security Services allow organizations to follow a lifecycle methodology that enables them to design, implement, operate, and optimize secure networks that are resilient and reliable, and align technology investment with business strategy. Businesses today are increasingly mobile, extended, and operating in collaboration with partners, vendors, and customers. In this environment, they must manage risk by protecting data at rest and in motion, maintaining regulatory compliance, and protecting themselves from both internal and external threats. Cisco provides a comprehensive suite of security services to help organizations meet these challenges. These services derive from Cisco's proven strength in designing, implementing, and managing many of the world's largest converged networks.

Cisco Security Intelligence Operations

With the increase in blended, cross-protocol, and cross-vendor vulnerability threats, the security industry has come to recognize that point defenses, which protect from individual threats or protect individual products, are no longer enough. Integrated security management, real-time reputation assessment, and a layered, multipoint approach are needed.

As infrastructures become more distributed, increased risk is inevitable. Cisco Security Intelligence Operations enhances the ability to identify, analyze, and mitigate today's threats. Cisco is committed to providing complete security solutions that are integrated, timely, and effective—securing borderless networks for organizations worldwide.

http://www.cisco.com/security

Cisco Partner Ecosystem

As customer networks continue to grow in sophistication and diversity, IT departments are challenged with both a fragmentation of security products and an increase in consumer devices. The fragmentation inhibits intelligent sharing among security products and can lead to security holes and management problems.

Cisco is partnering with best-in-class companies to deliver jointly tested and validated solutions for end-to-end, secure borderless networks. The Cisco Developer Network delivers interoperable, secure borderless network solutions that enable customers to quickly and efficiently deploy end-to-end systems with verified compatibility.

Cisco Channel Partners

The Cisco Security Specialization Program recognizes Cisco channel partners that have developed the skills required to sell, design, install, and support Cisco network security solutions for customers. As Internet business solutions are adopted, Cisco Security Specialized Partners can meet the growing demand for critical security implementations and support services.

http://www.cisco.com/web/partners/index.html

Conclusion

Cisco Training Services: Cisco Security Certifications

Using best-in-class training and exams, Cisco security certifications validate the skills and competencies of security professionals. The Cisco CCSP® certification validates the advanced knowledge and skills required to secure Cisco networks. A CCSP network professional demonstrates the skills required to secure and manage network infrastructures to protect productivity and reduce costs. Cisco security courseware also meets the 4011 training standard. This standard is intended for information systems security (INFOSEC) professionals responsible for the security oversight or management of critical networks.

Security-Focused Authorized Cisco Learning Partners

Many authorized Cisco Learning Partners worldwide focus on Cisco security training, offering courses, remote labs, self-study materials, and other resources on the latest security technologies. These include advanced Cisco ASA solutions, Cisco secure intrusion detection systems, and end-to-end security implementation. A Learning Locator, course information, exam dates, and a detailed list of security-focused partners are available at http://www.cisco.com/go/training.

Building Real-World Solutions for Today’s Business Challenges

Modern applications and communications tools are providing businesses with unprecedented efficiencies and flexibility, but they also carry a cost: continually expanding IT risk. Fortunately, although information security threats have never been more challenging, the tools at an enterprise’s disposal to address these threats have never been more powerful.

All information in this publication is Cisco Confidential and should not be shared unless expressly authorized by the Cisco Competitive Leadership Team.

To the best of our knowledge, information in this Competitive Reference Guide is current as of the date this document was released by Cisco Marketing.

www.cisco.com

The use of the term “partner” to refer to a Cisco authorized reseller does not and should not be interpreted to create a legal relationship of partnership between Cisco and its authorized resellers.

Product information provided in this Guide is derived from sources including competitor data sheets and testing performed by Cisco Systems. Product information provided is believed to be accurate as of January 2010. Cisco is not liable for redistributing inaccurate information received from third-party sources.

Lit No. XXXXXXXXX
C92-584102-00 02/10