

BroadScan™

Spam-Virus Firewall Appliances

Comprehensive Security Solutions to Protect Business Networks from Spam, Virus, Spyware and Intrusion Threats with No Recurring Subscription Costs.

BroadScan™ is a total security solution delivering comprehensive network protection in an all-in-one appliance. In response to the growing breadth and sophistication of threats adversely affecting business today, BroadScan™ brings together a multi-layered defense system that reduces reliance on client based software as a primary defensive strategy. The resulting Unified Threat Management (UTM) solution is a more efficient and cost effective way to preserve the productivity and security of SMB and distributed branch office networks.

Available in four Firewall appliance models, BroadScan™ combines the industry's most respected scanning engines to detect and filter Spam, viruses and Spyware before they enter the business network. Integrated IDS/IPS, VPN, SPI Firewall and RADIUS authentication insure data security, and prevent Denial of Service attacks. BroadScan™ simplifies the IT administrator's control of security, reducing the inherent risk associated with dependency on client software and streamlines the implementation of a unified security strategy. The open source scanning engines update automatically without a subscription fee. As a result, BroadScan™ offers higher Return on Investment value for providing Enterprise-class security to Small and Medium businesses.

Adaptive Spam and Virus Blocking

Identifies Spam from the **SpamAssassin** signature matching engine by using header and Heuristics analysis, and then dynamically self trains by utilizing Bayesian filtering to optimize accuracy to better than 95 percent. Viruses are identified from Email, HTTP and FTP sources using the **ClamAV** virus signature scanning engine. Both engines are automatically updated daily.

IDS/IPS based Spyware Control

Employs advanced Intrusion Detection pattern matching using the **SNORT** signature scanning engine, and allows detailed threat-by-threat prevention response to a wide range of attacks including Spyware. This active monitoring and control process is integral with the Stateful Firewall (SPI), providing the administrator a highly accurate view of all threats against the network along with effective tools to combat them.



Appliance Models

Appliance Models:

- **SCN1000** Small business of up to 200 users.
- **SCL2000** Medium business of up to 500 users.
- **SCL3000** Distributed Enterprise of up to 1000 users.

Desktop models:

- **SCN200** SOHO desktop gateway for up to 25 users.

	SOHO
	SCN200
Network Size	Home Office Up to 25 Users
Performance Forwarding rate Email capacity Concurrent Sessions 3DES VPN	50 Mbps 90,000 / day 110,000 15 Mbps
Platform Platform CPU DRAM / Flash Hard drive	Intel XScale IXP 400 MHz 128 MB / 16 MB ---
Installation	Desktop

Scanning Spam Viruses Spyware	Yes Email ---
Engines Virus Spam IDS/Spyware	ClamAV SpamAssassin SNORT
Intrusion Protection SPI Firewall IDS/IPS	Yes ---
VPN Support PPTP IPSec / IKE SSL	2 4 ---

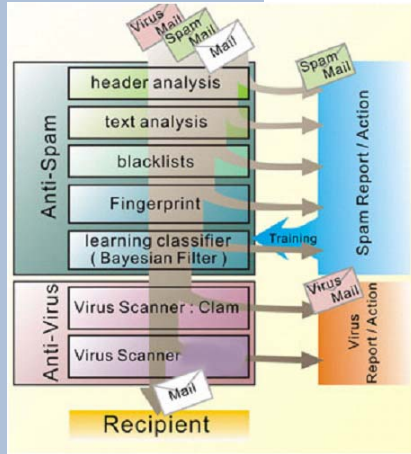
Policy rules Inbound Outbound Content filtering	50 200 Yes
QoS for VoIP	Yes – SIP ready
Authentication MAC filtering RADIUS client Internal DB Group policies	Yes --- --- ---
WAN Load balance	---
Management Web login DDNS Event reports High availability	HTTP 16 entries --- ---

SMB and Distributed Enterprise		
SCN1000	SCL2000	SCL3000
Small Business	Medium Business	Enterprise
Up to 200 Users	Up to 500 Users	Up to 1000 Users
90 Mbps 300,000 / day 582,000 20 Mbps	100 Mbps 620,000 / day 582,000 45 Mbps	100 Mbps 2,200,000 / day 1,000,000 80 Mbps
IPC VIA 1.0 GHz 512 MB / 64 MB 40 GB	IPC Celeron 2.0 GHz 512 MB / 128 MB 40 GB	IPC Pentium 2.4 GHz 1 GB / 128 MB 80 GB
Rack mount 1U	Rack mount 1U	Rack mount 1U

Yes Email/HTTP/FTP Yes	Yes Email/HTTP/FTP Yes	Yes Email/HTTP/FTP Yes
ClamAV SpamAssassin SNORT	ClamAV SpamAssassin SNORT	ClamAV SpamAssassin SNORT
Yes Yes	Yes Yes	Yes Yes
10 20 Yes	50 100 Yes	100 200 Yes

300 1000 Yes	1200 4000 Yes	2400 8000 Yes
Yes – SIP ready	Yes – SIP ready	Yes – SIP ready
Yes Yes 500 users 100 groups	Yes Yes 2000 users 400 groups	Yes Yes 4000 users 800 groups
---	Yes – 2 WAN ports	Yes – 4 WAN ports
HTTPS 64 entries Yes ---	HTTPS 256 entries Yes Yes	HTTPS 512 entries Yes Yes

BroadScan™



Comprehensive Email Scanning

Inbound and outbound email pass through a multi-layered scanning system that includes dynamic intelligence to self-learn and continually improve detection accuracy.

Anti-Spam

- *SpamAssassin* signature matching database
- Header and Heuristics analysis
- White and black lists; Personal and Global rules
- Bayesian self-training

Anti-Virus

- *ClamAV* virus engine detects of viruses, worms, Trojans
- Heuristics analysis
- Scanning of POP3, FTP and HTTP sources
- Automatic signature updating on 10 minute intervals

Anti-Spyware

- *Snort* IDS signature matching database
- Heuristics analysis on inbound and outbound traffic

Intrusion Protection, AAA and Secure Communications

Administrators have advanced tools to control inbound and outbound policies, identify and track network intrusions, prevent unauthorized access and secure branch communications.

IDS-IPS and SPI Firewall

Combines the *SNORT* intrusion signature engine with an SPI Firewall to employ a proactive and flexible system against intrusions and Denial of Service attacks from inside as well as outside threat sources.

Authentication and Policy Management

Provides rich inbound and outbound policy setup and mapping, with internal and external RADIUS authentication options.

Content and Application Filtering

- URL filtering list
- Scripts such as ActiveX and Java
- Instant Messaging
- File downloads by type and extension

VPN Secure Communications

Provides secure branch to branch communications with IPSec/IKE or PPTP.

QoS and VoIP

Traffic shaping capabilities support for H.323 or SIP voice applications.

Intuitive and Secure Web Management

BroadScan™ management is specifically designed for ease of use through a secure HTTPS interface.

Graphical performance and statistics reporting

Visual analysis tools provide detailed performance information in graphical presentation that reduces management time.

Comprehensive event reports

Mail activity may be viewed by any of a number of reporting formats including time period, history, and event type (content).

Proactive alerts

Includes event alarms to notify administrators and clients.

- Hacker alert - firewall detection
- Blaster alert - email and SNMP trap notification
- Traffic alarm
- WAN link failure alert

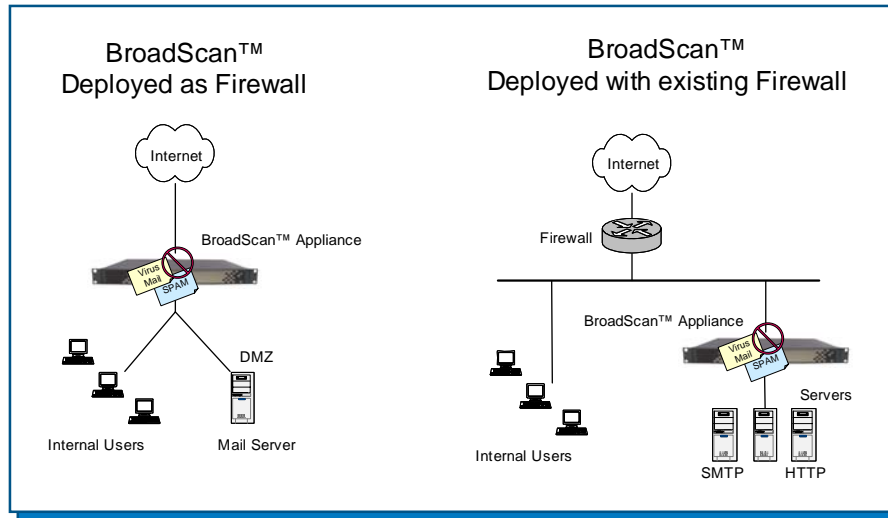


Deploying BroadScan™ in the Business Network

BroadScan™

As a Network Gateway for Small and Medium Business

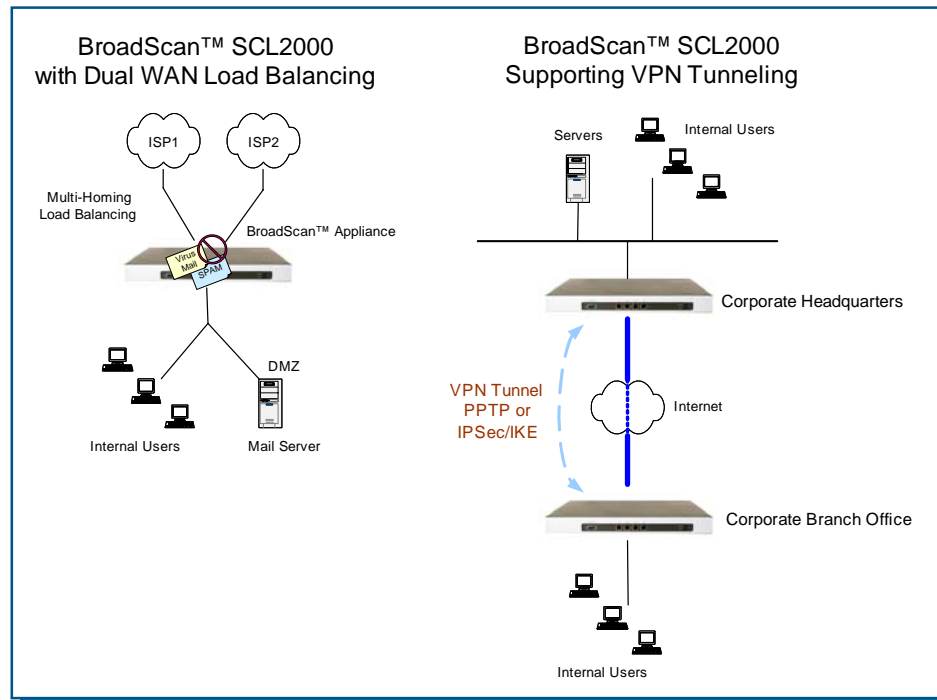
Deploy as an all-in-one network gateway solution or as a network segment security appliance.



Multiple WAN and Distributed Network Links

Medium businesses and distributed Enterprise networks require additional features available in the SCL2000 model to secure communications between branches and protect against ISP interruptions.

- WAN Load Balancing provides inbound and outbound access redundancy, plus offers intelligent traffic shaping to optimize for Quality of Service.
- Point to point VPN tunnels between two BroadScan™ appliances are supported with internal PPTP client/server or certificate based IPSec/IKE configuration.



(c) 2005, SOHware, Inc. All rights reserved (v2.0). Product image and specifications are subject to change without prior notice. BroadScan™ is a trademark of SOHware, Inc.

SOHware®

Your Partner for SMB Networking™. SOHware, Inc. Headquarters 3050 Coronado Dr. Santa Clara, CA 95054 Tel. 1.800.632.1118 Fax. 1.408.565.9889 www.sohware.com