

Frequently Asked Questions

BroadScan™ Spam-Virus Firewall Appliances

Revised 070705

[Anti-Spam Features](#)

[Anti-Virus Features](#)

[VPN Features](#)

Anti-Spam Features

What methods of scanning for Spam does BroadScan use?

ANS: Possible parameters for anti-spam include:

- a. Pre-configured rules already on the system
- b. Spam fingerprint check
- c. Bayesian filtering
- d. Check sender IP address against RBL (Real-time Blackhole List)
- e. Rules in five categories: Personal Rule, Global Rule, Whitelist, Blacklist and Training

How are Spam signatures obtained and updated?

ANS: Spam signatures acquirement and updates methods:

- a. "Rules", "Whitelist" and "Blacklist" are based on user defined rules for incoming mail scanning.
- b. "Spam fingerprint check" connects TCP 2703 and UDP 53 ports to the Fingerprint Server and compares with the current database.
- c. "Bayesian filtering" scans for criteria established in a database generated through the accumulation of Spam and Ham mail.
- d. "Check sender IP address against RBL" scans sender IP addresses against an updated address database in the RBL server via UDP53 port.

Where do database "updates" come from and who manages the service?

ANS: In 3 steps as follows:

- a. "Spam fingerprint check" connects to the Fingerprint Server while scanning mail; results are fed back to "spam mail" of the control center for verification where a hash value is calculated for a confirmed spam, updating database of the Fingerprint Server.
- b. "Bayesian filtering" is not a pre-configured "Training Database" but rather a real-time updating mechanism that is user defined and therefore fully user customizable through "rule-setting, feedback and system input" options.
- c. "Check sender IP address against RBL" compares sender IP address with the RBL server; Result is forwarded to the Open Relay Mail Server of the control

center for relevant verification and updating of the RBL Database with confirmed "open relay" Mail Server ID".

How are new Spam patterns incorporated into the database (learned)?

ANS: Use the following methods to incorporate new Spam patterns to the Training Database. Note, select these categories from the Mail Security => Anti Spam location in the Web UI.

- a. Personal Rule: select "Quarantine Spam Mail", and then press "Training".
- b. Spam Mail: from Search and Sender List select Quarantine Spam Mail, and then press "Training".
- c. Global Rule, Whitelist and Blacklist: select "Auto-Training" for each entry.
- d. Training - two options available: select "Import Training Database" to utilize a 3rd party pre-created list, or create and maintain a custom list. Custom lists are created via mail servers set up to collect Spam and Ham, from which the "Import Spam Mail from Client" or "Import Ham Mail from Client" may be selected.

How do the methods of scanning work and do they include email text content?

ANS: The BroadScan Spam mechanism prioritizes scanning in the following order: "Rule" ("Personal Rule" => "Global Rule"), then "Whitelist" => "Blacklist", then "Spam fingerprint check", then "Bayesian filtering", then "Check sender IP address against RBL", and finally "Pre-configured rule".

- a. If no detection is activated, the pre-configured rules are used to do comparisons and calculate a Score value; if equal to or greater than the Score value then the mail is regarded as Spam, otherwise, it is regarded as Ham.
- b. Mail is then calculated with a logarithm for a Hash value and checked for a "Spam fingerprint"; if it conforms to the database the mail is regarded as Spam, otherwise, it is regarded as Ham.
- c. Spam and Ham Mail Analysis; when both quantities reach above 200, then Bayesian filtering is used to sort mail Header and Content character strings characteristic from the database for comparison, from which a Score value is calculated; if equal or greater than the Score value, the mail is regarded as Spam Mail, otherwise, it is regarded as Ham.
- d. Mail IP address is then compared against the RBL database and a Score value is calculated; if equal to greater than the Score value, the mail is regarded as Spam, otherwise, it is regarded as Ham.
- e. Rule functions are then used to compare mail Header and Content; if a match is found to the rule, the mail is regarded as Spam, otherwise, it is regarded as Ham.
- f. Whitelist is then used to compare the sender and recipient's email addresses, and if conforms, the mail is regarded as Ham.
- g. Blacklist is then used to compare the sender and recipient's email addresses, and if conforms, the mail is regarded as Spam.

Is the Bayesian filter pre-trained?

ANS: No. We provide an un-trained Bayesian database to enable a clean criteria list for Spam to be created specific to the user's network and email activity. Pre-trained databases are inherently inaccurate and generate unacceptably high false positives and false negatives. Utilizing the "Training" function in BroadScan yields exceptional filtering accuracy.

How are false positives minimized or prevented?

ANS: In order to enhance scanning accuracy BroadScan employs five rule systems in an integrated manner. These rules include Personal Rule, Global Rule, Whitelist, Blacklist and Training. For example:

- a. If an email is falsely marked as Spam, BroadScan allows for updating or training of the Spam database. The same training mechanism is available for Spam that is allowed through without being marked or filtered.
- b. If a specific sender or mail account is found to be a source of Spam, port 89 can be used to record the account in the Blacklist, which blocks all future mail from this source; Likewise, If you consider a specific sender or mail account to be legitimate email, port 89 can be used to record the account in the Whitelist, which allows all future mail from this source.
- c. The network administrator can prepare utilize "Junk" email folders to isolate and store suspected Spam for review by intended recipients. BroadScan supports network notification of quarantined email, further enabling discrete user by user accuracy.

How do the filtering results impact the user experience?

ANS: User experience varies with configuration. Administrators have the option to delete Spam, dramatically reducing incoming mail to a user's email client, or pass Spam mail to the user with a message added to the subject line identifying the mail as Spam. This option is made by Selecting Mail Security => Anti-Spam => Setting where the choice to "Delete the Spam Mail" or "Deliver to the Recipient" is made.

Can the current list of blocking patterns be viewed?

ANS: No. The variables in Spam mail as defined by the five rule system employed by BroadScan makes the viewing of individual pattern definitions impractical. The dynamic nature of training enables participation by all network users in building a corporate specific filtering database that is highly accurate.

Are both inbound and outbound Email scanned and filtered?

ANS: The BroadScan SCN200, SCN1000 and SCL2000 models scan for inbound Spam only. SOHware will be introducing a new model, SCL3000, in Q3, 2005 to address simultaneous outbound scanning capabilities.

Can a user be warned if their computer is being used as a source of outbound Spam?

ANS: BroadScan will support host user warning in a new model scheduled for release in Q3, 2005, which provides outbound email scanning. Both Mail Server and Host PC sources of LAN based Spam will be filtered. The new model is designated SCL3000.

Can a user report an email to be "Spam" so that all future email from that sender is discarded?

ANS: Yes. Users may report specific email to the network administrator who adds sender to the Blacklist, which will filter all future email from that source.

What reporting and post analysis are possible?

ANS:

- a. Mail analysis is available for annual reports, monthly reports, weekly reports, or daily reports by mail notification.
- b. Statistics are also available to report on Spam levels received by each user and include graphical display.

Anti Virus Features

How does ClamAV compare with other virus engines?

ANS: ClamAV is a leading open source engine for virus scanning. Below is a comparison on response time when updating various scanning engines with new virus threats:

Table 1

Engine Name	Update Time		Virus Name
Clam-AV	02.05.2005	18:36	Worm.Sober.P
Kaspersky	02.05.2005	18:39	Email-Worm.Win32.Sober.p
F-Prot	02.05.2005	18:54	W32/Sober.O@mm
Gdata AVK	02.05.2005	18:56	Email-Worm.Win32.Sober.p (KAV)
Bitdefender	02.05.2005	19:19	Win32.Sober.O@mm
Sophos	02.05.2005	19:27	W32/Sober-N
Command	02.05.2005	20:07	W32/Sober.O@mm
Ikarus	02.05.2005	20:14	Email-Worm.Win32.Sober.P
Virusbuster	02.05.2005	20:44	I-Worm.Sober.Q
Panda	02.05.2005	20:49	W32/Sober.V.worm
Etrust	02.05.2005	21:54	Win32/Sober.53554!Worm
Antivir	02.05.2005	22:24	Worm/Sober.P
Norman	02.05.2005	22:46	Sober.O@mm
Trend Micro	02.05.2005	23:18	WORM_SOBER.S
AVG	02.05.2005	23:27	I-Worm/Sober.P
McAfee	02.05.2005	23:38	W32/Sober.p@MM
Etrust	03.05.2005	01:15	Win32.Sober.N (VET)
Symantec	03.05.2005	03:38	W32.Sober.O@mm
QuickHeal	03.05.2005	03:28	Sober.p
Dr. Web	03.05.2005	10:46	Win32.HLLM.Generic.345

Source: <http://www.pcwelt.de/news/sicherheit/111012/index2.html>

How are the virus signatures updated?

ANS: Virus signature updates are configured under Anti-Virus => Setting in the Web GUI and include two actions. Both actions are performed by connecting to the official ClamAV site for updating with new virus signatures:

- o Auto update - performed on 10 minutes intervals by BroadScan.
- o Update now - performs update on demand.

What frequency do virus signatures update?

ANS: BroadScan checks itself for the latest version every 10 minutes, and if a more current version is detected, the auto update will be started. An alternative option to update on demand is also available.

What assurances are there that ClamAV updates will remain subscription free?

ANS: ClamAV is a leading open source scanning engine and is well-established in the "anti-virus" market. As an open source system, updates will remain available with no subscription fee. BroadScan will only use ClamAV to maintain SOHware's subscription free update policy.

How can the administrator/user determine that an update has taken place?

ANS: In the Web GUI, under Mail Security => Anti-Virus => Setting, a log posts the updated date/time and version of the signature database.

Can the administrator/user view the current version of signatures installed?

ANS: Yes. From the Web UI, select Mail Security => Anti-Virus => Setting to view the version number. For additional information about the virus signature database go to <http://www.clamav.net>.

How does an administrator know what viruses have been detected and who was the intended recipient?

ANS: From the Web GUI, select Mail Security => Anti-Virus => Virus Mail to view report categories by Recipient. The report also lists each Recipient's Total Virus, Total Mail, Duration, Virus percentage, Sender, Recipient, Subject, Received Time, Virus Name, and Mail Size information. Alternatively, view this information in chronological log form by selecting Mail Security => Mail Report => Log, which provides information on Sender, Recipient, Subject, Date, Attribute, Action.

How do the filtering results impact the user experience?

ANS: BroadScan detects viruses in e-mail, and from http and ftp sources.

- Virus infected email: Instead of receiving the original infected email, the user will receive an email notification with the following message:

Warning!!! This e-mail is sent by Mail Security Gateway. It means the original e-mail contains a virus and Mail Security Gateway had removed the content already. The original e-mail has been replaced by this message.

- Web infected URL: When a user clicks on a malicious web link, a message will show on the user's browser alerting of the threat.
- FTP: BroadScan will stop an FTP operation when detecting an infected file and alert the user.

What capabilities are available to determine malicious URLs (Phishing and virus threats)?

ANS: The administrator can utilize a Policy function to invoke Anti-Virus scanning of malicious web sites. Select Policy => Outgoing => New Entry => Anti Virus and then select HTTP/ WebMail.

Are virus attacks detected if originating from a client located on the network LAN?

ANS: Yes, if the virus were generated internally, BroadScan will alert that particular client's by sending warning message on its display monitor.

Are senders of viruses warned that their computer is a source of viruses?

ANS: No. Current BroadScan models do not support internal network scanning or source identification. The roadmap of future support includes internal network scanning beginning with model SCL3000 to be launched in Q4, 2005.

Where does the database of quarantined virus e-mail reside?

ANS: When the 'quarantine' function is enabled, filtered Virus emails are stored on the internal hard disk. This feature is available on SCN1000 and SCL2000 models. To retrieve quarantined emails, select Mail Security => Anti-Virus => Virus-Mail, and enter the user's account. Hand select the desired email and email addresses to be retrieved.

What reporting of viruses and post analysis are possible?

ANS: The following respective reporting and Analysis configuration are available:

Reporting: Both Periodic and History reporting are available configuration options, by selecting Mail Security => Mail Report => Settings. Periodic settings allow for automated report generation on a daily, weekly, monthly or yearly basis. History settings allow for custom selection of time period to generate a report.

Analysis: Report history of all the virus email detected is viewable in a graphical statistics display by selecting Mail Security => Mail Report => Statistics. Percentage of virus and Spam mail over specified time period is displayed for relational analysis.

VPN Features

What types of VPN protocols does BroadScan support?

ANS: BroadScan includes an IPSec engine that supports IKE auto-key, 3DES AES and MD5/SHA1 authentications. BroadScan also includes a PPTP server and client. This allows IPSec or PPTP to be used in creating VPN tunnels between separate networks.

What network scenarios are possible for VPN?

ANS: BroadScan can support branch-to-branch VPN where two VPN gateways are connected, typically between two BroadScan gateways. BroadScan can also support remote client to gateway VPN where client VPN software on a PC, as with mobile or telecommuter users, connects to a BroadScan gateway from a remote location. Both types of VPN tunnels are initiated and / or terminated on the WAN port of the BroadScan gateway.

How is throughput performance affected by VPN tunneling?

ANS: BroadScan models include processing capabilities appropriate for the network size they are recommended to support. This includes the presence of VPN encryption processes for inbound and outbound communications. Throughput performance is listed in the following table:

	SCN200	SCN1000	SCL2000	SCL3000
VPN Tunnel Connections				
IPSec (max. entries)	32	200	1000	2000
PPTP Server (max. entries)	16	50	200	400
3DES Throughput	15Mbps	18Mbps	43Mbps	80Mbps

Is BroadScan's VPN interoperable with other VPN solutions?

ANS: BroadScan IPSec and PPTP engines have been tested for interoperability with a range of industry leading vendors. This enables a BroadScan gateway to form a VPN tunnel with another vendor's VPN gateway. It also allows many VPN software clients to connect to our gateway over the Internet. Interoperability testing is ongoing, but the following is a current list of tested platforms.

Compatible Software Clients:
Microsoft Windows PPTP or IPSec
SafeNet
Netscreen

Compatible hardware platforms:
SonicWall
Cisco
Fortinet
Netscreen