

Product Features

1. Built-In SPI Firewall to Protect Your Enterprise Network

- BroadScan UTM core design is based on its Stateful Packet Inspection (SPI) firewall, providing complete firewall protection.
- By default, the BroadScan UTM device will deny all incoming access originating from an external network. In this case, only packets that satisfy the security configuration and answer the internal user's requests will be permitted to pass through to the internal network.

2. Multi-Spam-Filtering Function Providing High Spam-Filtering Accuracy

- It employs Fingerprint, Bayesian Filtering, Greylist Filtering, spam signatures and more as a method, together with periodic automatic training from the Bayesian database, to serve as the defense line against spam. Along with Personal Rule, Black List and White List, spam filtering could plateau at 99% accuracy. In addition to that, spam disposal can be decided based on the detailed reports that BroadScan UTM offers.
- Personal Rule allows users to have their personal email settings. It also provides users with spam filtering criteria as well as an access to their email services (the built-in Web Mail) without any additional software or configurations.

3. Virus Detection

- BroadScan UTM offers you ClamAV for virus scanning. It can detect over forty thousand kinds of viruses, worms, and Trojans. Additionally, virus definitions are updated automatically once they are available. More benefits offered to you are free lifelong virus definition updates and no user limit (ClamAV only) that not only saves you money but also keeps your protection up-to-date.
- Capable of scanning SMTP, POP3, HTTP and FTP, it can protect a business' susceptibility to viruses, Trojans, website scripts, spyware, phishing etc.

4. Inbound and Outbound Email Filtering

- BroadScan UTM provides incoming and outgoing email filtering with virus and spam protection. All emails are subject to the criteria that determine whether they are spam or virus infected ones, protecting the business' email security.

5. Email Notice

- emails that are rated as spam will be quarantined. BroadScan UTM will then notify the recipients of the quarantined emails and enable them to decide whether to retrieve those emails.

6. Intrusion Detection and Prevention (IDP)

- Built-in IDP (IDS + IPS) can inspect the packets from OSI layer 4 (transport layer) to OSI layer 7 (application layer) using Deep Packet Inspection (DPI), and block concealed malicious code such as worms and buffer overflow attacks.
- With a possession of over 3,000 signatures, and with an automatic update frequency of once every 30 minutes, it provides an effective defense against various forms of recognizable attacks. The IT administrators can set the actions for suspected packets or Internet services.

- Can filter out all the packets that originate from the sessions of P2P, IM, NetBIOS, etc.
- As soon as an attack is suspected, BroadScan UTM will immediately notify the IT administrator. Moreover, an extensive range of reports is available for the IT administrator to analyze.

7. Email Auditing & Archiving

- email Auditing – based upon the IT administrator's settings, all incoming and outgoing emails can be subject to auditing. If the incoming/ outgoing email matches the predefined criteria settings, then only after inspection from the IT administrator will the email be allowed to proceed to its intended destination.
- email Archiving - business emails can be stored for the IT administrator to locate the emails anytime and anywhere. This is extremely useful for any unforeseen situations that require the historical emails.

8. Detailed Email Statistics & Logs

- Detailed daily reports allow IT administrators to gain an insight into the business' email activities.
- Detailed daily, weekly, monthly and yearly reports in visual charts indicate quantities of spam and virus infected emails, to allow IT administrators to observe the results of its anti-spam and anti-virus mechanisms.

9. Multi-WAN Ports Enabling Load Balancing and Link Redundancy

- Outbound Load Balancing: When an internal user is accessing the Internet, the BroadScan UTM device will automatically enable the load balancing function to allocate the network traffic to each port equally and then effectively combine the bandwidth into a single connection. In addition, once any one of the WAN ports develops a failure, the BroadScan UTM device will switch the connection to other ports, ensuring the reliability of the network.
- The exclusive "By Source IP" mode (i.e., a kind of load balancing) is ideal for online gaming, Internet banking, etc. It ensures the continuity of the connection, and will not cause the session to disconnect.
- Inbound Load Balancing: Unlike third-party products, BroadScan UTM offers inbound load balancing and not just outbound load balancing. With inbound load balancing, inbound flows can be distributed to each port according to the regulated weighting and priority of each port, ensuring the quality of the connection. In addition, its link redundancy provides additional reliability to the inbound links upon a connection failure.

10. Comprehensive Policy-Based Routing

- The IT administrator can set policies to make routing decisions according to any specific routing needs of the business.
- Inbound PBR is exclusively intended for the delay accessing between the two major ISPs in China – China Unicom and China Telecom. BroadScan UTM can distinguish the ISP of the visitors to your website and route them to the same ISP connection (if available).

11. 3A Server

- Authentication: Its built-in authentication along with the authentication support for RADIUS, POP3 and LDAP servers effectively bans unauthenticated users from accessing the Internet.
- Authorization: All sessions, whether incoming or outgoing, can be strictly regulated by policies.
- Accounting: IT administrators may adjust the bandwidth distribution based on the faithfully recorded accounting

report.

12. Optimal Quality of Service (QoS) Mechanism

- QoS mechanism allows IT administrators to assign a guaranteed bandwidth, maximum bandwidth and priority to each user respectively; In addition, it helps the device to accommodate networks with the needs for hierarchical management.
- Personal QoS enables IT administrators to assign bandwidth to each user respectively, avoiding bandwidth being occupied by minority individuals. It is intended for networks that requires less policy management, such as Internet cafés, school dormitories, residential communities, etc.
- Bandwidth distribution can be simplified by utilizing QoS together with Personal QoS. For instance, you may allocate 20 Mbps of total bandwidth to a specific department using QoS; and then, distribute the 20 Mbps to each user based on the settings of Personal QoS. To do so, it merely takes one network policy to achieve the bandwidth distribution.

13. Complete VPN Capabilities

- With BroadScan UTM, IPSec and PPTP VPN connections are made available for users between company headquarters and branches. It merely takes another BroadScan UTM device or a VPN-enabled gateway deployed on the remote site to achieve a secure, private connection.
- VPN Trunk provides your IPSec and PPTP VPN connections with survivability by integrating your available bandwidth. It also comes along with better manageability (combining the use of policies, authentication mechanisms and bandwidth management) and an additional layer of protection (by virus scanning) to your virtual private networks.
- Web VPN (or SSL VPN) offers you an easy VPN access to your headquarters simply through a web browser. Offsite users may create VPN connections at anytime from anywhere with ease.
- BroadScan UTM can perform a hardware authentication upon using Web VPN. When the hardware authentication is active, users' hardware information (the serial numbers of your hard drive, processor, etc.) rather than a set of username and password will be used for authentication, which greatly boost the network access security.

14. Application Blocking

- Internet-enabled applications are not only difficult to regulate, but often a way for someone to compromise your information assets or network security. The users' access to various Internet-enabled applications can now be regulated through using BroadScan UTM. (For information on supported applications, see Table 1.)
- Its automatic updating mechanisms provide the device with the latest application signatures, ensuring its ongoing effectiveness.

IM Messaging	MSN, Yahoo, ICQ, QQ/TM2008, Skype, Google Talk, Gadu-Gadu, Rediff, WebIM, etc.
File Transfer over IM	MSN, Yahoo, ICQ, QQ, Google Talk, Gadu-Gadu, etc.
P2P Blocking	eDonkey, BitTorrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, GoGoBox, QQDownload, Ares, Shareaza, BearShare, Morpheus, Limewire, Kazaa, etc.
Multimedia	PPLive, PPStream, UUSee, QQLive/QQGame, ezPeer,vodplayer, etc.

Streaming	
Web-Based Mail	Gmail, Hotmail, Yahoo, Hinet, PChome, URL, Yam, Seednet, 163/126/Yeah, Tom, Sina, Sohu, QQ/Foxmail, etc.
Online Gaming	GLWorld
VPN Tunneling	VNN Client, Ultra-Surf, Tor, Hamachi, etc.
Remote Controlling	TeamViewer, VNC, Remote Desktop, etc.

-

- Table 1 Applications Supported

15. Content Blocking

- URL Blocking blocks the access to a website by using wildcards (e.g., “*”, “?”) or keywords.
- Script Blocking blocks pop-ups, ActiveX, Java and cookies from websites such as stocks, futures, etc.
- Download/Upload Blocking prohibits file uploading and downloading using HTTP and FTP protocols. Specific file extensions such as exe, iso, mpg, etc. can be blocked.

16. LAN Security Mechanism

- Provided a DoS / DDoS attack is suspected from the anomaly traffic detection, the BroadScan UTM will proactively block the packets originated from the victim user and immediately notify the user and the IT administrator.
- It's anomaly traffic detection capability along with a core switch may perform a combined defense against DoS / DDoS attacks originating from the internal network. Once BroadScan UTM detects the attack, it will instantly notify the core switch to block the attacking packets to avoid further damage.
- The device can work in combination with edge switches by immediately detecting to which edge switch and port the virus-infected PC is connected.

17. Featuring a Physical DMZ Port to Provide Server Security

- BroadScan UTM features a physical DMZ (Demilitarized Zone) port, in which the servers of your external services may be deployed for the purpose of providing LAN security. By the means of network policies and the protection derived from the physical design of DMZ, merely the users that meet the criteria may access the services you provided in the DMZ.
- Three types of DMZ modes accommodate diverse network infrastructure or topology: NAT, Transparent Routing and Transparent Bridging.
- The physical DMZ port can also serve as a WAN port, adding even more flexibility to your network deployment.

18. Policy-Centric Design & Web-Based Interface

- All configurations can be done simply through the web-based interface, greatly facilitating the network management.
- Policy-based design helps IT administrators achieve network management of every kind.

19. Easy Remote Access

- The IT administrator can access the web-based management interface via any web browser on any computer without any additional software installation.
- The IT administrator may easily locate a problem through the help of charts, statistics and operating information. In addition, it supports traditional Chinese, simplified Chinese and English.

20. Hardware High Availability

- Its Hardware High Availability offers you with additional survivability during down time and helps your network stay connected.