

# FAQ: BroadGuard®

---

[General FAQs](#)

[NAT FAQs](#)

[Firewall FAQs](#)

[VPN FAQs](#)

----- General -----

## **What is BroadGuard?**

BroadGuard is a fully integrated security solution designed for small and medium businesses. As a Firewall gateway, BroadGuard secures corporate networks from external threats and cyber attacks while managing a Broadband service connection. As a VPN tunneling endpoint, BroadGuard creates secure communication links between distributed business networks allowing the transfer of confidential data and media and the sharing of corporate resources.

## **How is BroadGuard designed to handle data and bandwidth demands?**

BroadGuard is built on the Intel XScale network processor, and includes Flash and DRAM memory capable of handling the performance demands of small and medium businesses. Specifically for the BBR1000, up to 50 3DES IPsec VPN tunnels can be managed simultaneously while maintaining up to 10 Mbps throughput.

## **How much memory is included in BroadGuard?**

The BBR1000 includes 16 MB of Flash and 64 MB of DRAM.

## **Is BroadGuard remotely manageable?**

Yes. BroadGuard's Web interface may be accessed from the Internet via secure HTTPS connection. In addition, Telnet may be used from remote and secured using a VPN tunnel. SNMP will be available in a future firmware download.

----- NAT -----

## **Can NAT be enabled selectively?**

Yes, the NAT feature can be selectively enabled at the policy level.

## **Does BroadGuard support content filtering?**

Yes, filtering of traffic passing through BroadGuard is possible at different levels of granularity with the following parameters:

- Source / destination address of the packet
- Packet destined to a specific port (This is used to filter traffic such as ftp, http, nds, https, etc.) User can define a specific TCP or UDP port to which, if traffic is destined, the packet will be filtered.

- For ftp, you can filter operations such as storing files, retrieving files, directory list, create directory, change directory or passive operation
- For http, you can filter based on proxy, ActiveX controls or java controls. We can also filter based on file extensions we encounter in the http traffic.
- For smtp traffic, you can filter based on specific smtp commands.
- For RPC traffic, you can filter based on specific RPC numbers
- URL filtering for specific sites based on a permitted list or disallowed list.

#### **Does the BroadGuard NAT include ALG's?**

Yes. BroadGuard's NAT includes over 40 currently supported ALG's to provide advanced application support.

#### **What ALG's does BroadGuard support?**

BroadGuard includes ALG's supporting FTP, IRC, Net2phone, H323, SIP, RTSP, ICQ, AOL Instant Messenger, MSN Messenger, CUCME, PPTP, IPSec, IKE and NetMeeting, as examples.

#### **How can NAT be configured in BroadGuard?**

NAT may be configured as many-to-one (NAPT), one-to-one, reverse many-to-one, reverse one-to-one and multiple instances in addition this.

#### **What routing protocols does NAT-Router support?**

BroadGuard supports the following protocols - IP, TCP, UDP, ARP, and RIP v1/v2.

----- Firewall -----

#### **What type of Firewall is provided in BroadGuard?**

The Firewall is a complete Stateful inspection Firewall technology.

#### **Is the SPI Firewall certified?**

Yes, the Firewall is ICSA certified.

#### **What features are supported by the Firewall?**

The 3 main functions of the Firewall are policy definition and enforcement, guarding against attacks(details) and providing logging. Selectors for Firewall policies can be IP addresses or user groups and policies can be applied for specified time intervals. Specific elements of the Firewall include:

- Complete Stateful packet inspection firewall (SPI)
- Corporate Inbound/Outbound policies
- Service time-outs
- Statistics
- Application content filtering
- Authenticated remote user access
- E-mail alerts
- Syslog support for event logging
- Comprehensive network access statistics

#### **What DOS attacks does the Firewall protect against?**

The major types of attack patterns blocked include the following:

1. LAND attack

2. Smurf attacks
3. Winnuke attack (Netbios out-of-bound)
4. Unknown IP protocol
5. Reassembly attacks, including:
  - Syndrop
  - Teardrop 2
  - Opentear
  - Tentacle
  - Ping of Death attack
  - Nestea
  - Big ping
  - Targa 3
  - Newtear
  - Bonk
  - Boink
  - IP fragment overlap
  - IP fragment last length changing
  - Too many IP fragments
  - Very small IP fragments
  - Empty fragment
  - SSPing
  - Flushot
6. IP Spoofing across network
7. Twinge
8. TCP SYN flood
9. IP source route option detection
10. Jolt and Jolt2
11. Ascend attack
12. TCP XMAS scan
13. Octopus
14. Overdrop
15. Echo / chargen
16. Ascend Kill
17. Mime flood
18. Zero length IP option
19. IP unaligned time stamp
20. ICMP router advertisement
21. Snork attack
22. Fraggie attack
23. UDP short header
24. TCP header fragmentation
25. TCP short header
26. TCP null scan
27. TCP sequence out of range
28. TCP FIN (Stealth)
29. TCP postconnection SYN
30. TCP invalid urgent offset
31. RFProwl
32. Blind spoofing
33. W2K domain controller attack
34. FTP bounce attack
35. Sequence number prediction

### **How many concurrent sessions can be established through the Firewall?**

There are no user restrictions or session restrictions in BroadGuard's Firewall.

### **Can Firewall policies be enabled based on time schedules?**

Yes, selectors for Firewall policies can be IP addresses or user groups and these policies can be applied for specified time intervals.

----- VPN -----

### **What is VPN?**

A Virtual Private Network (VPN) provides a means for remote computers to securely communicate with each other across a public wide area network (WAN), such as the Internet. A VPN connection may be used to link two local area networks (LANs) or for a remote dialup user to connect to a private LAN. The three major technologies used for VPN include PPTP, LT2P and IPSec.

### **What is IPSec/IKE?**

IPSec provides a mechanism for secure data transmission over an IP network, ensuring confidentiality, integrity, and authenticity of data communications over unprotected networks such as the Internet. Internet Key Exchange protocol (IKE) is used for key and security information exchange. In addition, ESP (Encapsulated Security Payload) and AH (Authentication Header) are used to encapsulate IP packets for tunneled data.

### **What is IKE used for?**

IKE is used in IPSec to authenticate peers, manage the generation and handling of keys used by the encryption and hashing algorithms between peers, and negotiates IPSec security agreements (SA).

### **Is the IPSec certified to be interoperable with other VPN endpoints and clients?**

Yes, VPN has been tested under various conditions for VPNC certification. The Companies with whom BroadGuard has been tested include:

3Com, Checkpoint, Cisco, F-secure, Hifn, IBM, Intel, Lucent, Lucent (Xedia), Net Screen, Nortel Networks, Ramp Networks, Trilogy, VPNet, Timestep, RedCreek, SSH, Shiva, Network Associates, DataFellows and UUNet.

### **What are PKI certificates?**

PKI refers to the ability to manage certificates as part of the IKE authentication. BroadGuard provides complete support for PKI certificates and has interoperated with certificates generated from CA companies such as Entrust, Verisign, Baltimore, and others. The certificates used by BroadGuard are industry standard x.509 certificates.

### **How does BroadGuard handle NAT/NAPT with IPSEC?**

NAT/NAPT is supported after tunnel end points and thereby enables network traffic to be uninhibited by the VPN process.

### **Why does BroadGuard support NAT Traversal?**

NAT traversal is important to support access to the business network by a remote client, such as a telecommuter using a VPN client on their computer. The VPN tunnel only functions if the IPSec packet integrity is maintained throughout the tunnel, and NAT Traversal enables a "keep alive" function for each packet. This feature is essential for a truly business-class VPN solution.