

Protecting Local Area Networks with Easy-To-Use Firewalls

As cable deployment continues to bring broadband to the masses, it is now becoming easier to safeguard both personal data and computing resources. The buildout of cable access networks is encouraging cable subscribers to connect multiple computers to share broadband connections.

Cable subscribers can connect multiple PCs using combinations of wired and wireless Local Area Network (LAN) technologies, allowing each of these PCs to share a single broadband connection. Both home users and companies need to protect against hacker attacks and remove the risk of unauthorized users gaining entry into the LAN.

Residential subscribers need the ability to safeguard their home computing resources and personal information, and Small Office Home Office (SOHO) users and Small to Medium Enterprise (SME) users must protect the value of their business information. Telecommuters and people working from home after hours need to similarly protect the integrity of company information.

The United States Federal Government recommends that Internet users add firewall protection — a system designed to prevent unauthorized access to or from a private network and also warns that PCs without firewalls can be accessed through their Internet connection. Without firewall protection, users can lose valuable personal or corporate information and they risk permanent damage to PCs and



peripherals. Multi-PC households, small businesses and corporate telecommuters can all benefit from easy-to-use firewalls that allow them to enjoy the advantages of broadband Internet connections — while avoiding the risk of intrusion.

Always-on broadband connections present particular risks that must be addressed. It is critical that each LAN is protected by a firewall. Without a firewall, anyone on the Internet could theoretically access computing resources and private data. Everyone operating a LAN connected to the Internet should deploy a firewall that secures the LAN and protects it against outside attack.

All traffic entering or leaving the LAN pass through the firewall, which examines each traffic flow and blocks flows that do not meet the specified security criteria. There are different configurations for firewalls, and cable subscribers need to ensure that they provide the appropriate security levels.



MOTOROLA
intelligence everywhere™

Wireless Cable Modem Gateway Family

Firewalls

➤ Firewalls — An Overview

The primary purpose of a firewall is to provide a single point of entry where defense can be implemented.

Firewalls allow access to resources on the Internet, and public and private networks from devices on the LAN, while preventing unauthorized access from the Internet to the LAN.

The firewall must provide a method for system administrators to configure access control lists to establish the rules for access according to local policies. All access should be logged to ensure adequate information for a detailed security audit. But deployment should not be a daunting task because most home or small business networks do not have Information Technology (IT) departments.

When selecting cable access equipment, subscribers should make sure that access equipment offers pre-configured firewall capabilities that are sufficient to meet their needs. Set-it-and-forget-it is the right approach for residential subscribers, but many gamers and small business subscribers will want the flexibility and power to customize the firewall for added levels of security and flexibility.

Security

➤ LAN Security with the Motorola Wireless Cable Modem Gateway Family

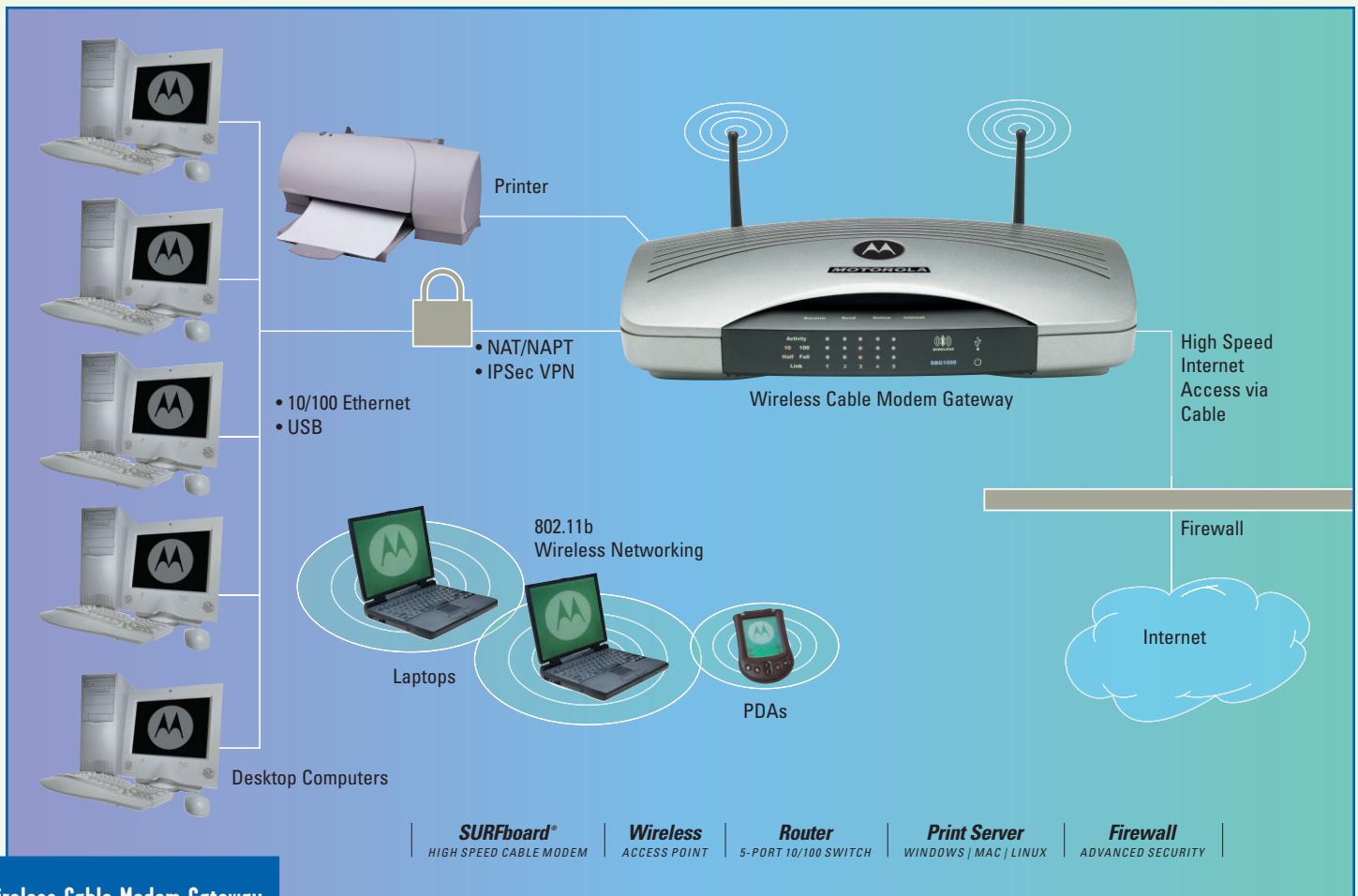
The Motorola Wireless Cable Modem Gateway Family allows cable subscribers to easily secure LAN resources.

The SBG1000 includes a robust, flexible and easy-to-use integrated firewall. This Data Over Cable Service Interface Specification (DOCSIS) cable modem provides unprecedented functionality in a single platform.

Subscribers can deploy this space-saving solution to connect to the cable network and safely allow both wired and wireless clients to share the broadband connection.

The Motorola SBG1000 Wireless Cable Modem Gateway even includes a print server so that residential users, SOHO subscribers and small businesses can reduce printing costs by connecting a single printer as a shared resource for Windows, Macintosh and Linux computers. Cable subscribers can easily deploy wireless LANs, wired LANs or hybrid wireless/wired LANs to share resources such as hard-drives, printers and peripherals while protecting each computer from outside intrusion. Only Motorola offers such a compact, secure and full-featured solution that allows cable subscribers to quickly and easily establish secure LANs connected to broadband cable networks.

It includes an 802.11b wireless access point that allows PCs to connect securely to the Internet without the need for expensive home cabling.



**Wireless Cable Modem Gateway:
Typical network configuration**

The Motorola SBG1000 includes a router with a five-port 10/100Base-T Ethernet switch that allows wired PCs to access the Internet and shared resources on the network. Future versions of the Motorola Wireless Cable Modem Gateway Family will include all of the features of the

SBG1000, and will also provide an enterprise-grade Virtual Private Network (VPN) endpoint so users can create secure, tunneled connections to corporate resources. *For more information, please download the VPN whitepaper available at <http://www.motorola.com/broadband/whitepapers.html>.*

Wireless Cable Modem Gateway Family

Features

► Advance Firewall Features on the Motorola Wireless Cable Modem Gateway Family

A Web-based graphical user interface simplifies configuration so the authorized administrator can create customized levels of security. The full-featured firewall capabilities of the Motorola SBG1000 come pre-configured so users do not have to be security experts to effectively protect their LAN. However, for those LAN connections that require increased security or flexibility, the Motorola SBG1000 can be easily customized to secure LAN resources to desired levels. It contains the following robust firewall features:

Network Address Translation

The Motorola SBG1000 Wireless Cable Modem Gateway is an ethernet router and it also supports Network Address Translation (NAT) so private Internet Protocol (IP) addresses within the LAN can be automatically mapped to the public IP address on the Gateway.

The cable operator issues an IP address to the SBG1000, which includes an integrated Dynamic Host Control Protocol (DHCP) server that issues dynamic IP addresses to computers on the LAN. Smaller LANs can add PCs simply, or in larger LANs network administrators can create a NAT table that does the global-to-local and local-to-global IP

address mapping. The use of NAT allows increased security since different levels of security can be defined for each IP address on the LAN. Private IP addresses within the LAN are hidden from the public Internet because external users only see the IP address of the SBG1000.

The Motorola SBG1000 Wireless Cable Modem Gateway's implementation of NAT supports multi-session IPsec VPN passthrough as well as H.323 video conferencing standards. Authorized users can take advantage of the built-in IPsec support to establish secure VPN tunnels to enterprise resources. Multiple tunnels can be established at a single time and multiple users can each establish a tunnel. For example, a husband and wife on separate PCs can tunnel into their respective employers' VPNs at the same time using the SBG1000.

As broadband connections deliver increased bandwidth to the home, video conferencing is becoming more widely deployed. Intelligence within the Motorola SBG1000 Wireless Cable Modem Gateway will identify video conferencing sessions using the H.323 standard and allow them to be established through the firewall so authorized users can establish secure video conferencing over the Internet. Firewall features within the SBG1000 will create an opening to allow the H.323 sessions to be securely established so video conferencing tunnels can be easily established.

Stateful Packet Inspection

The Wireless Cable Modem Gateway Family maintains stateful information for every TCP/IP session at both the network and transport layers. It monitors all incoming and outgoing packets, applying policies to each one while screening for improper packets and intrusion attempts. The Motorola SBG1000 inspects and analyzes the state of each traffic flow and offers programmable filters so authorized users have the flexibility to optionally enforce specific rules for port usage, blocking specific domains or implementing customized security levels. The firewall within the SBG1000 Wireless Cable Modem Gateway analyzes the relationships of the newly created session so new protocols can be added to the firewall configuration. This allows maximum flexibility for supporting additional protocols and new services while maintaining a secure LAN connected to the Internet.

The Motorola SBG1000 Wireless Cable Modem Gateway comes pre-configured but users can also customize stateful packet inspection to address the following parameters:

- IP address and port numbers
- Packet count and byte count
- Sequence and acknowledgement number
- Time stamps
- Payload modification history
- Dynamic association
- Other identifying information requested by the LAN administrator

Intrusion Detection

Attempts to infiltrate the LAN are monitored and repelled by the Motorola SBG1000, which includes extensive intrusion detection features to prevent unauthorized access. If the system suspects that an external party has attempted to crash through the firewall, it will attempt to identify the IP address of the potential culprit, prevent access, log the event and automatically generate an e-mail to the LAN administrator with information about the intrusion event. This information can even be shared with the cable operator to help identify hackers and filter them off the cable access network.

The firewall within the SBG1000 Wireless Cable Modem Gateway analyzes the relationships of the newly created session so new protocols can be added to the firewall configuration.

Wireless Cable Modem Gateway Family

Denial of Service Attack Prevention

With the expansion of the Internet we often hear about Denial of Service (DoS) attacks harming major Web sites. Yahoo, Amazon and even the White House Web sites have all been shut down by DoS attacks as publicly reported in 2000. A DoS attack is an incident in which users or organizations are deprived of the services they would normally expect to have operational. In the worst cases, LAN services may be temporarily forced to cease operations or an intruder may gain access onto the LAN to corrupt processing resources to support other malicious attacks.

Although DoS attacks are usually intentional and malicious, they can happen accidentally and they can cause major damage to LAN computers and require a great deal of downtime. These attacks can range from buffer overflow attacks, in which more traffic is sent to the LAN than it can handle, to Smurf attacks, in which the perpetrator sends an IP ping to computers on the LAN specifying that they broadcast to a number of hosts so there will be innumerable ping replies that flood the LAN so it can no longer receive or distinguish valid Internet traffic.

The Motorola Wireless Cable Modem Gateway Family comes pre-configured with extensive features for preventing DoS attacks. Stateful packet inspection features monitor traffic flows in real time for both LAN sessions and Internet access sessions. The SBG1000 Wireless Cable Modem Gateway detects misuse of LAN resources and flags anomalies that may, in fact, be suspicious traffic. It can be customized so future DoS attacks can be catalogued and added so the LAN can be protected for the long term. It also offers blockers for the following DoS attack types, as well as over 20 additional attack types.

- SYN flooding
- TCP hijacking
- LAN attack
- WinNuke
- Christmas tree
- SYN/FIN
- BackOrifice
- Net Bus
- Smurf
- ICMP flooding
- Trojan Horse

DMZ Hosting

A Demilitarized Zone (DMZ) is a neutral zone between the private LAN and the public Internet. It opens up a computer for clear, non-secure connections to the outside, and the machine becomes vulnerable to security threats.

The SBG1000 monitors all incoming and outgoing packets, applying policies to each one while screening for intrusion attempts.

Because there are no security prevention safeguards in place, there are also no potential link impediments either. The use of a DMZ may therefore be desirable for specialized applications, such as File Transfer Protocol (FTP) or Web servers. The DMZ Hosting feature allows one local computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming and video conferencing.

The Motorola SBG1000 Wireless Cable Modem Gateway serves as a DMZ to enable firewall security of protected LAN resources. It not only offers NAT but also has Network Address Port Translation (NAPT) to identify source ports. For example, the firewall supports multiple popular gaming protocols, including Quake, Unreal Tournament, Hexen and EverQuest. The LAN administrator can easily add support for a new gaming protocol so online games can be established through the firewall. The private LAN can remain secure, yet these specialized sessions can be easily established.

Resources

► The Efficiency of Shared Resources with the Security of a Firewall

The Motorola SBG1000 Wireless Cable Modem Gateway allows secure LAN connections to shared broadband networks. It is a complete, out-of-the-box firewall solution

that combines vigorous security with compact, full-featured wired and wireless networking.

This “plug ‘n’ play” solution comes with default settings including a firewall that addresses the needs of most users but can be easily configured and customized to support even more rigorous levels of security. The Motorola SBG1000 Wireless Cable Modem Gateway offers the mobility of a wireless LAN and the flexibility of multi-port Ethernet — behind the security of a firewall. Motorola, the leading supplier of cable modems worldwide, offers “plug ‘n’ play” router connectivity so multi-PC homes, SOHO and SME business customers can cost effectively share high speed Internet connections.

The Motorola SBG1000 Wireless Cable Modem Gateway is available from both cable operators and retail channels and is backed by the quality and reliability offered by Motorola. Additional networking accessories are also available from Motorola, including:

- 802.11b client cards for wireless access to the Motorola SBG1000
- 802.11b Universal Serial Bus (USB) adapters for adding wireless capabilities to a desktop computer
- External wired diversity high-gain antenna for extending the reach of the wireless LAN

Residential users, SOHO customers and SME businesses alike can deploy secure wireless and wired LANs while managing the safety of computing resources and the privacy of personal and business information.

Integrated firewall capabilities allow users to secure LANs while gaining the peace of mind that comes from knowing that their information and resources are well protected.

