Firewall Technologies

This section discusses several types of firewalls and describes the firewall services provided by Novell BorderManager 3.7. It contains the following subsections:

Firewalls are a combination of hardware and software that reduce the risk of a security breach into a private intranet. An effective firewall between the intranet or private network and the Internet, or between intranet segments, enforces corporate security and access control policies. A firewall also helps regulate the type of traffic that can access the intranet and provides information about that traffic to the administrator.

You can set up your firewall to deny access to a private network from the Internet, but to allow access to the Internet. Or you can allow some access from the Internet, but only to selected servers for e-mail or general corporate information.

The purpose of a firewall is to create a system that prevents unauthorized users from accessing proprietary information. As previously mentioned, designing an effective security policy that meets your needs requires careful planning and consideration of your objectives. This section focuses on understanding the firewall portion only.

The Open System Interconnection (OSI) model shown in the following table provides a view of each layer mapped to the corresponding Internet firewall technologies. Some technologies span more than one layer. Higher levels in the OSI model provide a better or finer capability of controlling data that enters your network, at the expense of performance. Lower levels require less time to route data but sacrifice security for performance.

OSI Layer	***Firewall Technology***
Application	Virtual Private Network (VPN) Internet Object Caching
Presentation	VPN
Session	VPN
Transport	VPN IPX/IP and IP/IP gateways Packet filtering
Network	VPN Network Address Translation (NAT) Packet filtering
Data Link	VPN Point-to-Point Protocol (PPP) Packet filtering
Physical	Not applicable

Types of Firewalls

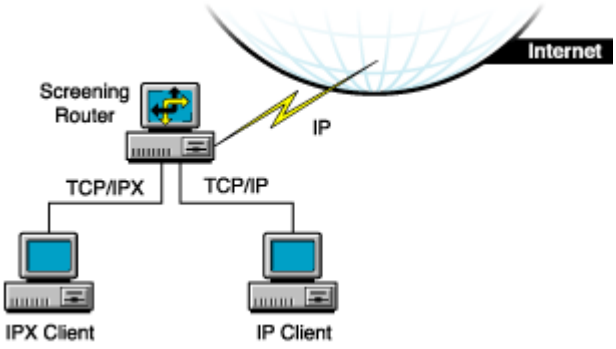
Although a firewall is sometimes referred to as a single technology, it is actually a combination of several services that work together as a protective layer to ensure a secure network border. These technologies build on the basic security already available in many Internet services. Firewalls provide security for services that do not have security, for example, e-mail. Firewalls also protect hosts. There are several basic types of firewalls:

- Screening routers
- Bastion hosts
- Dual-homed hosts
- Screened hosts
- Screened subnets
- Tri-homed hosts

Screening Routers

A screening router is the most basic type of firewall and uses only the packet filtering capability to control and monitor network traffic that passes though the border. Screening routers on a server with packet filtering can block traffic between networks or, for example, traffic to or from specific hosts on an IP port level. For example, you can let employees on your intranet use Telnet, but bar any Telnet activity from the Internet. Direct communication is usually permitted between multiple hosts on the private network and the Internet. The following figure shows a basic example of how a screening router works.

Figure 1
Firewall Using Screening Routers



The risk of break-in is large with this type of firewall: each host on the private network is exposed to the Internet and is still a potential break-in point. Unauthorized users can detect and use internal addresses to access information within the firewall. To avoid break-in, screening routers can be set to look at the source address of each incoming IP header instead of the destination address, and drop private addresses that come from the Internet.

Bastion Hosts

A bastion host represents the private network on the Internet. The host is the point of contact for incoming traffic from the Internet, and as a proxy server allows intranet clients access to external services.

A bastion host runs only a few services, for example, e-mail, FTP, Domain Name System (DNS), or Web services. Internet users must use the bastion host to access a service. A bastion host does not require any authentication or store any company-sensitive data.

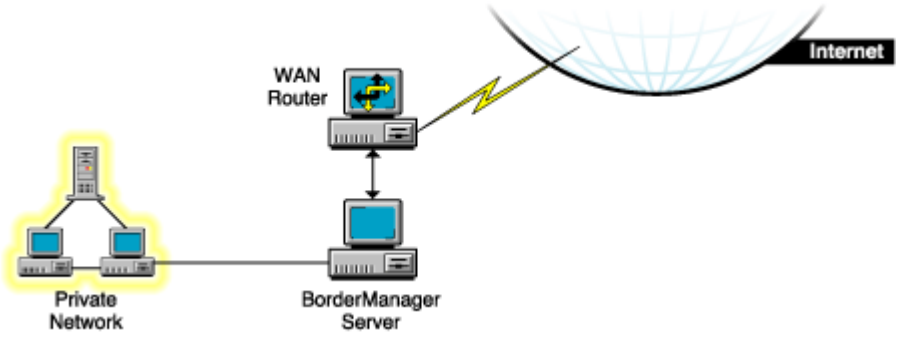
Dual-Homed Hosts

A dual-homed host is based on a server with at least two network interfaces. The host acts as a router between the network and the interfaces to which it is attached. To implement a dual-homed host type of firewall, the routing function is disabled. Therefore, an IP packet from one network (for example, the Internet) is not routed directly to the other network (for example, the intranet). Systems inside and outside the firewall can communicate with the dual-homed host but cannot communicate directly with each other.

A dual-homed host blocks direct traffic between the private (protected) network and the Internet. The following figure provides an example of a configuration in which a WAN router provides general WAN connectivity, packet filtering, and access to the Novell BorderManager 3.7 server. Private network users can access the Internet by using Proxy Services and the Novell IP Gateway, which are running on the Novell BorderManager 3.7 server.

The router allows traffic only to and from the Novell BorderManager 3.7 server. Break-in is limited to other hosts reachable from the Internet, although any illegal access severely compromises security.

Figure 2
Dual-Homed Host Firewall



Screened Hosts

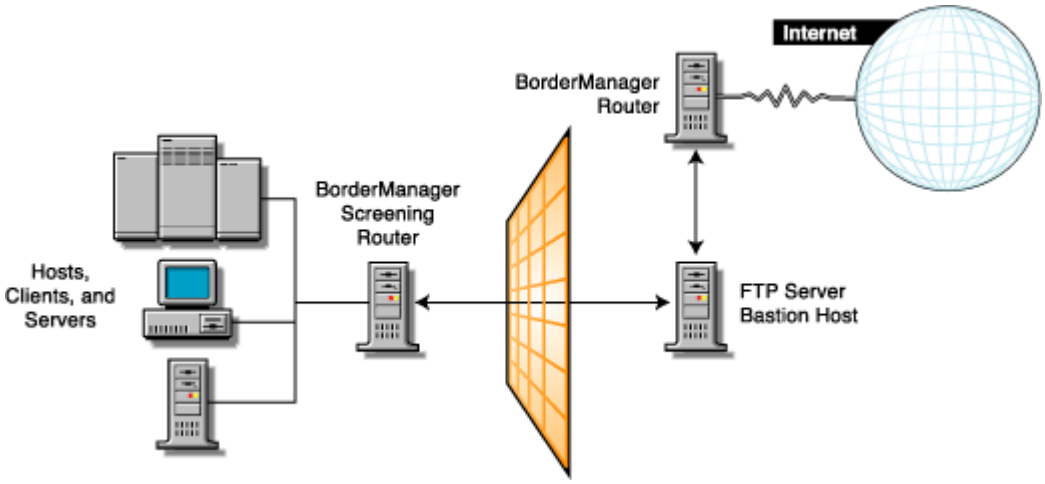
A screened host uses a combination of a bastion host and a screening router, as shown in the following figure. The screening router adds security by providing Internet access to deny or permit certain traffic from the bastion host. It is the first stop for traffic, which can continue only if the screening router lets it through.

For additional security, you could set up a bastion host for each type of service: HTTP, FTP, and e-mail. The screening router will then send the corresponding traffic to the appropriate bastion host.

In this example, the Novell BorderManager 3.7 server and the WAN router can be reached from the Internet. In addition, the Novell BorderManager 3.7 server acts as a screening router on the private network. Using Network Address Translation (NAT) and packet filtering, the Novell BorderManager 3.7 server can be configured to block traffic on specific ports, and only a select number of services can communicate with it.

This type of firewall is fairly secure because security risk is limited to the Novell BorderManager 3.7 server.

Figure 3
Screened Host Firewall

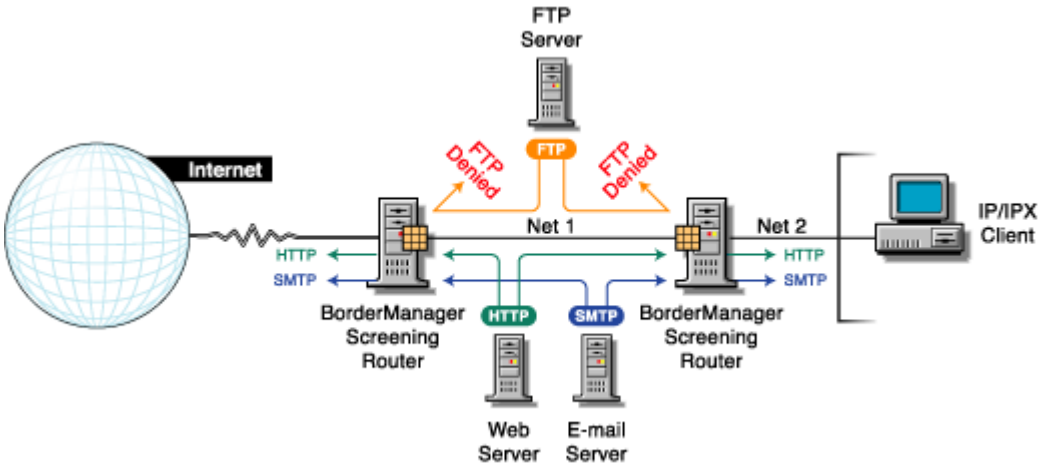


Screened Subnets

The screened subnet is a variation of a screened host. In screened subnetting, the bastion host is placed on its own subnetwork. Two screening routers are used to do this: one between the subnet and the private network (with the bastion host) and the other between the subnet and the Internet. The first screening router between the private network and the screened subnet denies all services from crossing into the subnet. The screened subnet allows only specified services. An example of a screened subnet firewall is shown in the following figure.

In this configuration, the Novell BorderManager 3.7 server is used as a proxy server. Both IP routing and IP forwarding are disabled to prevent any direct access between the private network and the public Internet.

Figure 4
Screened Subnet Firewall

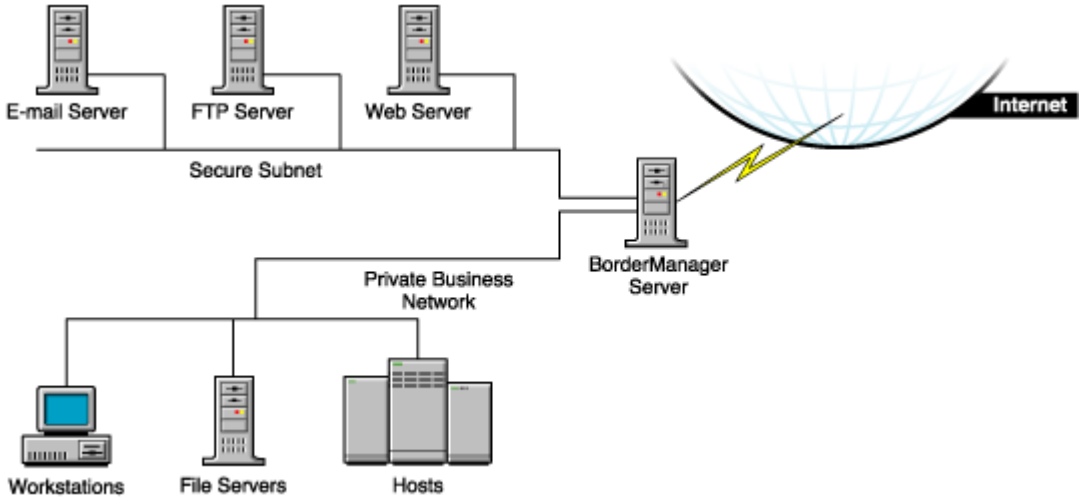


IMPORTANT: Although a firewall focuses on the restriction and use of internetwork services, for a complete security access policy you must consider all other outside network access, including dial-in lines and SLIP/PPP connections.

Tri-Homed Hosts

A tri-homed host combines elements of a screening router and a screened host, thereby overcoming the limitations of each. Security is centered on the screening routers by using interfaces for the Internet, the intranet, and the subnets that contain the bastion hosts and application servers. An example of a tri-homed host is shown in the following figure.

Figure 5
Tri-Homed Host



Types of Firewall Technologies

The technologies that create a firewall service include packet filtering, NAT, circuit-level gateways, application proxies, and VPNs. The security and efficiency of these technologies and services vary, depending on their efficiency and sophistication.

Packet Filtering

Packet filtering is the basic method for protecting the intranet border. Packet filters work at the Network layer of the OSI model. The limitation of packet filtering is that it cannot distinguish usernames.

Packet filters filter data based on service type, port number, interface number, source address, and destination address, among other criteria. For example, a packet filter can permit or deny service advertisements on an interface. You can use incoming and outgoing filters to dictate what information passes into or out of your intranet.

Network Address Translation

Network Address Translation (NAT) maps private IP addresses to public IP addresses. NAT can perform this mapping both dynamically and statically. An alternative to NAT is a circuit-level gateway.

Circuit-Level Gateways

A circuit-level gateway works at the Session layer in the OSI model, which means that even more information is required before packets are allowed or denied. Access is determined based on address, DNS domain name, NDS or eDirectory username. Special client software must be installed on the workstation. Circuit-level gateways can bridge different network protocols, for example, IPX to IP.

Your username is checked and granted access before the connection to the router is established. Compare this with NAT, where only the private source IP address is used to gain access. Here again, NAT performance is greater than circuit-level gateway performance. However, circuit-level gateways are more secure.

Application Proxies

In a circuit-level gateway, after a virtual pipe is established between the client and host, any application can be used across the connection. The reason is that circuit-level gateways cannot determine the application-level contents of packets being sent between the client and host during a transmission. An application-level proxy works as a proxy server to intercept information running across a gateway, preventing direct communication between the client and the host.

An application proxy is specific to an application, for example, an FTP proxy or SMTP proxy. An application proxy accepts only packets that are generated by protocols that the proxy can copy, forward, and filter.

Virtual Private Networks

Virtual Private Networks (VPNs) allow two hosts to exchange data using a secure channel. The data stream is encrypted for security. A VPN can be configured as a connection between two endpoints or between many endpoints. You can connect two offices over an Internet connection, or connect several offices to create a secure private network. Remote VPN clients are also supported.

Novell BorderManager Firewall Solutions

The previous sections describe the firewalls and firewall services that are currently being implemented in the industry in general. This section describes the firewall services provided by Novell BorderManager 3.7, and explains how you can effectively use Novell BorderManager 3.7 as part of a comprehensive and versatile solution to your security policy.

Novell BorderManager 3.7 firewall services provide increased security through three levels of firewall protection, including packet filtering (Level I firewall), circuit-level gateways (Level II firewall), and application proxy services (Level III firewall). In addition, Novell BorderManager 3.7's Network Address Translation (NAT) services can allow unregistered intranet IP addresses to connect to the Internet and, at the same time, conceal these addresses from outsiders. Also, Novell BorderManager 3.7's Virtual Private Network (VPN) services deliver secure, encrypted connections over the Internet, eliminating expensive leased lines.

A firewall can consist of several components. Novell BorderManager 3.7 provides a comprehensive firewall solution that includes the following services:

- Packet filtering
- Novell IP Gateway
- Network Address Translation (NAT)
- Proxy Services
- Access control
- SOCKS 5 for authentication and SSL for encryption services
- Virtual Private Network (VPN)
- Alerts for specific server conditions

IMPORTANT: To use Novell BorderManager 3.7 to secure your network border, you must specify a public IP address. Public IP addresses specify server interfaces to a public network, typically the Internet. Public network interfaces are not secure. Private IP addresses specify server interfaces to a private network, or intranet.

Packet Filtering

Packet filters provide network-level security at the router by permitting or denying packets based on a predefined set of rules. Novell BorderManager 3.7 supports Routing Information Protocol (RIP) filters and packet forwarding filters to control the service and route information for the common protocol suites, including IPX and TCP/IP.

A packet filtering router, for example, can filter IP packets based on the source or destination IP address and the TCP/UDP port number, and can filter based on the source or destination interfaces. Filters can also block connections to or from specific hosts or networks and to specific ports.

Specific services and protocols can also be filtered. For example, X Windows System*, RPC, and rlogin services should be blocked because they can create an open threat to corporate security. Refer to Packet Filtering Overview and Planning for more information on packet filters.

Novell IP Gateway

Novell BorderManager 3.7 comes with two circuit-level gateways---IPX/IP and IP/IP---and a SOCKS service. Together, these services are called the Novell IP Gateway. The Novell IP Gateway provides a form of address translation to add an extra layer of security. The gateway monitors traffic between an intranet and the Internet.

The Novell IP Gateway provides circuit-level security by enabling IPX and IP clients on your local network to access the Internet without your having to assign globally unique IP addresses to each local system. If each client is already assigned a unique address, the Novell IP Gateway enables you to hide the IP addresses of your local network from the Internet.

The Novell IP Gateway also uses the eDirectory software and access control to manage connectivity to the Internet. eDirectory-based access control can be used to restrict access to particular files on the Internet. Authentication can be based on the type of service and time of day, and the user can be authenticated at a container, group, user, or server level.

To use the Novell IP Gateway, your clients must be running the latest Novell Client™ software or a SOCKS 4 or 5 application, and the gateway service must be enabled at each workstation. Note that Windows applications that do not use WinSock cannot use the Novell IP Gateway.

For detailed information on the Novell IP Gateway, refer to Novell IP Gateway and NAT Overview and Planning.

Network Address Translation

NAT offers several advantages over the Novell IP Gateway: it does not require special client software and can be used by hosts on any platform that use the gateway as a route to the Internet. NAT enables any IP host on your local network to access the Internet without your having to assign globally unique IP addresses to each system.

Novell BorderManager 3.7 provides both dynamic and static IP network address translation. For static IP address translation, tables are defined with sets of public IP addresses. These are then used to map the source addresses of packets being sent through the firewall to their public addresses.

NAT also acts as a filter, allowing only certain outbound and inbound connections. The type of filtering that occurs is determined by whether NAT is configured to operate in dynamic or static mode.

For detailed information on NAT, refer to Novell IP Gateway and NAT Overview and Planning.

Proxy Services

Proxy Services provides application-level security by providing application proxies that forward and filter connections for such services as HTTP, Gopher, FTP, SMTP, RealAudio*, and DNS. In general, Proxy Services allows services only for which there are proxies. For example, if a gateway has a proxy for FTP, then only FTP is allowed into the protected subnet; all other services are blocked.

HTTP proxy improves performance by locally caching frequently requested Internet information and optimizing WAN bandwidth use. The client (browser) makes a request directly to a proxy, which locates the object in its cache and returns the object to the client. If the object is not in the cache, the proxy retrieves it from the origin Web server on the Internet, stores it in the cache, and returns the object to the client. Benefits include reduced Internet traffic and reduced request load on the object source, which in turn reduce delays in returning information to the client.

Proxy Services also allows protocol filtering. You can set up the firewall to filter FTP connections and deny use of the FTP put command. This can be useful if you do not want users writing to an anonymous FTP server.

When using the proxy server (or gateway), you can hide the names and addresses of internal systems---the gateway is the only hostname known outside the system. Also, traffic can be logged before it reaches the internal hosts. Proxy Services improves security by hiding private network domain names and addresses and sending all requests through a single gateway.

For detailed information on Proxy Services, refer to Proxy Services Overview and Planning.

Access Control

Access control controls Internet and intranet access at the Application layer by allowing or denying access requests made through proxy servers, Novell IP Gateways, and VPNs. By controlling access at the Application layer, you can attain a higher level of security than you can with packet filtering, which controls access only at the Network layer. Access control can also use usernames instead of source or destination IP addresses.

Access control involves establishing a set of rules. Each time an access request is made, the Novell BorderManager 3.7 server searches for the rules that apply to the request. If no rule is found, the request is denied (the default). You can create access control rules at the Country, Organization, Organizational Unit, and Server object levels. Rules can be based on criteria such as users, groups, IP addresses, or services. With access rules, you can control access to network and Web services, Novell IP Gateways, proxy services, VPNs, and URLs.

In general, firewall security should provide the following levels of access control:

- Host control---Determine which hosts can be accessed.
- Application-level control---For example, allow access to the Web but prevent access to news groups.
- Content control---Determine which network files and information can be accessed.

For detailed information on access control, refer to Access Control Overview and Planning.

Virtual Private Networks

A VPN is used to transfer sensitive company information across an untrusted network, such as the Internet, in a secure fashion by encapsulating and encrypting the data. For site-to-site VPN, only the VPN members must be running the VPN software; for client-to-site VPN, the VPN client must also be running the VPN software.

Client-to-site VPNs can use two types of secure connections:

- Direct dial-in connections
- Internet Service Provider (ISP) connections through the Internet

Site-to-site VPNs can use the following types of secure connections:

- Between two departments within the same company using the company's private network, or intranet
- Between two or more sites within the same company using the Internet
- Between two or more different companies using the Internet

Both intranet and Internet site-to-site VPNs can be deployed in one of two ways:

- With the VPN member on the border between your private network and the public network
- With the VPN member behind a high-end router that is on the border between your private network and the public network

For more detailed information about VPNs, refer to Virtual Private Network Overview and Planning.

Source:
https://www.novell.com/documentation/nbm37/?page=/documentation/nbm37/over/data/ae70nts.html