

# Featured Article

## Firewalls in Networking

### March 2006

Typically, when people first mention network security the first thing they think of is a firewall. Firewalls are the front line when it comes to securing networks. They can stop attacks originating from within your network as well as those originating from the outside. Firewalls have several tools to protect your network including Network Address Translation (NAT), Port Address Translation (PAT), Access Control Lists (ACLs), and DeMilitarized Zones (DMZs).

### Differences in Network Address Translation and Port Address Translation

Firewalls can use NAT to allow one address on one interface to be translated to another address on a different interface all the time or only under certain circumstances. The two most common types of NAT are dynamic PAT and static NAT.

Dynamic PAT is probably the most widely used form of NAT. PAT takes a group of private IP addresses and lets them all talk to the Internet through one public IP address. This is extremely useful when there are small numbers of public IP addresses available. For example, looking at Figure 1, every computer on the inside is translated to the same IP address (207.157.15.6) when communicating with the Internet. Using PAT, each internal IP address is assigned a port on the one public IP address. The port assignment is done dynamically, and since every IP address has more than 65,000 ports, there is no worry about running out of ports. Also, since port translations are not static, they will expire after a certain amount of time. PAT provides a basic level of security to inside networks because there is no way for a malicious machine on the Internet to initiate a connection directly to one of the private IP addresses.

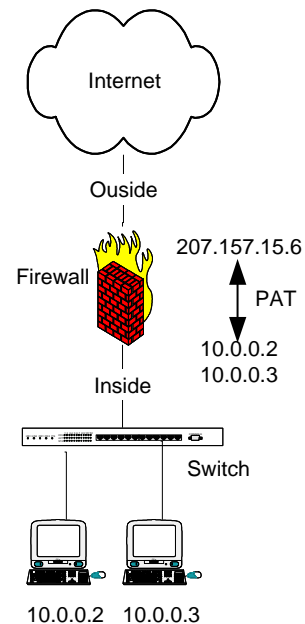
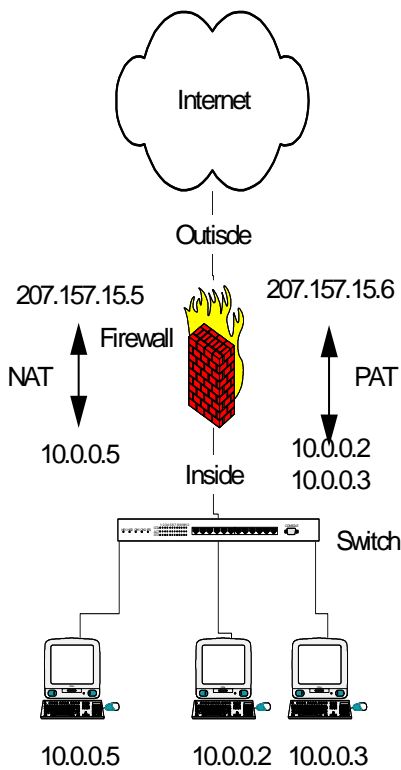


Figure 1

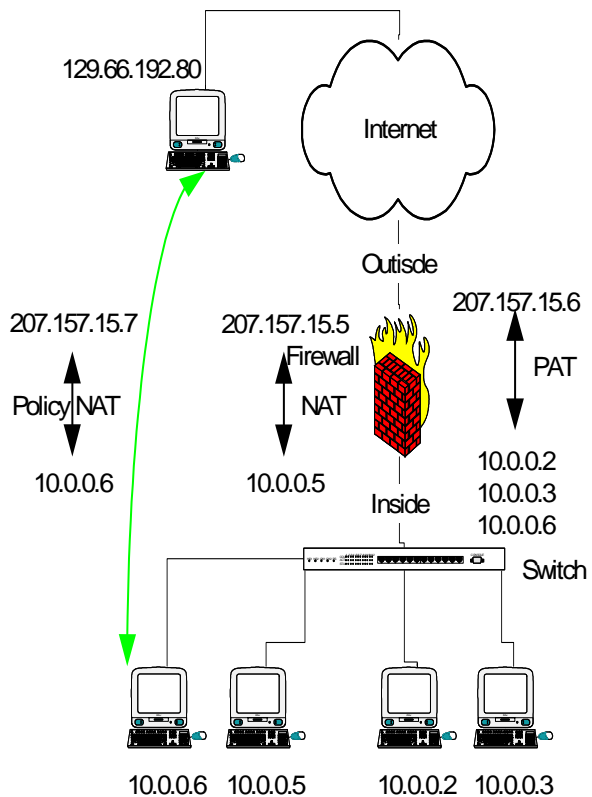
Static NAT is different from PAT in that it simply translates one IP address to another IP address. This is useful when there are machines on the inside network that need to be accessed from the Internet, (i.e. web and FTP servers). In Figure 2, 10.0.0.5 has a static NAT to 207.157.15.5, meaning that every machine on the Internet has direct access to 10.0.0.5 through the address 207.157.15.5. Static NAT can also be applied for specific traffic, and this is called Policy

NAT. Considering Figure 3 for example, using Policy NAT, 10.0.0.6 can be translated to 207.157.15.7 only when talking with 129.66.192.80 (represented by the green line). In this case, 10.0.0.6 could be translated using PAT when talking to the rest of the Internet. One possible use of policy NAT is when there is a LAN-to-LAN VPN connection. Both the VPN and the Internet connect through the outside interface. In this case, an IP address on the inside of the network would need a private IP address on the network on the opposite end of the VPN, and it would need a public address when talking to the Internet.

Since static NAT dedicates an outside IP address to an inside machine, it is not as secure as PAT. ACLs must be used to control access to these public addresses to have any security at all.



**Figure 2**



**Figure 3**

## Securing Networks Using Access-List

Access Control Lists (ACLs) are probably the most versatile tool that firewalls have for securing networks. ACLs are used by the firewall to secure its individual interfaces, either collectively or separately. They act as filters allowing certain traffic to pass, while denying other traffic. For instance, one ACL can allow the inside IP address 10.0.0.2 to send web traffic to the outside IP address 129.66.192.80, while it also denies web traffic from 10.0.0.2 to anywhere else. Likewise, that same ACL can deny only mail traffic from 10.0.0.2 to 129.66.192.80 while allowing 10.0.0.2 to send all other traffic to 129.66.192.80. It is important to note that if 10.0.0.2 has a static NAT, the firewall must be configured to block incoming traffic to that NAT address or else there is a much higher risk of being attacked. For example, if 10.0.0.2 is a mail server and it is statically translated to 207.157.15.5, there must be an ACL to prevent the Internet from initiating all connections to 207.157.15.5 that are not related to email.

Another key feature of firewall ACLs is that they are stateful. Stateful means that the firewall remembers the requests that pass through it for a specific amount of time, and it knows what type of response to expect. ACLs take advantage of this because they don't require reverse access to be configured on the ACLs of the other interfaces. For example, if a machine on the inside of the network requests a web page from the Internet, the destination machine is automatically allowed to respond back to that source machine. Without a stateful ACL, the web page would not be allowed to come back through the firewall unless another ACL on the outside specifically permitted it.

## Using DeMilitarized Zones on Networks

As mentioned before, using NAT provides a direct path for internet users to attach a machine. Even using ACLs to protect it, a mail server can still be attacked if mail is used to attack it. What if the mail server gets broken into? It's on the inside and can attack other inside machines. What if an inside user attacks the mail server? The firewall never sees the traffic between two machines on the same interface. This is the exact reason for firewall DeMilitarized Zones (DMZs). DMZs provide the ability to separate the inside network into independent zones. Often firewalls will have one or several DMZs. Each DMZ is its own network with its own interface on the firewall. Since it has its own interface, it can use NAT or PAT, and has its own ACLs. With this flexibility, servers can be separated from the

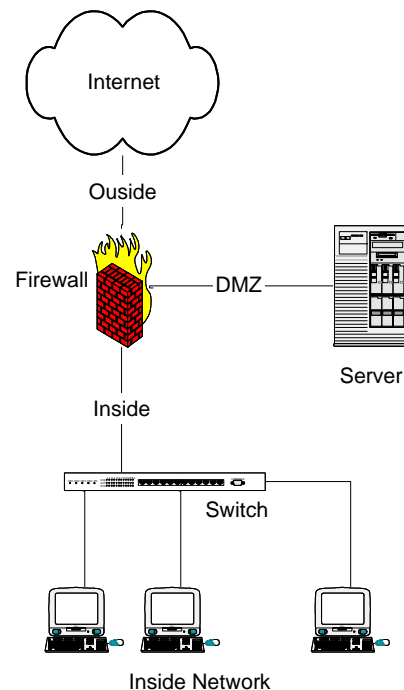


Figure 4

inside network. This allows the inside to use PAT, which is more secure than NAT, and it allows the firewall to protect the servers from both inside and outside users (see Figure 4). If properly configured, the ACLs that separate the DMZs from the inside can prevent the spread of some viruses from the inside network to the servers in DMZs and vice versa.

## Virtual Private Networks

Beyond the security that a firewall provides to the local network, firewalls can also provide a secure means of accessing your local network when you are away. This is accomplished using a Virtual Private Network (VPN). There are two main types of VPN connections; LAN-to-LAN connections and client-server connections. A LAN-to-LAN VPN provides a permanent connection between two networks that allows the two networks to talk to each other as if they are physically connected. A client-server VPN connection allows one machine outside the firewall to connect to the inside network. ACLs must be applied to VPN connections so that the connections over the VPN can only access certain IP addresses. VPNs are a great tool to allow outside access to and internal network without simply opening the firewall to the whole Internet. However, it is important to note that VPNs merge two separate networks. Therefore they also merge the risks associated with each network.

## Do's and Don'ts of Firewalls

While firewalls are great security devices, there are several things they don't do. Firewalls are designed to permit and deny traffic, not route it. That being said, firewalls typically do have some basic routing ability built-in. However, they are not intended to be the core of your network. Firewalls will not prevent end-users from downloading viruses, malware, and spyware. However, they can help prevent the spread of these types of software between interfaces through the proper application of ACLs. Also, firewalls are not spam filters. The only effect firewalls have on email is how mail servers talk to the outside world through the firewall. Finally, and most importantly, firewalls do not configure themselves. Simply installing a firewall inline with an Internet router will either block all traffic, or allow all traffic, depending on the firewall's default configuration. Neither is acceptable. The true value of any firewall is found in the expertise of the person setting it up, and the staff who will maintain it. For this reason, when installing a firewall, it is important to seek the assistance of an experienced professional.

Firewalls are the first line of defense when it comes to protecting your network from external threats. Through the proper application of the tools provided, firewalls can secure servers from internal threats, prevent the spread of malicious software, and allow secure access to and from internal networks.