

# What makes a firewall?

The following was taken from a post I made to the private Microsoft Trainer Newsgroups. I have not edited it, so if it sounds like I am responding to something... I was. ☺ Someone had made the comment that the Linksys DSL Routers were firewalls, which I disagreed with. I did some research to support my statements and what follows is what I found.

\*\*\*Begin Post\*\*\*

I hear you. Now that I have a few extra minutes (OK, this has become an extra few hours), here is an abridged (OK, it has become a detailed) firewall definition that I think is the "defacto" standard definition used by the industry. I say that because of the references, RFC's and whitepapers I used as research.

The term "firewall" at it's most simplistic definition is a network devices that enforces an access policy between 2 networks. This definition has been further expounded upon to define a firewall as a device that protects a trusted network from an untrusted network, which possesses 3 qualities:

1. All traffic must pass through it in any direction.
2. Only authorized traffic, defined by the security policy, actually can pass through it.
3. The system is highly resistant to penetration.

Now for the details.

A router which posses the ability to do content filtering could be construed as a firewall, but only in the most simplistic and loosest of definitions. This is due to the fact that while a packet filtering router may very well filter data, it is an entirely different question as to whether/how well it can log such filtering decisions, etc. The packet filtering router also typically does not do a very good job of meeting the 3rd qualifier above. As a result, a packet filtering router is rarely termed a firewall on it's own, but rather as part of a firewall system with the router acting as a forward filtering host and a filtering gateway acting as a backend filtering host. See diagram:

Internet---Router---DMZ---Filtering Gateway---Trusted Network

So let's look at the definitions in more detail.

Packet Filtering Firewall - This generally refers to a firewall that can filter data based on the Source or Destination IP address and/or TCP/UDP port. It is of note that almost all firewalls do packet filtering to some degree. The drawbacks to packet filtering firewalls tend to be the difficulty in configuring them, and the relative inability to verify that the rules are functioning properly. In addition, packet filtering firewalls do not tend to have very robust logging capabilities making it difficult to detect if dangerous packets are being permitted.

Application Gateways - This generally refers to a firewall that, while it may do everything a packet filtering firewall can do, has the additional ability of being able to forward and filter application layer services, where as packet filtering firewalls tend to not function on data above layer 3/4. This manipulation of data is referred to a proxying of data, and application firewalls are sometimes known as proxy firewalls (not to be confused with Microsoft Proxy Server or similar products). In this case, the application firewall will only allow traffic for which it has a proxy. When used in conjunction with packet filters, a much more secure scenario can be created as follows:

Inet---Router---AppFirewall---Trusted  
|  
WebServer---DMZ---FTPServer

In this case, lets say a user wants to FTP to a server on the DMZ. The user requests an FTP session using the AppFirewall as the target. The packet filtering router/firewall will only allow the packets through it that meet it's rules. The AppFirewall then gets the request for FTP access and a connection between the user and the AppFirewall is created. The AppFirewall has a proxy for FTP and only FTP. When it gets the FTP

# What makes a firewall?

request the AppFirewall may or may not authenticate the user and creates a connection between the AppFirewall and the FTPServer on the behalf of the user. It is important to understand that the user and the FTPServer NEVER have a connection with each other directly. The proxy will then pass the data between the 2 connections. See below

Actual: User<--->AppFirewall<--->FTPServer  
Logical: ^-----^

If someone were to attempt to connect to the webserver, since the AppFirewall does not have a proxy for the web, that traffic is dropped. The benefits of this are many and varied, but some of the biggies are:

1. Better logging. AppFirewalls tend to have much more robust logging capabilities since they can log data up to layer 7.
2. Hide information. Since the user never connects to the host, the host can effectively be completely hidden from the user.
3. Authentication. AppFirewalls can require authentication for proxied connections.
4. Less complex filtering rules. Since all inbound requests go to the AppFirewall, a filtering router/firewall can simply allow traffic to the AppFirewall only and deny everything else.

One of the biggest drawbacks of application firewalls is that if there is not a proxy for the application you wish to permit, an application firewall will block that traffic. This puts the admin at the mercy of the vendor to develop and deliver proxies in a quick and timely fashion.

Packet Inspection - A packet inspection firewall combines the packet-filtering and application-gateway to provide a high degree of access control due to the ability to deal with packets at all 7 layers if needed. As one would expect, this comes at the cost of simplicity. In addition, packet inspection firewalls can actually inspect the contents of the packet to integrate all the data from all the layers to ensure that, as best can be determined, the actual data in the packet is consistent with the type of packet it claims to be. For example, instead of simply accepting that a packet destined for port 80 is HTTP, a packet inspection firewall can actually verify that the data actually is consistent with what is expected in an HTTP datagram throughout all layers. This provides a tremendous amount of granularity in terms of filtering risk.

Packet inspection firewalls can also typically perform two other types of inspection/filtering. The first is called a stateful inspection method of filtering. With stateful inspection, the firewall takes into account the state of the connections they are handling to match incoming packets with outbound requests (inspecting the state of the communication that has been occurring, hence stateful inspection). As a result, a rogue packet to a non-existent outbound request would be blocked, since there is no previous communication to determine the state of the current inbound connection request. The other method is session filtering. Session filtering takes this process one step further by controlling the network session instead of the individual packets. Essentially this allows the administrator to create fewer rules to define access, since the firewall knows that an outbound session which is permitted (rule #1) is going to have an inbound session in the opposite direction, thus not needing a second rule. This is sometimes called using "smart rules". The biggest benefit is the efficiency of rules processing, since there are fewer rules that need to be checked.

However, since the packet inspection firewall allows the packets to pass through the firewall, as opposed to application firewalls that actually recreate the packets, it may be deemed as actually being a less secure solution than an application firewall in some cases. This takes us to the next category.

Hybrid Firewalls - Today, many of the better commercial firewalls no longer fall cleanly into the realm of a packet filtering, application or packet inspection firewall. Instead, they are hybrids, mixing, matching and combining features from all of the types. This is not to say that since they do more methods of security that they are actually more secure. Rather it simply means that the admin has more flexibility.

This has all lead to an even more specific list of requirements that is considered the esoteric requirements of all devices which are considered firewalls.

# What makes a firewall?

1. Support a "deny all, permit only" policy.
2. Support, as opposed to impose, a security policy.
3. Accommodate new services as needed.
4. Contain advanced authentication measures, or the hooks for installing those measures if needed.
5. Log access to and through the firewall
6. Flexible IP filtering capabilities including, but not limited to, source and destination IP address, protocol type, source and destination TCP/UDP port and inbound/outbound interface.
7. Mail gateway capabilities

So now that we have gone through the theory, what makes a firewall? TrueSecure, formerly ICSA, has developed a firewall testing criteria that is generally recognized as the most complete firewall certification process out there. Rather than reprinting the details, the criteria that is used for certification of a firewall can be found at:

[http://www.icsalabs.com/html/communities/firewalls/certification/criteria/criteria\\_3.0a.shtml](http://www.icsalabs.com/html/communities/firewalls/certification/criteria/criteria_3.0a.shtml).

In a nutshell, the criteria requires that a firewall have the following capabilities:

1. Ability to set a policy that is enforced at all times. This includes inbound, outbound permitted and all other denied policies.
2. No special software should need to be installed on the client, with the exception of management machines.
3. Logging capabilities are required. At a minimum it must log events based on the security policy, certain data elements (date, time, protocol, source and destination IP addresses, etc.), precision date/time logging, human readable output, event correlation in the case of multiple logs (conditional), and the ability to log to an external server (conditional).
4. Administrative functions must exist on the firewall allowing the security policy to be specified, logging to be enabled, and remote administration (conditional). All administration functions shall require password or stronger authentication. If remote admin is permitted authentication of the remote station should include more than just the IP address of the client. If remote admin is possible from a public client, the session needs to be encrypted and/or one time pass or strong authentication is required. Finally, remote admin needs to be able to be disabled if desired.
5. Services that are not enabled by the security policy must not function, but any services that are enabled must function properly.
6. Unauthorized admin access must not be possible.
7. It should not be vulnerable to any vulnerabilities that are known and capable of being tested at the time of testing. It should also ensure that the firewall does not introduce vulnerabilities.
8. No traffic other than that which is specifically permitted in the security policy should be allowed to pass.
9. The firewall can not be rendered inoperable by any trivial denial of service type attacks.
10. If the firewall is rendered inoperable through a DoS attack for which there is no known defense, the firewall MUST fail closed.

OK, so here you are at the bottom of all this mess wondering "what kind of a loser spends his Friday evening typing this". Well, if you have gotten this far you should know that the term "firewall" is a broad term. Is a packet filtering router a firewall? Possibly. There have been qualifiers added to the definition to try to give a better definition. This is due largely to the nature of the devices we speak. They provide security. As such, they should be treated with the most narrow focus we have. Otherwise, we are really being irresponsible with security out of the gate. For many things, that doesn't matter. But for security, a broad focus in cases like this can, will and does contribute to people implementing solutions thinking they are being secure, when in reality they are not. A point could be made that a false sense of security is worse than no security, because a false sense of security causes people to relax. This in turn can cause the damage to be greater when the security, or lack thereof, has been breached. It is for this reason, and this reason alone, that we as trainers MUST not lead our students into a false sense of security. We need to be specific enough to make sure our students understand that when they get a packet filtering router, it is NOT a firewall, unless it can meet the various definitions and qualifiers listed above.

# What makes a firewall?

So... about this Linksys router... "The Linksys Instant Broadband EtherFast Cable/DSL Router is the perfect option to connect multiple PCs to a high-speed Broadband Internet connection or to an Ethernet back-bone. Allowing up to 253 users, the built-in NAT technology acts as a firewall protecting your internal network."

So what does NAT do? It translates addresses. That's it. This is defined in RFC 3022 <ftp://ftp.isi.edu/in-notes/rfc3022.txt>. You will note that security is not guaranteed with NAT. At best, NAT provides some privacy. Since NAT prevents the use of IPSec, a strong argument can be made that NAT is actually \*less\* secure than not using NAT at all. Furthermore, RFC 2663 <ftp://ftp.isi.edu/in-notes/rfc2663.txt> goes through various security consideration of NAT in section 9.0 and makes it extremely clear that NAT is NOT a firewall or security consideration. While NAT in conjunction with ALG's and/or firewalls provides additional security, NAT alone is NOT secure and is in fact susceptible to most DDoS attacks (this alone should rule out the Linksys as a firewall).

From the user guide FAQ: "With which type of firewall is the router equipped? The Cable/DSL router uses NAT and TCP/IP port inspections."

OK, I have already picked NAT apart, but port inspections... well, that is marketing speak. The router can do packet filtering based on port numbers. It does NOT actually inspect the packet in any way, per the definition of packet inspection above. So... the router claims that 2 things make it a firewall. NAT, which doesn't make anything a firewall by RFC and port "inspections" which is an over glorified way of saying "we do packet filtering". So, let's hold on to the packet filtering (I'll give them that for now) and continue picking this thing apart.

"Does the Router do Stateful packet inspection? No".  
Well, what more can I add to that?

So what about the other items that define a firewall. So far, the router does packet filtering. That may or may not meet the first 2 most basic qualities of a firewall. Data must be able to pass, but only authorized data can pass. Quite frankly, I don't know how well the Linksys security policy is, but based on their lacsidasical definition of security so far, I don't put too much faith in it. However, the definition of the filtering rules has been expanded to include filtering by source and destination IP address, TCP/UDP port, protocol type and inbound/outbound interface. The Linksys can only do IP address and/or TCP/UDP port packet filtering. Which means that the Linksys can perform packet filtering in only 2 of the 4 scenarios required. Remember how I gave them packet filtering... I take it away now.

For grins though, we will take a look at the 3rd most basic quality of firewalls. It must be highly resistant to penetration. Well, I can not find any documentation what so ever that says the Linksys is not susceptible to any trivial denial of service type attacks. Lack of documentation to the contrary is as good as documentation that it is susceptible to DoS in this particular case. And even if I haven't convinced you prior, this last point causes the Linksys to fail to meet the third of the most basic qualities that all firewalls possess. By my count though, they fail to meet 2 for sure, 3 IMHO. I guess "data must be able to pass" is still true...

And the advanced definitions? Well here is another quote: "Does Linksys provided syslog support? No, Linksys does not currently provide syslog support."

Well... logging is also required by all firewalls, so here is another nail in the coffin, and quite frankly the last one I will reach for.

So, here I am, thousands of words later and I will say it again. The Linksys router is NOT a firewall. Doesn't matter how you cut it, if you use the definitions of a firewall which are recognized throughout the industry, there is no way to come to the conclusion that the Linksys is a firewall. Packet filtering router? Sure. Packet filtering router with NAT? You bet. Firewall? No way. No, there is no room for opinion here. The only possible way one could disagree is if they decided to make up their own definition of what makes a firewall... kind of like Linksys did in the first place. ;-)