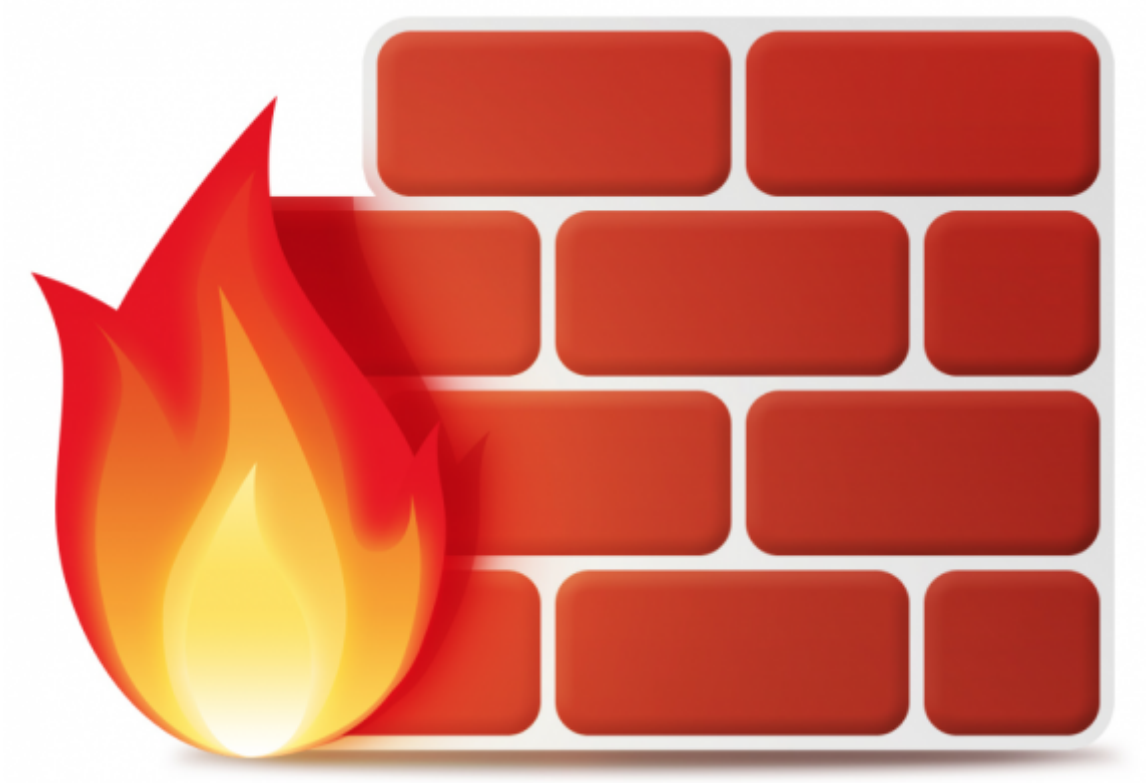
Firewalls



You can ask five different people what a stateful firewall is, and you're likely to get at least four answers. The truth is there are only a few types of firewalls — the rest are simply variations. The firewall vendors, however, would have you believe otherwise.

Packet filtering, Circuit-Level Gateways, Stateful Inspection, Application-Level Gateways, Deep Inspection — all these terms are thrown around quite liberally by various companies trying to sell their next offering. As a result, these terms have lost much of their meaning.

Remember that there are only 7 layers of the OSI model; it's not as if *truly* new concepts are being invented. All the buzzwords you hear spewed about are the result of overactive marketing departments — not engineering breakthroughs.

My goal here is to give a picture of firewalling that will allow one to map vendor buzzwords to understanding — to be able to take an arbitrary description of a technology and match it up with what's *really* going on. It's my hope that after reading what lies below you'll never be confused about firewalls again.

Basic Packet Filters

As a general rule, the more advanced the firewall technology, the higher up in the OSI Model it works. The first and most basic type of firewall to come about is simply referred to now as a packet filter. These firewalls worked at the 3rd level of the OSI model, aka the network layer.

Packet filters worked primarily off of two paramaters within packets — the source and destination IP addresses — but they were able to look at (and filter on) the protocol field in the IP header as well.

The key here, however, is that very few checks were done on packets, and they were only done at the network layer. As a result, it has become somwhat trivial to trick these sorts of filters via various techniques. Spoofing, fragmenting, and various other sorts of tinkering allow an attacker to get traffic through simple packet filters that they were set up to block.

One advantage of packet filters, however, was (and is) their speed. Because they perform so few checks they are able to do so quite efficiently.

Proxy Firewalls

One of the most interesting and powerful types of firewalls is the proxy firewall. The main thing to remember when considering proxy firewalls is the fact that they initiate a second connection from themselves. In other words, when a request is made for a resource that's handled by a proxy firewall, the original reqest does not make it back to the host in posession of the resource. *The proxy* makes the request to the resource and then returns the information back to the client.

This is a highly secure way of doing things because it allows one to filter out a large amount of potentially malicious content within the original request. For example, imagine that there is 150,000 areas in a request that can be tampered with by an attacker — some of which could create a security issue on the host being targeted. Well, if only 10 pieces of information are needed to make a legitimate request, the proxy knows this and can take those 10 things and make its own request. This way, when the proxy asks for the resource, the host is far less likely to be tricked into doing something it's not supposed to do.

Stateful Inspection

Without a doubt, "stateful" is the most misunderstood term used when it comes to firewall technology. People seem to attach some sort of quasi-magical meaning to it; it's like they just want to hear that whatever product they're using is "stateful".

Well, what does that mean exactly? What *is* a stateful firewall?

The term was originally coined by Check Point in reference to their Firewall-1 product, but the term is now used by virtually very firewall vendor in existence. A stateful firewall differs from a standard packet filter in a very simple way — *a stateful firewall deals with **connections** and their characteristics rather than packets individually.*

In short, stateful firewalls keep track of open, legitimate connections and compare traffic moving through the firewall to these known-good entries. The firewall knows all about the connections in its "state table" (the list of

legitimate connections) — and anything deemed not part of one on the list is discarded.

This was a major advance over basic packet filtering in terms of security. It suddenly became much more difficult to inject spoofed packets into legitimate connections and have them accepted by the firewall because stateful inspection looks at TCP sequence numbers, TCP Flags, etc. rather than just source and destination IP and port numbers.

Another thing that stateful inspection brought to the table was the ability to touch the application layer to some degree. The most commonly known example of this is the abilty to handle an FTP session — a complex task involving two seperate connections. Without being able to watch actual FTP traffic, the firewall wouldn't be able to deal with this level of complexity. This should not, however, be confused with true layer-7 visibility. The original forms of stateful inspection dealt predominently with layers 4 and below.

The most important thing to remember when discussing stateful inspecition, however, is arguably what it *isn't*. Firewall vendors have hyped the term to the point that it carries almost magical overtones. Don't fall for it. Again, stateful firewalls deal with connections rather than individual packets, and they build state tables that hold the connection information. Then they simply compare traffic moving through them to the contents of their state tables. *No magic.*

Some implementations do it better than others, of course, i.e. a SOHO Linksys box's stateful inspection is **not** equal to Firewall-1's stateful inspection, but the concept is basically the same.

Deep Packet Inspection

For the last few years it's been stateful inspection that's received most of the attention. As mentioned, every firewall vendor on the planet hurried to throw together an implementation just so they could say they had it.

Well, now there's a new player in town — *deep inspection*. Just as with stateful inspection, vendors are trying their best to make this technology

something it isn't.

To make a long story short, deep inspection is stateful inspection — but with visibility into the application layer. In other words, deep inspection allows the firewall to see the actual data passing through it rather than just keeping track of connection information. As mentioned above, many stateful inspection implementations allow for interaction with the application layer in certain circumstances, but that's not the main function of stateful inspection.

So what's the practical advantage of deep inspection over stateful inspection? Content filtering. Is the client that just made a connection to our webserver trying to propogate a worm? Is a website trying to install malware via an HTTP session?

These are questions that stateful inspection cannot answer and that deep inspection can. This is made possible by two technologies familiar to anyone in the IDS world — signatures, and anomaly analysis.

Once the firewall can see into the application layer fully, it can start matching what it sees against a list of known bad content. This is signature-based analysis, and it's the backbone of all antivirus technology. The advantage here is the ability to catch a whole lot of known nastiness, along with the relative ease of updates. The disadvantage would be the fact that, like in the AV world, the ability to stop unknown attacks is virtually nil, i.e. a new threat usually requires a new update. Anomaly analysis, on the other hand, works by establishing what's normal and then flagging traffic that strays from those boundaries. Theoretically this is quite powerful, but in practice it's often too hard to determine with any confidence what a "known good" baseline is. Without that, it's very difficult to to be able to say "this is bad because it's not normal." As a result, it's the signature paradigm that's dominated this space.

So that's basically what "deep inspection" turns out to be — a stateful firewall with content analysis that uses signatures and anomaly analysis. Sexy? Maybe. Magic? Not hardly.

Summing It All Up

The bottom line for all this is that there are only a few ways that firewalls work. Every type of firewall you have ever heard of likely falls into just three or four main categories.

Once you realize this it becomes much harder to get confused by the various buzzwords. So if I were to tell you that there's a new firewall out that does "über filtering", you should be able to ask a few questions.

What layer(s) of the OSI model do the firewall filter on? Is this simply another stateful firewall? If it has some application layer functionality, then how is it different from existing application filtering technology? After asking questions like these you'll often find that the creative engineering being sold is nothing more than creative marketing.: