

# What's In Your Firewall?

By **Bob Ayres, CISSP CISM**  
*bayres@symantec.com*

The murderous barbarian horde thunders toward an unsuspecting couple, blood lust and violence in their eyes. The couple unaware of their impending doom casually discusses their recent purchases. As the horde prepares to descend on the couple, the male asks, "Did you use ABC credit card?" The female replies, "No, the new XYZ credit card!" With this, the horde stops, defeated and sullen, their leader looks to the camera and asks, "What's in your wallet?"

If you substitute the barbarians for Internet evil doers, your management and company for the couple, and any number of firewalls for the credit cards you have a scenario that plays itself out everyday on your network. The question instead being asked is "What's in your firewall and are you really stopping the horde?"

Do you really know if your firewall is doing its job? Has it been configured to enforce your security policy or reduce the time your telephone rings? Are the features you highlighted to your management during your initial decision part of an integrated security posture or just bullet points on a glossy sales presentation? Ever tried to perform forensics on a security issue using the logs from your layered security architecture components?

For most companies, firewalls just enforce policy by whom or what is connected to which service. After the three-way handshake, any header information and the contents within that connection are invisible to the firewall. As attacks focus more on application weakness using blended threat exploits (any threat that uses multiple means of propagation such as Nimda), customers are requiring their firewalls to step up to the task. They want protection against these new types of threats.

In the past, customer firewall concerns focused mostly on questions such as speed vs. security, stateful vs. application proxy, next generation vs. hybrid. However in the last six months the leading stateful inspection firewall vendor has announced support for application intelligence and protocol standard compliance, features application proxy firewalls have had for years. Application proxy vendors added support for custom stateful rules years ago. More often than not, the sales pitch you hear from these different vendors address the same rather than different features.

With customers seeing firewalls as commodities and security perimeters becoming blurred, it is important that firewalls have the ability to look deep into the packet and application as well as move deeper into the network. In fact, your old firewall is now becoming the *security gateway* for the perimeter; a perimeter that is becoming more nebulous as it is placed deeper into your network infrastructure. Allowing data to be examined multiple times as it moves through your network with more or less granularity.

Even Gartner has recast their Firewall Magic Quadrant to reflect customer demands for the following:

## 1. Perimeter Security

2. Intrusion Prevention
3. Application defense
4. XML filtering

What are users to do now that each firewall vendors marketing sheets are distinguished more by their marketing department's style rather than the functions of the firewall? Well, instead of just firewall functionality we need to expend the increasingly complex security issues addressed by the firewall and the functions it needs to perform. The traditional firewall needs to evolve into today's security gateway.

In order to mitigate the risks faced today by IT organizations, a security gateway needs to perform the following functions and do them well:

1. Classic Firewall Protection
2. Deep Packet Inspection
3. Protocol Standard Compliance
4. Intrusion detection and prevention
5. Protocol Anomaly detection and prevention
6. Content Filtering
7. Virus Protection
8. Anti-Spam
9. IPSEC compliant VPN support
10. Dynamic delivery of Updates

**1. Classic firewall protection** is those commodity features we have come to expect: 1) A GUI with distributed management that is easy to use and that works. 2) The ability to do self hardening of the OS platform and firewall application so we can focus on network security access. 3) A combination of application proxies for well-known protocols and stateful inspection rule creation for those other protocols we require to do our business. 4) Scalable HALB (high availability and load balancing) designed to be integrated into the firewall OS and accommodate a hardware solution, as my throughput needs change. 5) Logging that is useful and detailed enough so that forensics follow up is enhanced not hampered. 6) In addition, of course they must have integration to centralized and scalable logging, alerting and reporting systems.

**2. Deep packet inspection**, the new buzzword for application compliance checks, includes circuit and application layer checks to determine adherence to expected usage. While application inspection is limited and always will be, protocol compliance should be done on all packets passing through a firewall, including VPN packets upon decryption.

**3. Protocol standard compliance** is the ability to look at every packet (IP, TCP, UDP, and ICMP) for adherence to RFC and expected usage. This lets you protect against attacks like SMURF (IP), Denial of Service (TCP), UDP flood, or Ping of death (ICMP) to name a few.

Combine protocol compliance with alerting on suspicious activity like port scans and service scans.

**4. Intrusion detection and prevention** using attack signatures, traffic rate monitoring, flow policy violation with IDS evasion handling to provide what are now classic IDS features.

**5. Protocol anomaly detection and prevention** is the next step in IDS, allowing it to move beyond signatures and interpret traffic flows, patterns and states. This enables the IDS to identify signature evasion and undocumented zero-day attacks in real time.

**6. Content filtering** on HTTP based applications with integration into industry-accepted services to allow automated updates.

**7. Virus protection** on HTTP, FTP and SMTP protocol based packets and attachments. Giving us the ability to repair or drop infected files, then log and inform us of the occurrence. Add to this a multi-threaded fast scanning engine to handle increasing volumes of traffic.

**8. Anti-Spam** features to block e-mail messages actively by subject line, file name attachment and size as well as known spam sites.

**9. IPSEC VPN support** for AES, 3DES and DES.

**10. Dynamic, automatic delivery of update**—This is probably the most important and least discussed or prioritized function of the security gateway. This is critical for current virus definitions, intrusion detection signatures and content filtering. For long term success, give this more than lip service; make sure it is accomplished by proven technology and process to ensure it happens when you need it most.

How does this all benefit the customer? I like examples, so let's follow a packet through a security gateway as it enforces security policy and helps stop viruses, malicious attacks, and blended threats.

First, the full inspection firewall, which allows administrators to set granular policies for complete control of information entering and leaving the network, performs deep packet inspection that drops and logs bad packets. If a VPN session is active, the proxy-secured, VPN technology decrypts the packet and drops it into the data stream.

Next, the security gateway performs session checks at the circuit layer. Again, it drops and logs bad packets. The integrated intrusion prevention and intrusion detection technologies block packets that contain threats, and automatically notify the firewall of malicious sessions from specific IP addresses. This will enable the security gateway to block specific sessions that contain threats or block specific IP addresses that continue to pose a threat.

The security gateway then opens and examines application layer protocol packets. These packets are checked to ensure conformity with the applicable RFCs and valid commands. Again, bad packets are dropped and logged.

If the packets are HTTP-based, content filtering technology compares the source IP against a list of prohibited Web sites. Prohibited content is dropped and logged.

If the packets are HTTP, FTP, or SMTP protocol based, files and attachments are sent to the virus scanner, which also actively blocks email messages by subject line text, file name attachment type, and message size. If a virus is found, the file is either repaired or dropped. All viruses are logged and a message is added to mail messages indicating that a virus was found and the attachment was deleted.

If all of these checks are passed, the security gateway allows the packet to enter or leave the network.

In the background it is imperative the security gateway perform timely updates of virus definitions, attack signatures, and URL filtering lists. This function all too often is ignored or passed over, however it is at the heart of an ongoing successful security management strategy.

Aren't we asking the security gateway to perform functions that may already be performed by standalone products? YES we are and should be; the security gateway of today must be up to the task in terms of performance, features and reliability. In fact the more you can identify and stop malicious attacks and viruses at the security gateway, the better your standalone products will work. By blocking more at your perimeter, the security gateway allows you to fine tune and focus your standalone security systems to your specific business needs. For those of us who do not have the luxury of additional security systems, security gateways enable comprehensive security management.

Too often our attempts to enhance security have resulted in excessive strain on an already over burdened staff. The deluge of access requests, updates, alerts and logs too often leads to a reality where security is ignored in favor of getting by. Many times, I have seen perfectly good network security systems powered off or ignored because of TMI (too much information). A security gateway helps to minimize this burden.

In life, there is no silver bullet, but you can have a game plan for success. Here are four topics to consider for successful security gateway integration. The answers and questions these produce will help you to plan for success.


**1. Security Policy**—Any security device is just an extension of your security policy. The more you understand what you are trying to solve, the more you see the pieces to your solution and the better you can mold those pieces to your solution. You require a security policy and game plan before you can quantify success. The result too often of not doing this is that we end up with pretty devices sitting in a room that go "ping", with little long term impact to our real issues.

**2. Horse Power**—Whether your security gateway is a software bundle or appliance, does it have the horsepower you need? What happens when you turn on all the features you require? Will the platforms support your data flow. The more you understand your data flow and you security gateway's performance, the better you can address price/performance and prepare for future growth.

**3. Auto Update**—Nothing is more critical than the ability to update your AV, IDS and content filtering signatures in a timely and trusted manner as time goes on. There are many options out there, so make sure you understand what your security gateway's update ability is and what it means to you to be successful in the long term. Sitting in a meeting with a blank face is not the answer you want to the question "Our vendor X released this signature months ago, why didn't we have it?"

**4. Periodic Review**—If you are not doing this now, it is time to think about it seriously.

Now is the time to look at your options for reviewing log files and configurations. This is a whole other topic, but the ability to track or benchmark traffic patterns, events and incidents then correlate these across your security devices helps to bring the big picture into focus.

The networks of today require a more comprehensive approach to defense. The rise of new and lethal blended threats demands it. Security gateways are your new weapon in the fight to give your business and staff the best chance to be successful. 

---

*Bob Ayres is a principal security consultant with Symantec. He has been helping to provide solutions for success to others in the high tech field since 1980. He can be reached at bayres@symantec.com.*