

# Cyber Security Writeup 1 Comments

## Features

Most of you did fine write ups. Almost everyone included description of the following features:

- The application identification classification (or app-id). This seems to be the key new feature where the firewall automatically deduces the protocol regardless of the port that protocol happens to be traveling over. This is certainly a strong feature. Though on reflection, this seems perhaps like an evolution from the intrusion detection/intrusion prevention technology.
- Decrypts and re-encrypts SSL traffic to allow for filtering of encrypted traffic.
- Active Directory integration. Support for some sort of user-based firewall is fairly standard via protocols like RADIUS and access control servers or AAA servers. Most AAA servers will integrate with AD, LDAP, etc.

Some of you noted the following features

- Custom hardware.
- Management or visualization tools, which all vendors provide to varying degrees.
- Device failover, a tricky although fairly standard features for firewalls at that price point.
- Real time threat prevention. Again, this is offered to varying degrees by many vendors. Many of you noted that they are able to do this threat prevention in a highly integrated manner which means that their processing only touches the packet once. Other vendors solutions place a scanning unit in the same box (perhaps sharing the same back plane), and so are not able to leverage common processing as well.
- Analyzing multiple packets in the stream to continue to verify the integrity of the traffic stream and recognize related traffic streams being negotiated. Most firewalls analyze multiple or all packets in the stream for at least some protocols. For example in the ASA/PIX family the inspect or fixup commands control enabling this proxy feature which will do this dynamic port analysis. Presumably the PaloAlto Networks solution performs this multiple packet analysis for a wider variety of protocols.

## IPv6 Support

Few if any of you could find any documentation about IPv6 support. Many of you noted that the PaloAlto Network's key technology rides above layer 3, but in the absence of documentation or personal experience most of you would be leery of being sure that the PaloAlto device processes the IPv6 protocol. Given that IPv6 is not yet widely deployed, I would not be surprised that PaloAlto Networks deferred IPv6 support so they could use their limited time to address more immediately relevant issues.

## Concerns

- Keeping the application ID signature database up to date. Correctly recognizing protocols is critical to the security of the “negative enforcement”.
- Are speed claims realistic?
- How does the SSL decryption work? If it is a proxy, how can a user be aware of the potential for a man-in-the-middle attack? What about employee privacy concerns?
- People eventually learn how to trick the application recognition signatures.

## Recommendations

Here is a numeric breakdown of your recommendations:

1. Buy with minimal hesitation: 5
2. Positive but need some more information: 6
3. Stay put but keep an eye on the technology: 4
4. Run away: 4
5. Shop more broadly: 1

Based on reading your reports, I'd tend to option 3. I think the application ID is an interesting change in orientation in the firewall space, but I am concerned about whether this can be done quickly enough. The concern of keeping the application signature database up to date is also concerning. I would also like to know a good deal more about the SSL decryption/encryption logic. If Bob Co had sufficient manpower, performing a hands on evaluation would be a good idea. Otherwise, staying put and keeping an eye on the technology sounds like the way to go.