

Cisco PIX 515E vs. Fortinet Fortigate-300

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-01/0143.html>

From: Jon (nospamj_at_i0ta.com)

Date: 01/02/04

Date: 2 Jan 2004 07:31:45 -0800

Greetings:

I recently prepared a small report for the company I work for evaluating the Cisco PIX 515E and the Fortinet Fortigate-300. In researching my report, I found very little in the newsgroups comparing the two products. So, I thought I would post my report here for others to reference.

This was not a formal report so I didn't cite all my reference sources. All the quotes came from <http://www.fortinet.com> or <http://www.cisco.com> or from marketing material put out by the respective companies.

Enjoy the report and hopefully you will find it useful. :-)

Firewall Evaluation

Cisco PIX 515E vs. Fortinet Fortigate-300

Jon - 1/2/2004

For the past few weeks I have been evaluating two firewalls to determine which one would fit the needs of the Florida office and our own Schaumburg office. The two firewalls are the Cisco PIX 515E and the Fortinet Fortigate-300. Here is an overall evaluation of the two products.

Firewall Capability

Cisco 515E: Cisco is a good company that stands behind its products. Their PIX firewall is a very secure product and performs its duty as a firewall very well. According to the performance statistics on Cisco's website, the 515E can support clear text throughput of 188 Mbps and concurrent connections of 130,000.

Fortigate-300: Fortigate is a lesser-known company than Cisco, but has made quite a few waves in the firewall community with it's hardened, feature rich products. According to the performance statistics on the Fortinet website, the Fortigate-300 can outperform

the PIX by supporting 200Mbps and 400,000 concurrent connections.

VPN Capability

Cisco 515E: In April 2003, Cisco updated their PIX and VPN concentrators with a new VPN accelerator card called the VAC+. They began shipping it with the 515E's sometime in the summer. It has outstanding 3DES VPN throughput of 140Mbps, compared to the previous model's 63Mbps. It not only outpaces the Fortigate-300 in this category but any other firewall/VPN gateway in the class.

Fortigate-300: The Fortigate-300 also has very good hardware encryption/decryption. It is capable of supporting a maximum throughput of 65Mbps.

Ease of Administration

Cisco 515E: According to Cisco "the integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a Cisco PIX 515E Security Appliance—without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. A setup wizard is provided for easy installation into any network environment. Alternatively, through methods including Telnet and Secure Shell (SSH), or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX Security Appliances using a command-line interface (CLI)."

Cisco does not offer a demo version or any screenshots of its PDM. However, I did have the opportunity to see a demo of the latest version of Cisco's PDM at a local reseller. The PDM is actually a java applet that loads onto the workstation via a browser. The interface is somewhat intuitive, but more complex compared to the Fortigate firewall.

Fortigate-300: The Fortigate firewall has the most organized and intuitive interface of all the products that I have looked at. It is completely HTML web based and available to demo on their website at <http://www.fortinet.com/demo/index.html>. The Fortigate box includes all the administration capabilities of the Cisco box and adds a "Front-panel LCD and keypad" to "ease deployment by setting basic system parameters without an external console".

Intrusion Detection/Prevention

Cisco 515E: Since Cisco has a separate IDS (Intrusion Detection System) appliance, they didn't put too much effort into this category for their PIX firewall. However, they did add a number of intrusion protection rules. According to Cisco, the 515E uses "a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in

addition to looking for more than 55 different attack signatures, Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time."

Fortigate-300: Fortigate has both a built in IDS and intrusion prevention. Its IDS consists of a "customizable database of over 1300 attack signatures, which provides real-time warning and forensic data to identify and analyze attacks". On top of that, it features "active prevention of over 30 intrusions and attacks, including DoS and DDoS attacks, based on user-configurable thresholds". Version 2.80 of the Fortigate OS, due out in February 2004, combines the IDS and IPS into a single system capable of detecting and preventing nearly 1400 attacks.

Content Filtering

Cisco 515E: The Cisco PIX relies on 3rd party products for this.

Fortigate-300: The Fortigate box "processes all Web content to block inappropriate material and malicious scripts via URL blocking and keyword/phrase blocking". Fortigate allows you to either import your own black list from a free site such as SquidGuard or to subscribe to a service from Cerberian. It also features e-mail content filtering based on keyword/phrase and domain. Major e-mail filtering is included in the Anti-Spam section below.

Anti-Virus

Cisco 515E: The Cisco PIX relies on 3rd party products for this.

Fortigate-300: The Fortigate firewall "detects, quarantines, and eliminates viruses and worms in real-time. Scans incoming and outgoing email attachments (SMTP, POP3, IMAP), Web (HTTP) and FTP traffic, and encrypted VPN tunnels - without degrading Web performance".

Anti-Spam

Cisco 515E: The Cisco PIX relies on 3rd party products for this.

Fortigate-300: "In addition to the FortiGate systems' native content filtering functions for email [listed above under Content Filtering], FortiOS 2.8 provides enhanced capabilities to filter email content for Spam attacks. These features include services for checking and marking messages with Spam characteristics based on keywords and phrases in an email message's body and subject line, blacklists of known Spam senders, invalid return email addresses, MIME header checks, as well as blocking of SMTP Messages based on IP address blacklists, reverse DNS lookups, and checks against the Real-time Blackhole List (RBL) and the Open Relay Database (ORDB)."

Logging/Reporting

Cisco 515E: "Provides wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events." The previous statement found on Cisco's site is a bit misleading. Cisco's PDM has very nice real-time graphs, but is unable to store many log entries locally. Any historical reporting will need to be done by another device. Cisco admits to this later on by restating that the PIX can perform, "remote monitoring and logging capabilities, with integration into Cisco and third-party management applications".

Fortigate-300: The web interface provides real-time graphs on system performance, such as CPU, Memory, Hard Disk, Sessions, Network Utilization, Virus History, and Intrusions. "Logging capabilities are built into the FortiGate-300 through an internal, high capacity hard drive." Also, instead of having one main log, it is split into various groups: Traffic, Event, Attack, Anti-virus, Web Filter, and E-mail Filter. You can view the log through the web interface or logs can be sent to another machine via syslog.

Auto-Updating

Cisco 515E: The PIX is able to download new attack definition updates on a periodic basis from Cisco.

Fortigate-300: The Fortigate box receives updates to all its features (Anti-Virus, Intrusion Detection, Intrusion Prevention, and OS updates) pushed to it by Fortinet. According to the literature, "the FortiGate-300 is kept up to date automatically by Fortinet's FortiResponse Network, which provides continuous updates that ensure protection against the latest viruses, worms, Trojans, and other threats — around the clock, and around the world."

Price

Cisco 515E: There are different versions of the 515E. The Unrestricted version has the VPN accelerator card and more ports so that a DMZ could be created. The price quoted to us by a local reseller was \$5,636.58, plus \$29.90 for 3DES for a total price of \$5,666.48.

Fortigate-300: The Fortigate-300 includes all features available on the box and costs \$5,095.50, according to a local reseller.

Conclusion

Both firewalls are very mature stateful firewalls and although the firewall throughput is higher on the Fortigate box, I believe that both boxes would be more than sufficient for a single T1. Both firewalls have very workable administration interfaces (although the

Fortigate interface is more intuitive despite having more features). Both firewalls have comparable intrusion prevention. And, both firewalls are able to automatically receive updates. As far as general firewall features go, the two boxes are very close.

The difference between these two boxes comes down to two things: features and branding.

As far as features are concerned, the Cisco PIX has only one feature on its side: amazing VPN throughput. With the new VAC+ card that Cisco released in the 2nd quarter of 2003, the VPN throughput of the 515E more than doubles that of the Fortigate and most other VPN/firewalls that I have seen on the market.

The Fortigate on the other hand has several features that are not included or available with the PIX, namely: Intrusion Detection, Anti-Virus, Content Filtering, Anti-Spam, and Historical Logging. The Fortigate is made for small to mid-sized companies that want to have all the features that have traditionally only been affordable to larger companies in one easy to administer appliance. As far as features, the Fortigate definitely has the lead.

As far as branding, Cisco has a very reputable name and is extremely common in the market. In fact, many 3rd party products tout Cisco compatibility as a feature. Others use Cisco as the standard by which they develop products. Their support is also well known for being one of the best.

Cisco has been around since 1984 and quickly became well known in the Internet arena as a quality provider of routing equipment. In 1993, it began to make acquisitions into other areas of networking starting with switching equipment. In 1995, it acquired NTI (http://newsroom.cisco.com/dlls/1995/corp_102795.html) which produced a box that it called a Private Internet Exchange (PIX). Cisco integrated some of its router IOS commands into the PIX, but left many others unchanged. That's the reason why I was previously frustrated with the command line of the PIX 506. Even though I'm a CCNA and know the routers quite well, the PIX did not behave the same. In 2000, Cisco acquired Altiga (<http://newsroom.cisco.com/dlls/fspnisapi56bb.html>), which is largely responsible for Cisco's entrance into the VPN market.

Fortinet doesn't have as much history or isn't as well known. Fortinet was founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen (founded in 1997). The company is listed as a "Visionary" in the latest Gartner Report. It is doubtful that Fortinet will simply abandon its product line and disappear. Fortinet is an up-and-coming company with a great product.

My Opinion

Either firewall would be suitable for our location(s). They both have pros and cons. The decision depends on what is important to the company. In my opinion, it is important that the company take security more seriously. Viruses, worms, and other attacks are increasing in number and complexity each year. We need a firewall that will handle all aspects of security threats, not just one that will block IP addresses and port numbers. In order to do that the firewall has to take on the role of virus scanner, intrusion detector, content filter, attack watchdog, etc... The Fortigate firewall is meant to be that all-in-one appliance.

Florida Office: VPN throughput is a concern here. However, I'm not certain that the difference between the Fortigate's 65Mbps and PIX's 140Mbps of VPN throughput will be noticeable through a 1.544Mbps T1 Internet connection (or even 2 or 3 T1s). The Fortigate's VPN throughput should be more than enough. Beyond that, I certainly don't think that VPN throughput outweighs the benefits of the many other features that are available in the Fortigate appliance. These are features that the Florida office could and really should be using.

Schaumburg Office: The Schaumburg office ISP is protecting us from many things, but it is by no means comprehensive. Mc.net should be seen as more of a broadsword whereas a firewall appliance such as the Fortigate performs at a much deeper level. Mc.net provides outbound content filtering for one of our IP addresses and inbound e-mail virus and SPAM filtering for 3 of our domain names. That is about the extent of the protection they provide us through their Managed Secure service. They provide no intrusion detection. They provide very little intrusion prevention. Mc.net's policies in general are formulated to support everyone on their network. If we wish to get specific, we need to do that with our own equipment.