SMS IT Group

www.smsitgroup.com

213.222.5182

Written by Scott G. McCarthy

sgm@smsitgroup.com

How to Select a Firewall

Revision 2, September 2014

SMS IT Group
www.smsitgroup.com

How to Select a Firewall

About the author: *Scott G. McCarthy is the Director of SMS IT Group in Los Angeles, CA. Mr. McCarthy has been programming and supporting firewalls for over 15 years. He has literally programmed and supported almost every major firewall brand on the market between his two security related positions. Mr. McCarthy can be reached at sgm@smsitgroup.com or at the SMS IT Group at 213-222-5182.*

About this Guide

I have literally used almost every commercial firewall on the market at this point with the exception of a small handful. I worked for an IT security company that programmed and supported almost every type of firewall out there and I was in the unique position to use almost every firewall made. Today, I still work for an IT company that has a security division and continue to support a wide variety of firewalls for businesses. I have started to use a semi-open source firewall you will read about below.

For some reason, firewalls provoke a very emotional response in people. Maybe it's because they are such vital pieces of equipment and one mistake can ruin your job or network. Or maybe it's the fact that once people learn this complex piece of equipment, they don't want to go through the learning curve on another device. Firewalls are pretty easy to learn but the detailed nuances can be tricky to master. A firewall is definitely not something you want to have a mediocre level of knowledge because your lack of knowledge can cost your company dearly.

I also find there is quite a bit of misinformation out there about firewalls. Many vendors rely on big names to mask the shortcomings in their firewalls and others have incredible features with a terrible name, reputation or not enough marketing muscle. Regardless, I am writing this article to shed some light on the firewall market and cast aside many of the myths and misnomers that exist in this market. It's very rare that the average IT person gets to program more than 1-2 firewalls so I hope this guide will help educate and be a starting point to select the right device or software for your network. This guide is also going to be brutally honest and not so politically correct so it may upset you, some vendors or others and all I ask is that you keep an open mind. It is written based on my own personal experience and nothing more.

Types of Firewalls

Over the years, firewalls have gone from simple devices that block ports and IP traffic to fully functioning universal content management devices and everything in between. In an effort to gain market share and keep up with the competition, firewall vendors have continually added more features which have been both good and bad. Firewall vendors have also tricked customers or quietly advertised features only for the customer to find out the feature he was interested in requires an additional purchase and yearly subscription. You have to be careful and do your homework. Some firewall features take a great deal of time and effort for the vendors to provide and may be well worth the purchase price.

Firewalls generally fall into two main categories: **1. Traditional firewalls** and **2. UTM devices** aka Unified Threat Management. Traditional firewalls focus more on core port blocking and performance using packet filters and NAT. They lack features such as web content blocking, antispam, or other higher level content analysis. UTM devices are firewalls that have the ability to inspect traffic at the application layer and can provide proxy functionality. A traditional firewall is only smart enough to know that there is traffic coming in and it needs to go through a specific port. For example, traffic for a website will need to go to port 80 generally and the traditional firewall will direct that traffic from the Internet into the proper web server via port 80. That's all it knows; it acts as a basic packet filter.

A UTM device not only knows the traffic needs to go through port 80 but can also read the data in the packets. Not only does the firewall know the traffic needs to go through port 80 but it also knows what exactly is in the packets. As an example, a UTM firewall can read through the web server traffic request and make sure it's a legitimate request and not some hacker sending fake HTTP calls to the web server to try and hack it. This firewall can also read through email (SMTP) traffic and ensure the email being sent or received through the firewall is a legitimate email and not junk or someone trying to relay or spam through the email server.

Over the years, UTM devices have become increasingly sophisticated. A good UTM firewall can be programmed to block all traffic that is related to Skype or to block all users from trying to download any .EXE files or others from using any type of instant messenger. The programming is limited only by your imagination. UTM devices are also able to provide "proxy" rules that act as mini servers when speaking to the Internet host. Instead of a traditional firewall simply taking the email request and forwarding it through to the email server, a UTM with a proxy rule can speak to the host and determine whether or not the host is trying to send through legitimate traffic. If not, the proxy will drop or block the host. This functionality takes the responsibility of blocking bad hosts from the server to the firewall and adds an additional layer of security. For example, if a spammer is trying to use your Postfix server to send a bunch of spam, the proxy server SMTP rule can act as an additional layer of protection to ensure the spammer doesn't abuse your email server.

I could write an entire paper just on this section but given the focus of the article, I am going to move on.

Brands & Comparisons

Personally, I see no reason to purchase traditional style firewalls anymore unless you only need basic port blocking and NAT functions with enormous bandwidth throughput. Even if you don't use many UTM features, you can always disable them. If you ever need them, they are there. Some argue the firewall should be separated from UTM. Some companies put Cisco ASA firewalls in place which typically don't have many UTM features and then install a separate content management system such as Websense that is designed to control to make sure employees aren't browsing porn all day. The Cisco ASA handles the traditional firewall functions and the Websense server handles the content management. To me, this is a very old and outdated approach and also very expensive.

When you go down that road, the downside is that you lose a level of integration between Websense and the ASA rule set. There is no way to truly integrate the rule with the Websense properties completely. Below is a screenshot (figure 1) of a SMTP Proxy rule from a WatchGuard XTM330 firewall. You can see it has the traditional port rules. Then take a look at the expanded rule set (figure 2) for the same rule and you will see you can control every aspect of the SMTP traffic. You can control everything from the header length to the size of the attachments. Not only that, you can define or customize the headers you want the proxy rule to accept or deny. It's powerful because you can combine this rule with the antispam engine and have total control over every element of email coming in and out of your network.

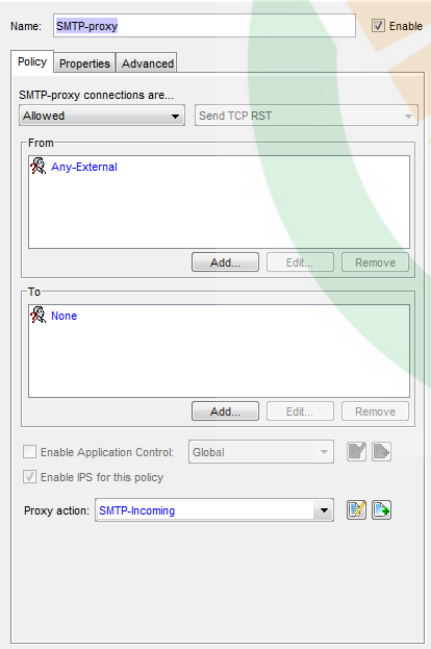

Figure 1 - WatchGuard SMTP Proxy

WatchGuard, Fortinet, Untangle, SonicWALL and Checkpoint all have excellent UTM engines and allow you to get extremely granular with your definitions. I am personally not a big fan of the ASA's UTM features because they rely too heavily on 3rd parties and the interface can be extremely complex and cumbersome to figure out. Out of all the vendors, I feel that Untangle, WatchGuard and Check Point have the best UTM feature sets on the market.

Fortinet is probably one of the most feature rich firewalls on the market and gives you excellent value for the money but the tradeoff is that the interface is extremely complex for a GUI. SonicWALL has an excellent easy to use interface but I feel that SonicWALL falls short in terms of granularity and is sometimes too basic for a medium sized business firewall.

My own personal favorite in terms of UTM features, functions and management tools is Untangle followed by WatchGuard. I believe Untangle delivers an amazing set of UTM tools and allows you to get extremely complex with the firewall config but keeps the GUI simple enough so you don't get lost in the details. Untangle uses modules to add additional functionality and there are dozens of modules to choose from. The application security layer control is ridiculously powerful and easy at the same time. With WatchGuard, HostWatch (figure 3) is an incredible tool that gives you a graphical representation of everything going

on in the firewall. It is a great tool to see if you are being attacked or the traffic you want blocked is actually being blocked. I know this tool is unique to WatchGuard and something SonicWALL, Fortinet and others lack. Untangle has a version of this but it lacks the true graphical representations. Untangle and WatchGuard also allows you to "blacklist" IPs based on rules and AI logic. For example, if someone pings you, you can automatically block that IP for a pre-set amount of time (IE. 10 Minutes). Let's say a hacker is trying to port scan you. You can block that person for 20 minutes and make it almost impossible for him to accomplish anything malicious.

WatchGuard didn't get my vote because I am often frustrated by the lack of stability of their devices. Last week, one of my WatchGuard's got hit with a DDOS attack via DNS and it brought the box down immediately. I had to add a rule in the firewall to block the DNS requests so it would not crash. I was able to block the attack given the WatchGuard's powerful rules but the box should have never crashed to begin with. Over the years, I have also noticed that their VPN connections are less than stable compared to an ASA or others. The one thing a Cisco ASA will deliver is stability. If you need a firewall that will never drop a VPN connection, ASA is your box. Cisco seems to be ultra conservative and error on the side of stability vs. features.

Untangle and WatchGuard also lack Geo Protection which Check Point offers. Check Point is a very mature firewall and has an amazing set of tools and IDS features. It is the only firewall that has impressed me with their ability to block traffic based on countries or locations. When I was consulting for a law firm, we found that most all the hacking attempts were coming from China and Iran. Since they didn't do business in either country, we simply told the Check Point to block traffic from those countries – problem solved! The complaint most often heard related to Check Point is how expensive it is. Check Point has been around a long time and is a great product but very expensive. Although they are expensive, I have never heard anyone complain they ever went wrong buying a Check Point. Check Point is very powerful, has excellent tools, is stable, and scales from small business to large enterprise easily. If you have the budget, you need to seriously consider Check Point. The only downside is that Check Point is probably the most expensive firewall mentioned in this document.

One other new element that has recently entered the market is open source or half open source firewalls. Years ago, I never considered using an open source firewall because they were just too basic and there were too many show stoppers every time I tried them. There are a couple out now that are good but not great. The one I mentioned before is **Untangle.** Untangle is an open source firewall you can download for free and run on your own box. The company sells premium add-ons you can purchase for

$500 a year. I run an Untangle firewall in my office and have been able to use it without the premium add-ons with no issues. More later.

WatchGuard – Runner Up

WatchGuard is aimed at both the small, mid and enterprise markets with their dedicated appliances. The bright red boxes are well built and extremely high quality. WatchGuard's are often referred to as feature rich high value devices. The unique feature of a WatchGuard is that it provides you with a web, Windows and command line interface so you can use whatever you are comfortable with. Personally, I like the Windows software to that's what I use.

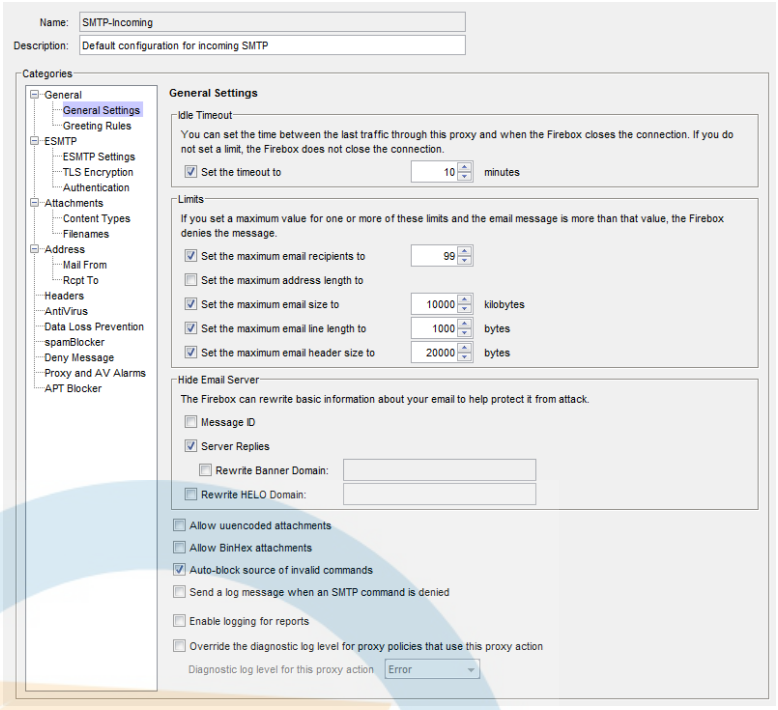

Figure 2 - WatchGuard Expanded Rule Set

WatchGuard's have a couple unique features I mentioned above that makes them stand out which are **HostWatch** and intelligent **IP Blocking**. With its tools, you can graphically see what is happening on your firewall and network quickly. They have some of the best tools hands down. There is practically no other firewall vendor that can even come close to their graphical tools. Some argue it's a gimmick but when you are being attacked, it sure beats reading through logs. I literally have found the source of an attack with their tools in 2 minutes compared to going through logs that would have taken 20 minutes to 2 hours and time is extremely valuable in an attack when your network is down. Their software is well designed, easy to use and understand. Their reporting needs some serious improvement and their subscription services are a little too expensive in my opinion. It has always bothered me how tied their devices are to needing a current subscription. You should be able to access new software releases without an active subscription. And WatchGuard doesn't make it easy to renew your subscription if you let it lapse too long.

WatchGuard's big downside is stability. I often find their VPN tunnels drop more than other firewalls and it's easier to crash a WatchGuard with an attack than others. With that said, it's also easier to stop an attack so it's a tradeoff. There is no way to block by country and some features require premium licenses (IE. IDS). Their optional web blocking service is excellent and easy to deploy. I also appreciate the fact that the reporting service run on a separate server so that reports don't overwhelm the firewall.

I cannot overstate how much I love their intelligent IP Blocking option. Yes, other firewalls do this but not the way WatchGuard does. If you configure the rules properly, you can block a hacker before he even knows what hit him. The control on the application side is crazy and if you spend the time to configure it, you can stop end users and hackers alike from even thinking about harming your network.

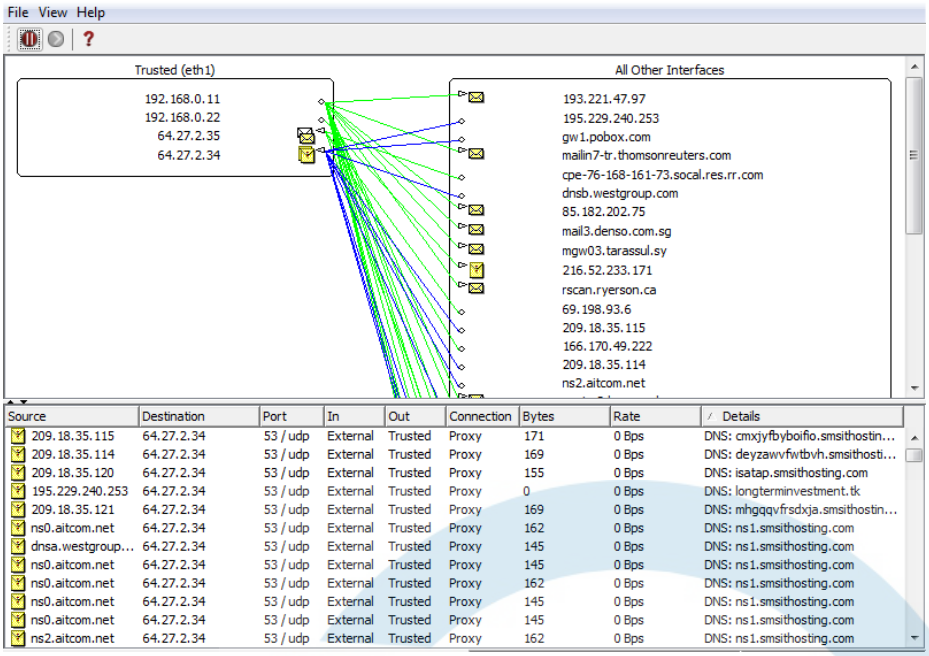

Figure 3 - WatchGuard HostWatch

Even with the downsides, WatchGuard is my 2nd favorite firewall. The features and flexibility make it a top quality firewall and give you total control of everything related to security. The support went downhill years ago when it was moved to India and has improved since being brought back to the US. Reporting still needs serious improvement and they need to stabilize the device and VPN connections.

Highlights: Excellent value for the money, includes free SSL VPN, PPTP, and IPSEC. Automatic IP Blocking and incredible monitoring tools. Outstanding management toolset, UTM, and support. Also includes application control, VOIP QOS/Shaping and traffic control. Most advanced security architecture on the market.

Downsides: Subscription required for software updates, stability issues with attacks and VPN, expensive subscription and additional features. Terrible reporting engine and bad reports out of the box.

Check Point

As mentioned above, Check Point is a solid option and has a great set of tools, features and functionality but has one of the highest price tags on the market. It beats out almost every other firewall in terms of the throughput it can handle. Its toolsets are easy to use and the GUI is nice and clean. Checkpoint has one of the best IDS modules in the industry and can handle things most others struggle with. I personally think its country blocking feature is one of the highlights of the firewall and it gives you great control over blocking countries you don't care about doing business with that present an unnecessary risk. Unfortunately, Check Point's reporting is very limited out of the box and requires third party tools to provide detailed reporting.

Checkpoint is known for excellent support and warranty services. I often compare Check Point to ASA in terms of features minus the UTM and IDS set. Both are expensive and lack a comprehensive reporting system but offer superior stability and throughput. Check Point, like Cisco, errors on the side of stability and performance over the latest bells and whistles. Check Point is a rock solid firewall and I doubt anyone is going to bring it down due to an attack without a massive amount of bandwidth thrown at it. The VPN connections are rock solid and I have never heard or seen any issues with VPN stability or connection issues.

I personally wish Check Point would be a little more price competitive and more aggressive about adding features in the base price. However, if you don't want to take any risks and want a top quality firewall, you can't go wrong with Check Point. Check Point didn't get my pick because of the high price tag and lack of some out of the box features.

Highlights: Incredibly stable, excellent company and support, market leader with great third party support, highest throughput in the industry, easy to program and use, safe choice.

Downsides: Very expensive for the features, only supports IPSEC (Lacks SSL and PPTP), and no network traffic monitor, and weak reporting system.

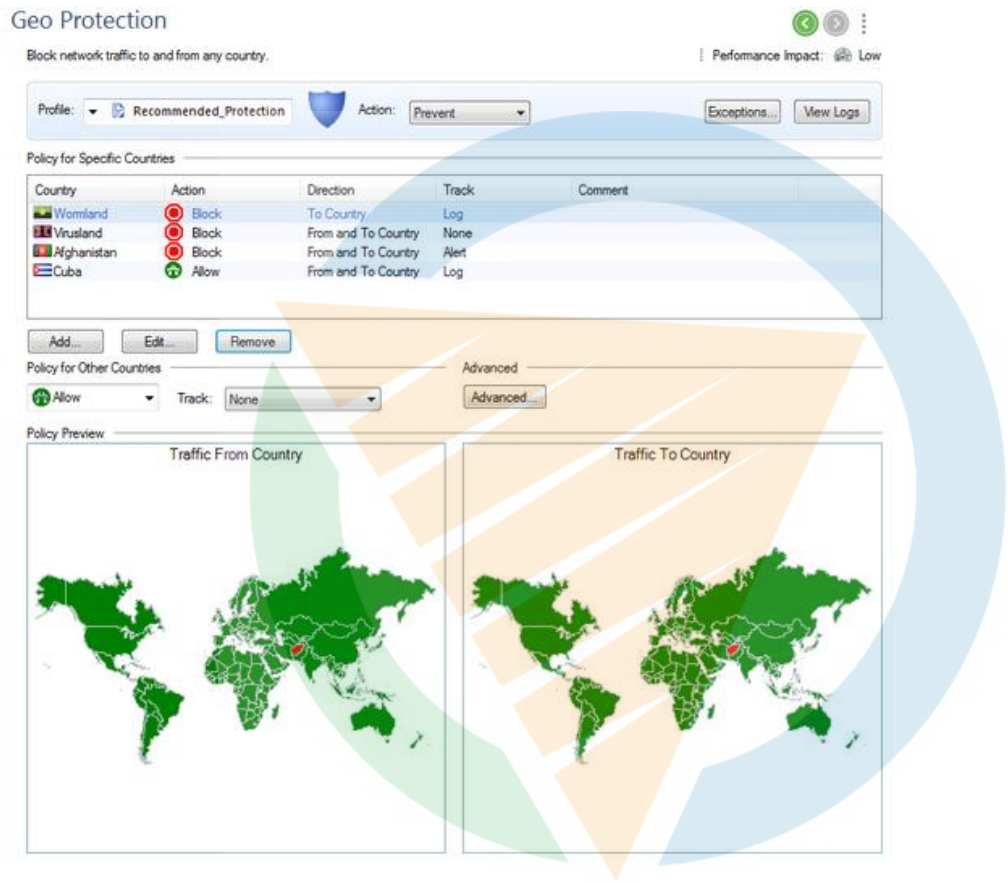

Figure 4 - Geo Protection in Check Point

Fortinet

Fortinet is one of those great products that does everything and comes with every features you can imagine and the throughput is insane! Fortinet is the only firewall that uses a different architecture than anyone else. I won't get into it because it's outside the scope of this article but its unique chip architecture gives it throughput up to 1 terabyte of bandwidth! No other vendor can even come close to this claim. The only feature not included with Fortinet is the reporting and monitoring tools called FortiAnalyzer. You probably want to include the purchase of FortiAnalyzer with the firewall because it's essential to managing it.

There are two reasons Fortinet didn't get my vote for the best firewall and the 1st is the complexity of the device. Yes, Fortinet literally does everything and has almost every feature but the interface is complex and confusing. Almost everyone that sits in front of one is completely confused by it and Fortinet will openly tell you that its support department has struggled for years to deliver good support because of the complexity of the device. I have had to call Fortinet to get advanced features working and even their support could not get them going. In one case, I had to hire a consultant to get a feature working because I couldn't figure it out and their support department couldn't either. I found a guy, by some miracle, who figured out how to get this feature working and had to hire him for a few hours to make it work. So there was essentially a consultant, support and another consultant to make a core feature work. The second reason is because of the security architecture. Fortinet has application inspection but Untangle, WatchGuard, and McAfee are the only firewalls on the market that can claim Application Proxy, EAL4+, and SSL inspection.

The major upside of the Fortinet is that fact it has an absolutely massive amount of horsepower. I seriously doubt anyone is going to max it out with bandwidth or deliver a DDOS attack to bring it down. Every time I have deployed one, I don't think I have even made the processor hit more than 5% - ever. FortiAnalyzer is a great addition for reporting and monitoring that delivers solid reports. I always feel very confident when I install a Fortinet that it will be extremely stable and secure. I just wish it had more application level control like the WatchGuard. Regardless, Fortinet is a solid choice if you want a high throughput extremely stable box and you have the patience to learn the interface.

Highlights: Unique chip architecture with highest throughput on the market, massive feature set included in the base license, IPSEC, PPTP, and SSL-VPN (web) are all included, easy upgrade path, great add on feature set, excellent optional reporting.

Downsides: One of the most complex interfaces on the market, very bad service and support, network traffic tools are optional.

SonicWALL

SonicWALL is one of the cleanest and simplest interfaces I have seen on the market. It is extremely fast and easy to learn and setup is very stable and secure. If you need a simple and straightforward firewall, SonicWALL is an excellent choice. It is a great value for the money and the service and support is not bad. The problem is that SonicWALL falls into a middle ground of being the average kid in the class. It has no real claim to fame and is pretty vanilla in terms of options and features. There is nothing wrong with it, however, compared to other options out there, there isn't much that sets it apart.

SonicWALL, like most others, can't deliver the granularity in the application security layer. It only has the ability to handle deep packet inspection with ICSA and lacks application proxies and EAL4+. This means its firewall is weaker than others and there are no proxy options to protect servers such as your email server. It comes with very good network traffic monitoring tools and has a great reporting system right out of the box. There is no doubt that the SonicWALL reporting system is one of the best on the market included with the firewall.

Overall, the SonicWALL is a good choice for anyone who doesn't need application proxies or to control application level traffic at a really deep level. For example, if you don't want to get in and change your email headers, what type of web calls hosts can make to your web server, etc., then it's a safe bet.

Personally, and this is just my opinion, I see no reason to pick the SonicWALL if I was writing the check. I would either select the Untangle, WatchGuard which is the same price or go for the Fortinet for throughput. Unfortunately the SonicWALL is just average and doesn't have any feature that will make you want to buy it over anything else on the market. Compared to Untangle, it looks pretty basic.

SonicWALL is definitely a very stable firewall but they charge extra for VPN client options other than IPSEC. To this day, I don't understand why they charge for other VPN options when their competitors don't. I only deploy SonicWALL if the client demands it.

Highlights: Great interface, excellent built in reporting, very good support and service, and good add on packages

Downsides: Lacks deep application inspection and proxies, only comes with IPSEC VPN, and lacks any stand out features.

Cisco ASA

Oh how the mighty have fallen. In the early days, the Cisco PIX used to be synonymous with firewall greatness. Unfortunately, Cisco really let their firewall offerings fall behind the market and the PIX quickly became obsolete. In an attempt to catch up, Cisco had this awful idea to combine the router and firewall into one device and thus the ASA. The problem is that the idea never took off because it was so complex to get it to work that not many people ever adopted it; and who wants their router and firewall on the same device anyway? Seriously? In fairness, Cisco has made a decent effort to push the ASA series back in the game and has worked at adding a better GUI and UTM feature set.

Unfortunately, the ASA is still the most bare bones firewall out there and comes with a very limited feature set compared to others. I am sure I am going to get hate mail for my comments on the ASA but if you are truly honest and compare the ASA to other offerings, it's pretty weak. The one thing I will give the ASA is the stability. The ASA is probably one of the most stable firewall devices on the market and probably so because it doesn't do much. The other scenario the ASA is a good fit is if you are running Cisco's proprietary routing protocols and you need the firewall to communicate with other Cisco devices. I have always recommended OSPF for routing but some people prefer Cisco's protocols.

I really can't recommend the ASA for much of anything. There are simply better choices out there with more features. If you are looking for stability, buy the Fortinet or Check Point. The ASA only offers layer 7 stateful packet inspection. The ASA has always been a mystery to me because Cisco is the networking company. You would think they would make one of the world's best firewalls.

Unless you are a diehard Cisco command line maniac, the ASA is really hard to program and the GUI isn't much better. The command line is great for very basic features such as port forwarding but I seriously doubt you are going to want to program a config file 20 pages long with application security options. If you don't believe me, open the XML file from a WatchGuard and take a look at how complex that file is. There is no way any human being is going to want to sit and write that much complex code to make firewall UTM features work.

I am not going to waste much more of your time on the ASA. When an open source firewall can do more than a commercial offering, it is just not fair to consider it in any regard.

Highlights: Stable, runs Cisco's proprietary routing protocols

Downsides: Poor feature sets, poor interface, weak security architecture, expensive support.

McAfee

I am going to review the McAfee with the disclaimer that I have used this firewall product the least. I have only programmed and used it a handful of times and I don't see it out in the market much. With that said, it is considered one of the market leaders in the enterprise market and I think it has been more coincidence than anything else as to why I haven't seen it more. I will not recommend McAfee for the small biz market but will recommend it for the medium and enterprise markets. For some reason, the McAfee doesn't come with any VPN clients or options which means you have to buy a third party client. This is crazy to me but that's how it works.

As I mentioned above, the McAfee is the only other firewall that is able to provide application proxies, EAL4+, SSL inspection and type enforcement. This makes it the only other firewall truly on the same level as the Untangle or WatchGuard in terms of application security architecture. The McAfee also comes with a great toolset and excellent support options. The company offers 4 hour replacement options and the support has been excellent the few times I tried it out.

This firewall is super easy to setup and the tool sets are top quality. This is the only firewall I have run across at the same level as the Untangle and WatchGuard. The only reason it didn't get my vote is because of the lack of VPN support and an offering for the smaller business market. The McAfee only supports IPSEC and lacks PPTP or SSL support in any form. With that said, it is probably worth a look given its strong application security layer and ease of use.

I have very limited hands on time with this firewall so I can't go into extreme detail but I will say I was very impressed with the few times I dealt with it. It is basically like a WatchGuard without many VPN options out of the box. For some reason, McAfee has not made a big marketing push for its firewalls and it's a shame because they have a great product.

Highlights: Strong application security layer (on par with WatchGuard), easy to use, great toolset, excellent support options, outstanding reporting and monitoring included

Downsides: Lack of good VPN options – both client and tunnel, no good small business offering.

ZyXEL

I didn't care for or consider ZyXEL a true firewall contender until about 1 year ago. The company has come out with some impressive appliances with software that puts them on the map. I have started to deploy the USG20W at small offices that need a lower cost option without a required subscription. ZyXEL is unique in the fact that they don't require a yearly subscription or license and provide you with all the device updates completely free of charge without a login, password or hoop to jump through. You simply login to the support page, download the firmware, and update your device.

ZyXEL is a good choice if you are on a tight budget but need quite a bit of features for the money. They are also a good choice if you refuse or cannot pay a yearly subscription fee. But as the old saying goes, you get what you pay for!

ZyXEL has some excellent features. The devices comes with a very good firewall, built in IPSec VPN, SSL VPN with a front end interface for end users, and L2TP VPN. It also has WAN load balancing built right in.

The box also gives you the ability to turn on Anomaly Profile detection to block attacks such as port scans, syn attacks, udp-land attacks, and more. Overall, the firewall and most components are pretty easy to program and the interface is clean and responsive.

You can purchase an optional license to use the content filter from either Commtouch or Bluecoat and report on user activity based on your custom settings. ZyXEL also offers an anti-spam feature that can be fully licensed to protect your email servers. Although it does offer reporting, the options are generally very basic and it does offer the option to send logs to a separate syslog server.

Now the negative. When you compare a ZyXEL to the other firewalls in this review, it is very feature poor in general. The firewall offers basic packet filtering rules and does not allow any type of proxy rules. Because the firewall operates at the packet filter level, there is no way to customize rules at the application layer. For example, you can't go into your SMTP rule and tell it filter out .EXE files over 5 megs. You can add schedules to firewall rules but not much else.

The device provides a good deal of VPN options out of the box but they are extremely difficult to program. Programming the IPSEC VPN was probably the most difficult VPN interface I have ever dealt with. The SSL isn't bad but everything else is cryptic and difficult. The real time session and log tools are pretty good but not wonderful. The biggest problem I encountered with the ZyXEL is stability. The 1st firewall I deployed would lock up out of nowhere and become nonresponsive to user browsing and sessions. One minute later it would start working again. I thought I had a bad box and a couple weeks later I setup another one and saw the same thing happen. The firmware was on the latest version and I still continue to see weird blips where the box just stops handling requests. It's very strange.

The bottom line is that the ZyXEL is more of a traditional firewall than a UTM device. Where it fits in is someone who is extremely budget conscious and needs an enterprise level firewall instead of a home router. In fairness, the company does seem committed to adding features quickly and I have seen many improvements in the last two firmware releases. How far they can actually go is yet to be seen.

I would only consider the ZyXEL in a situation in which the client needs something cheap but good and doesn't want to pay a yearly license. The business doesn't need any UTM features but needs good VPN options with the exception of basic web filtering, anti-spam and basic IDS. Also keep in mind when I wrote this article that I was still seeing some instability in the firmware.

Highlights: Great value for the money, no yearly license fees, excellent VPN options with SSL, easy to use and understand interface (minus VPN setup), aggressive firmware and feature updates

Downsides: Acts more like a traditional firewall than UTM device, extremely difficult VPN configuration, very limited content filtering and anti-spam, very basic IDS

Untangle (Open Source w/Premium Options) – WINNER!

I cannot believe I am selecting a semi-open source firewall as this year's winner. Untangle is the most impressive and flexible firewall offering I have ever used. The company offers either an ISO download or security appliance. You can download the firewall software for free and load it on any box that supports Debian Linux. I have one running on some clone hardware with an AMD six core processor and it is extremely stable and impressive. The upside to Untangle is you can throw a ton of hardware at it if you

need to process a lot of bandwidth. The limitation is the hardware you install it on. It's only limited by your hardware.

Untangle is more of a UTM device than a traditional firewall and it works by loading and configuring modules. For example, you can load and configure an anti-spam module that will filter through all your email. There is also a reporting module that allows you to configure and email out scheduled reports. The firewall is 1st configured through simple port forwarding and then you can go into the firewall module and further specify rule actions. Additional protection and features is handled through the modules.

I really like the approach Untangle takes because it lets the firewall handle the basic handoffs and then the modules come in and do the heavy lifting. The IDS module has over 2,500 signatures and is included free. You get a fully functional firewall and IDS right out of the box at no charge. They even include a free virus scanner integrated in to scan all incoming and outgoing traffic. Even further, you can turn on a phishing blocker to ensure no one emails your users with phishing requests or enable the ad blocker and filter out any web-based advertisements!

Figure 5 - Untangle Interface

What is even more impressive is they offer a WAN balancer, WAN failover, Active Directory connector, HTTPS inspector, bandwidth control, and high level web filter. If that wasn't enough, the out of the box reporting is amazing! The interface is one of the cleanest and most intuitive interfaces I have ever used and you can learn it in minutes. There is a real-time session viewer and a real-time host viewer. Untangle has something that is close to the WatchGuard IP Blocker called the penalty box that can isolate and block hosts which is very useful. You can even custom brand the firewall interface with your company's logo and require users sign a consent form before being able to access the Internet.

Even if you purchase all the premium modules, the entire subscription only costs $500 a year which is a deal for all the value you get in return. I have personally replaced several firewall installations with Untangle and have seen a good amount of WatchGuard users and others using the free firewall to

replace their own devices. See the conversation at http://forums.untangle.com/off-topic/32664-my-watchguard-experiment.html.

If you need to control the application security layer, you just install the application control module and customize what you want to block or unblock. The software comes with hundreds of pre-set application definitions such as DHCP, Citrix ICA, and Bit torrent application definitions. The application security layer customization is mind blowing! I literally cannot find one thing about this device I don't like. There is a module for everything and I sure there will be dozens more soon enough. The interface blows away all the pure commercial firewalls including the WatchGuard and is so easy to use it's ridiculous.

If you do a search for Untangle vs. your favorite firewall you will find an endless amount of posts from people replacing their commercial firewall with Untangle. The company offers different levels of support depending on what you need and the support is excellent. Untangle is now my go to firewall because it does everything I need in 99% of the situations and is free in some cases and a great value in others depending on whether I need the premium modules.

The best part is that it can even be virtualized and have put it in XenServer and VMWare deployments without the need for additional hardware.

Highlights: Complete application security layer control, modular control, endless options, more features than most other firewalls, easy to use and configure everything, stable, and powerful. Has almost every feature other firewalls offer and fits the bill in almost every situation. Can virtualize without additional hardware.

Downsides: Doesn't have geo protection like Check Point, Reporting can bog it down on the same box (Make sure you have enough horsepower)

Summary

Overall, Untangle is my recommendation in terms of firewalls. It has a ridiculous amount of features and the application security level control is better than anything out there. It has more features available than any other firewall I have used and the GUI is well laid out and easy to use. You can run it on either a dedicated PC, server, virtual session or purchase one of their appliances. The modular approach they take allows the company or third parties to quickly write additional modules to add on if additional functionality is needed.

My second choice is WatchGuard due to the feature set, price and GUI. WatchGuard comes in a close second but the VPN and device stability issues I have experienced put it behind Untangle. Furthermore, Untangle just offers more features and options for a lower price point. Untangle also has many features other firewalls simply don't offer such as an ad blocker, custom branding engine and user sign up portal.

If Untangle or WatchGuard doesn't fit the bill for you, look at the other vendors based on the strong points I highlighted in the reviews. There is absolutely nothing wrong with any of the other firewalls mentioned in this review as I have used every one of them in real world deployments and they all work great. Just focus on the strong points vs. the negatives in making you decision. You are welcome to contact me with any questions or comments at sgm@smsitgroup.com. Thank you for taking the time to read this comprehensive guide.