Understanding Security Appliances

Author: Felicia King

What is a security appliance

A security appliance is a device that protects the perimeter and the inside of your network. The perimeter is secured because the security appliance is between the internet connection and your devices. The inside of the network is secured to the extent that you make use of proper network design, and allow the device to secure the traffic between the networks. The security appliance, when properly programmed, will also isolate guest from trusted traffic allowing for secure functionality for both types of clients. The best security appliances are able to extend UTM (unified threat management) security out to wireless access points and connected devices.

Security appliances are direct replacements for standard firewalls and routers. If you are using a firewall or router that does not have unified threat management capabilities as your perimeter device, then you are not providing adequate protections to LAN devices.

“I don’t need that much security”

People tell me that they do not have anything that is that important that they need to protect. Or they tell me that they think that they aren’t a target since they aren’t a bank or a big business. Both of these statements indicate incorrect thinking about the situation.

If you think you do not need the security protections afforded by a security appliance, I would ask you to answer one question. Do you want your computer systems to keep working? Invariably the answer is yes. Realize that a compromised computer is no longer doing its job for you. It is under the control of the hacker. Consider the following facts.

Soft and easy targets

Home and small business users are considered soft and easy targets by hackers because they are easier to penetrate. Therefore, they are attractive targets. Brian Krebs has an excellent article on the value of a hacked PC.
http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

In a recent article about the Yahoo breach, I described how the malware turned the hacked PCs into Bitcoin miners that made money for the hackers.

Beyond the concept of your computer being used for things you did not authorize, you should also realize that your compromised computer can be used to destroy your reputation. Your license keys can be stolen and then sold on the black market. Your social media and banking credentials can be stolen and used for nefarious deeds. Really the sort of nefarious things a hacked PC can be used for is limited only by two things.

- The creativity of the hacker
- The hardware-level network controls that exist to stop egress traffic

This is because once a PC is hacked, the security software (if it is installed), may not be able to remove the malware effectively. Think of the Cryptolocker malware. It encrypted the entire hard drive of the computer and held it for ransom. You should also realize that most malware now installs and then randomizes itself making it nearly impossible for host-based security software to clean it once it has gotten onto the computer. At that point, you are totally reliant upon the skills of a support tech to help you get the malware off the computer, if that's even possible. Some malware infects the hardware layer like the firmware of hard drives.

It is guaranteed that a single visit to your computer from a support tech will cost more than if you had just bought a license of a proper host-based security product and used a real security appliance as the core of your network.

In my article on why detection is doomed, I explain how it is too late once the malware gets onto your system. The name of the game now is prevention. Technically, the most cost-effective solution has always been prevention.

Cleaning is more expensive than prevention

The question here is about the controllable and predictable cost of prevention versus the uncontrollable and unpredictable cost of a compromise. Target recently spent $130 million to deal with the breach of their point-of-sale systems.

When a breach occurs or malware infects a system, you do not get to control that malware or the actions of the hackers. Therefore, you have no control over the scope of the damage. I'll give you an example.

Let's say Sally is a teacher and she has access to the student folders for all high school students because she is a high school teacher. And Sally also has access to the teacher shared files, her own home folder on the server, and likely other resources. If Sally's computer gets malware on it, then that malware executes on the network with her credentials. The damage that is done is limited only by the security restrictions that were put in place by the systems engineers who designed the network and server system. By the way, this is a real example I have seen (name changed of course).

In this circumstance, 17 gigabytes of data was corrupted because of the malware. Yes, that is 17 gigabytes of data that Sally's account necessarily had access to in order to do her job. In this case, the server security product deleted the malware, but it could not stop the malware on the unprotected PC from using Sally's credentials to corrupt files. The server security software stopped the malware from propagating.

In order to repair the problem, the infected PC had to be cleaned, proper host-based security software installed, and all of the corrupted data had to be restored from a backup. In this case, the situation was TOTALLY preventable because the PC had McAfee Enterprise installed. The school was making the transition to Trend Worry-Free Business Security. Suffice to say, McAfee missed the malware, but Trend stopped it from propagating at the server.

Ultimately, the cost of the troubleshooting, cleaning, outage, repair, restore, etc. was in excess of $2000 at least. It caused problems with teachers and students not being able to access their files for a period of time. Fortunately, none of the more secure school data was affected because teacher accounts have no access to that data.

What was the cost of prevention? $40 for the Trend WFBiz software and someone's time to install it.

An additional thing to consider is the fact that the malware may not be cleanable. Over six years ago, I saw malware that infected the firmware of hard drives, meaning that it wasn't cleanable. You had to know that was the problem and rip out the infected hard drive. So even if you think you have cleaned the systems, aren't they always suspect once they have been compromised? If you want to understand this better, take a look at the example of BadBios.

Configuration matters

Configuring security appliances and correctly designing networks is not easy, and the vast majority of IT people do not have adequate skill in this area.

The effectiveness of your security appliance is based upon the following factors.

- The capabilities of the security appliance as designed by the hardware vendor
- The enabling of unified threat management or extensible threat management security subscriptions on the device that enable these necessary features
- The quality and frequency of issuance of security firmware updates supplied by the hardware vendor
- The level of maintenance and monitoring applied by the network security engineer who manages the device and applies firmware updates
- And most importantly, the skill of the network security engineer who programmed the device and designed the network

These factors are more fully explored in the following sections.

Security appliance capabilities

A device really cannot be considered a security appliance unless it is capable, via hardware vendor design, of having these features.

- PAT (port address translation)
- NAT (network address translation)
- port-forwarding lockdown based upon ingress IP or authentication group
- Dynamic WAN IP hostname update
- DDoS (distributed denial of service detection and protection)
- IPS (intrusion prevention)
- IDS (intrusion detection)
- web content filtering
- application control
- remote access two-factor authentication
- integrated authentication methods (example: LDAP)

- DLP (data loss protection)
- automatic attack blocking based upon configured thresholds
- IPSec VPN for remote access
- BOVPN (branch office VPN, for site-to-site connectivity)
- RADIUS or certificate-integrated wireless
- embedded wireless gateway controller
- compatible with centralized logging
- logging able to be fully customized
- sophisticated diagnostics built into the appliance management tools
- granular egress filtering capabilities
- SMTP, DNS, FTP, HTTP, HTTPS proxies
- cookie and header stripping from HTTP traffic
- ability to apply policies by IP, network, or user
- Ability to function as the network backbone defining networks, broadcast domains, VLANs and everything else that a standard router can do

Without these capabilities and UTM/XTM (extensible threat management) as well as detailed logging, you cannot really call the device a security appliance.

Here is a link to WatchGuard's explanation of UTM security subscriptions.

https://www.watchguard.com/products/xtm-software/overview.asp

Realize that these UTM subscriptions are only a portion of the feature set of a true security appliance. It is worthwhile reiterating that none of these features are enabled out of the box on any security appliance for very good reason. Therefore, a network security engineer is required to program the device to meet the needs of the organization or family the device is intended to protect.

UTM/XTM subscriptions

Security appliances must have active security subscriptions enabled on the device in order for it to be able to have access to security information to deal with today’s dynamic threat landscape. At a base level, a security appliance is one amazing firewall and router. But without the UTM subscription, it doesn’t have access to the dynamic content it needs in order to truly inspect and process today’s network traffic.

One example is web content filtering. The security engineer configures categories to allow and block. Those categories are maintained by a company through a subscription model. As the security appliance needs to process traffic, it queries the content category of the URLs being presented to it. In a simple example of this, you can block advertisements. This means that advertisement content will be blocked regardless of whether or not it is embedded in websites. This strategy protects you from malware delivered through advertisements like in the Yahoo breach.

Another example of dynamic content is the antivirus subscription. This is a signature list of viruses that network traffic is scanned against. If a virus is found, an action is taken. Typically the virus would be blocked, but the security engineer could use quarantine and other options.

Vendor-supplied firmware updates

WatchGuard is a security appliance vendor. They release six firmware updates per year, sometimes more if needed. These firmware updates are available for install on any WatchGuard security appliance that is covered by a Live Security subscription. Firmware updates are quite easy to do, but it is prudent to make backups of the configuration before and after firmware update installation.

In contrast, Cisco releases about two firmware updates per year which means that a greater period of time transpires before a fix for a bug or issue is able to be applied to the device. Cisco also makes it very difficult for average IT managers to get their hands on the firmware updates and install them. The ramification of this is that the firmware updates are not installed, so unpatched security vulnerabilities remain an outstanding problem.

Cisco also does not have a good mechanism to communicate to IT managers when firmware updates for Cisco devices are available to download and install. In contrast, WatchGuard emails every email address associated with a Live Security subscription when new firmware updates are available.

Maintenance and monitoring applied

Good security appliances are easy to monitor because they have real-time monitoring capabilities. For example, WatchGuard offers WatchGuard System Manager (WSM), which is a GUI (graphical user interface) tool, as a free download with any Live Security subscription. This means that by simply buying the security appliance and maintaining a valid subscription on the device, you have access to an incredibly powerful monitoring tool.

Whenever I walk into a Cisco network, I ask the IT manager or the network engineer what is happening on their network. The answer I always get is that they do not know. They do not have a tool that shows them what is going on in real-time on the network. Their Cisco equipment does not afford them the opportunity to centrally monitor network traffic natively.

It is possible to buy an extremely expensive third party application to do this, but I have yet to see any company do that except those that have eight full-time network engineers in their employ.

It is obvious that if you are not monitoring what is happening on the network, then you do not know what is going on. This also applies to what is happening to the perimeter. Who is trying to hack you and in what ways? What traffic is being stopped and what is coming in? Is all the LAN-to-LAN traffic legitimate?

WatchGuard devices even have an embedded web server that enables you to view traffic and all kinds of fun things without having the WSM tool. As of the 11.8 fireware version, FireWatch is now included in the embedded web interface of the appliance. No Cisco appliance can claim that capability.

FireWatch is a real-time, interactive report toolt hat groups, aggregates, and filters statistics about the traffic through your XTM device in an easy-to-understand form.

http://www3.watchguard.com/help/docs/dimension/v1/en-US/index.html#cshid=en-US/system_status/firewatch_web.html

The best security appliances have capabilities for advanced logging. WatchGuard devices have the ability to send log data in real time to WSM and a logging server. The latest logging server is called Dimension which is a really advanced logging and reporting server. This is another goodie you get with a valid subscription to Live Security. If you have a distributed network, you can even host your Dimension server in Amazon Web Services and send the log data from as many fireboxes as you want to your Dimension server in the cloud.

Ultimately, a good security appliance makes monitoring and maintenance easy to do so that a good security engineer can do their job effectively and quickly.

Skill of the programmer

One of my signature sayings is, "Your security is only as good as the skill of the person who programmed it." Given the fact that 97% of breaches are due to misconfiguration, the skill of the person who programs your equipment is very important.

It is true that the right appliance is necessary, and it needs to have a valid security subscription. But those two items by themselves will not get you very far without the skills of an experienced security engineer working to protect your interests.

A good security engineer will implement a configuration that maximizes your security while customizing allowances for the things you need to get access to.

How are they different from firewalls and routers?

Security appliances can do everything that a firewall and router can do, and then a bunch more. The section on security appliance capabilities shows this list of features in depth.

Standard firewalls are also routers that can do NAT and stateful packet inspection. They can do basic port-forwarding, but there are typically limitations on the ability to protect the incoming (ingress) traffic.

A standard firewall also has interface limitations. For example, Linksys, Netgear, and Cisco routers have a limited set of firewall capabilities including having a single interface for LAN traffic. Even if you look at Cisco’s business class line of smaller routers, they only have a single LAN interface. Cisco expects you to use expensive Cisco switches and use those to create VLAN definitions and segment traffic that way. That is because Cisco devices are not security appliances. They are really routers.

In all circumstances where I have seen a business-class Cisco router installed, I have seen misconfiguration problems. This is because the configuration of Cisco routers is extremely time-consuming and convoluted to sort through. A single configuration could be comprised of 20 pages of config that is very difficult to interpret. This is in stark contrast to a WatchGuard security appliance where all of the security policies are available for viewing on a single screen. It is easy to audit the configuration of a WatchGuard appliance, thereby knowing that there are not security misconfigurations that will lead to breaches.

A common misconfiguration problem I see is that the Cisco routers were being used as perimeter defense, but never had the firewall feature enabled. Clearly, this speaks to the incompetence of the person who configured the device.

Pricing and support model

The typical security appliance is designed to last 3 years. After that, you should keep your old unit as a spare and get a new unit. If you buy a compatible model, your security engineer can likely transfer the configuration file with minor changes rather than having to do a full configuration from scratch.

The big reason to buy a new unit is because hardware gets old and tired and the new hardware will have more horsepower. It is quite typical for more RAM and processor to be added to new units compared to older units. Given the need to have horsepower to deal with the dynamic threat landscape, you need that additional horsepower.

WatchGuard's security subscription suite includes a subscription for the UTM components https://www.watchguard.com/products/xtm-software/overview.asp as well as next business day hardware warranty. You also get limited support.

When I say limited support, there is a limit to how many support cases you can open with WatchGuard per year. The reason for this is obvious. There is a limit to the fee you paid for your subscription, so there has to be a limit to the support requests.

Security appliances are not designed to be managed by end users. They are designed to be managed by network security engineers. This means you should plan that your primary support is a WatchGuard partner company like QPC, and then the support tickets with WatchGuard would only be used for things that need to be escalated to WatchGuard.

There are two general ways to buy security appliances. You can buy them with a one-year of security subscription, or a three-year security subscription. You get a slight discount for purchasing all three years up front, but the acquisition cost is higher then.

Failure of common setups

Using a default or predictable IP scheme

I am always amused when I see some person who claimed to be an IT professional using a 192.168.0.1/24 IP scheme. Default IP schemes should never be used because they are predictable and make it easier for hackers to guess the network layout topology.

Switch-based VLANs do not extend security to subnets

In order to understand this, I'm going to use two examples: the Cisco example, and the WatchGuard example.

In the Cisco scenario, let's say you have an ASA device as your perimeter device and Cisco switches in your network plus a couple gateway wireless controllers. The VLANs are configured in the switches, therefore the switches determine the network configuration, not the ASA. The switches play a leading role, not a supporting role. This means that in order for you to audit your network configuration, you have to scrape through the 20 pages of ASA config and the configuration of every single switch you have. You also have to scrape through the config of the gateway wireless controller. Suffice to say that this is one hugely time-consuming difficult task that is prone to human error. Because of the sheer effort required, this type of an audit is rarely done, and misconfigurations are pretty well sure to exist.

In the WatchGuard scenario, let's say you have a Firebox as your perimeter device and HP 1910 series switches. The Firebox IS the gateway wireless controller. The Firebox defines the network and is the core router. It defines the VLAN configuration. The HP switches play a supporting role. In this scenario, nearly all of your network configuration is all in one device making it easy to troubleshoot, easy to monitor, and easy to audit. Even the wireless configuration can be audited from by accessing the Firebox. The only thing the HP switches are doing is handling layer 3 packet routing and tagging.

Because the Firebox defines the VLANs, defines the network, and IS the gateway wireless controller, then UTM security can be extended to all of the subnets. Remember that a security appliance can only apply security to network traffic it can see.

Now you may be wondering if you will experience a slow network because the Firebox is involved in so much of the traffic management functions. The answer is no if the Firebox was sized properly. I'll give you a real world example to elaborate on this concept.

How not to design a network

I did a project with an organization that had a Cisco ASA, a Microsoft ISA server (proxy), a WebSense server (web content filtering), a DMZ, an outsourced cloud-based SPAM filtering solution, and a bunch of VLANs configured in a stack of Cisco switches. Sounds confusing right? That would be an understatement. Imagine that you needed to figure out why packets weren't getting from point A to point F. What diagnostics do you have? What visibility into the network traffic do you have? None is the answer.

I looked at the mess and replaced the whole pile of confusing jumble with a single XTM 520 Firebox. The Firebox can do spam filtering, VLAN definitions, web content filtering, and proxy traffic.

It took us about 1 hour to swap the network cables around during the cutover to eliminate the ASA, ISA, and WebSense servers. We changed the DNS MX record to eliminate the cloud-based SPAM filtering solution. And we removed all the unnecessary VLAN config from the switches. We went from 12 VLANs to 3.

What was an absolute hoot about the project is that we immediately started receiving phone calls from the users who were flipped out about how fast everything was. That's a pretty big deal given than the users virtually never call to tell you when things are working well. They only call when things are broken.

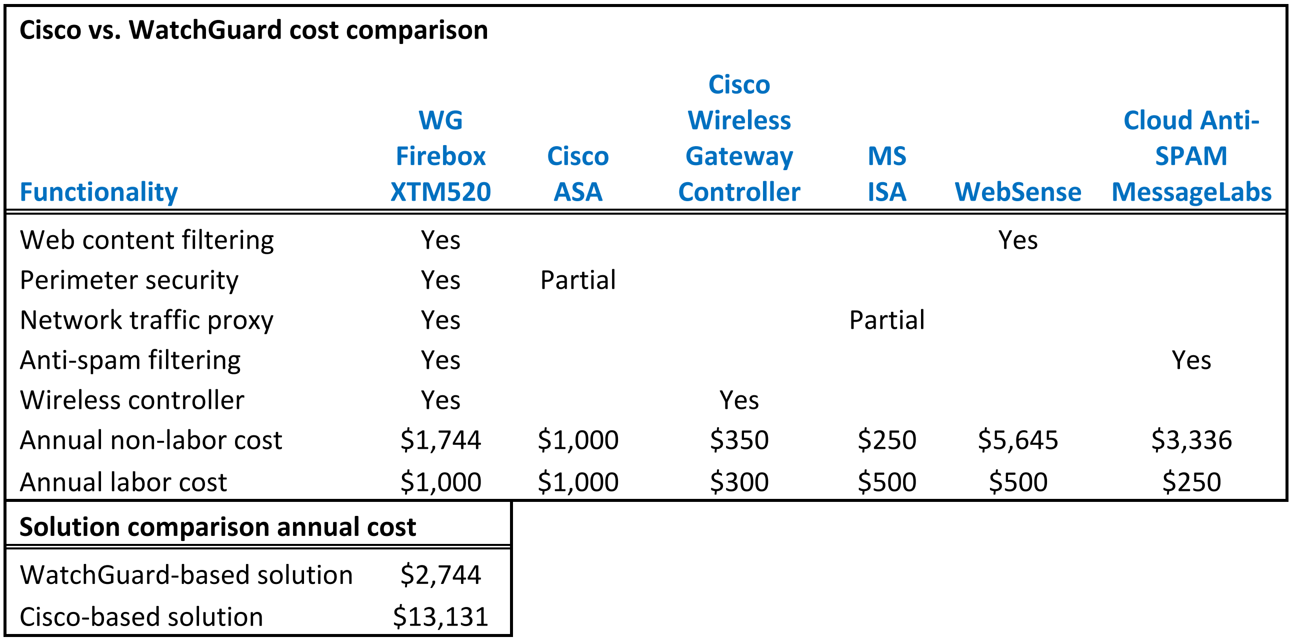
And I didn't even tell you about the cost comparison for this scenario yet. The cost for the WatchGuard firebox was $5233 with three years of warranty, support, and security suite subscription.

An annual WebSense subscription by itself was a cost of $5645!!!

The hardware warranty for the Cisco ASA and gateway wireless controller was quoted in excess of $1000 annually, and remember that the ASA isn't even a security appliance. It has no security subscription component.

There was an enormous difference in terms of support costs also. Instead of having to manage two servers, VLAN configs in switches, an ASA, and an external hosting service, only one WatchGuard device needed to be managed.

The table below shows the cost of the WatchGuard-based solution versus the Cisco-based solution. Clearly the figures speak for themselves.



Cisco vs. WatchGuard cost comparison

Functionality	WG Firebox XTM520	Cisco ASA	Cisco Wireless Gateway Controller	MS ISA	WebSense	Cloud Anti-SPAM MessageLabs
Web content filtering	Yes				Yes	
Perimeter security	Yes	Partial				
Network traffic proxy	Yes			Partial		
Anti-spam filtering	Yes					Yes
Wireless controller	Yes		Yes			
Annual non-labor cost	$1,744	$1,000	$350	$250	$5,645	$3,336
Annual labor cost	$1,000	$1,000	$300	$500	$500	$250

Solution comparison annual cost	
WatchGuard-based solution	$2,744
Cisco-based solution	$13,131

Trusted network isolation lacking

A rule of thumb to follow is that if the router component of the security appliance cannot see the traffic, then it has no ability to monitor, shape, deny, or otherwise provide its security functionality to that traffic. Therefore, it is best practice to isolate servers from less secure devices such as workstations. This isolation can be provided by VLANs as long as there are security traffic rules applied between VLANs. Too often I see Cisco-based VLAN network design doing ONLY broadcast domain traffic management. What has that done for security? Not much.

A better approach is to use a security appliance that can extend network security policy, traffic management, and traffic shaping rules out to each subnet whether they are physically separated or are VLANs. In this way, you can write policies that restrict the traffic between trusted subnets to a defined list of ports and protocols that you approve of. Think of this as a form of whitelisting. You define what are the approved types of traffic and everything else is just denied. This is a much better approach to trusted network design and more people should employ this tactic.

Another ramification of this tactic is that you can specify which networks certain types of traffic is allowed to come from. For example, do you think it's prudent to allow FTP traffic to egress from your point-of-sale network. Probably not, unless your egress policy specifically restricts egress traffic to a list of approved IP addresses. Given the Target breach, I wonder if this type of a network restriction would have prevented the POS card data from being FTP'd to the hacker's server.

I like to restrict egress FTP to a single subnet where the IT people can do their work while preventing unauthorized FTP of a company's intellectual property. And of course, you should always AV scan your FTP traffic on the fly. A WatchGuard firebox with the security suite and proper configuration can AV scan all FTP traffic.

Lack of guest and trusted isolation

Something that bugs me quite a bit is when I hear about people just willy-nilly giving out their wireless network information to their friends, neighbors, etc. You need to realize that wireless networks that rely upon PSK (pre-shared key) can be compromised by an asterisk revealer application. Don't you think the hackers load that onto your computer and look for that stuff? Of course they do. But, don't put it past the teenager friends of your kids to do that either.

So let's say the friends of your kid come over, and your kid gives them the SSID and passphrase for the wireless network. Oh, and you do not have a guest network. So the kids and their insecure computers (Kids don’t care about security. They care about FUN!) are now on the same wireless network where you do your online banking. Regardless of whether or not these kids themselves are capable of launching hacks, their computers are more than likely breached. The computers that I see which are owned and operated by the 20 and under crowd are almost always infected with something.

So not only do you need to be concerned about the malware on these computers you just allowed on your network, but you also need to be concerned about the fact that your pre-shared key is in their computer. I have seen social networking sites where the SSIDs and PSK are posted and shared among kids in a community. So if your kid's friend has the PSK, so might the entire neighborhood and anyone within driving distance of your house.

Obviously, a much better approach is to have a guest network. Keep those unknown, unsecured, untrusted devices off of your trusted network. Only allow trusted devices on your trusted network and use MAC access control or DHCP whitelisting to further enforce it.

By the way, this also helps with compatibility issues to have a guest network. I like to put tablets and smartphones on the guest network where security access restrictions can be less. If you were really pressed to maintain backwards compatibility with a device that couldn't handle WPA2, then you could set the guest network to WPA and put that device on it. All the while, your trusted network is still using WPA2 (better wireless security).

Misconfiguration, logging, and design issues

Typically each year a study is done by a large research company like Gartner or InfoTech and the findings regarding the causes of security breaches is nearly always the same at a high level. Their findings could be characterized as 97% of all breaches occur due to misconfigurations. This is absolutely true.

It is incredibly important that you understand that the vendor design of the security appliance you select dictates its capability. For instance, you are not going to be able to see all of the network policies in one easy-to-read screen if you decide to buy Cisco equipment. There is no management GUI for that configuration provided for free with the appliance. So if you are trying to avoid misconfigurations, then you need to select an appliance that is designed to be easy to maintain, and has powerful logging and troubleshooting capabilities.

What is meant by misconfiguration?

Misconfiguration is anything that should have been configured differently according to IT security standards and best practices. A good example is a perimeter-use Cisco SOHO router with the firewall engine turned off. Gee, that's a pretty big misconfiguration, yet I've seen it several times.

Misconfiguration could also mean setting up a port-forwarding policy and not setting it up in the most restrictive method that still allowed the business function to work. That is what you would call IT laziness in action. The least rights and highest restriction method should always be employed, and a configuration should only be opened up where necessary.

Misconfiguration could also mean using weak passwords, which unfortunately is also a side-effect of IT laziness.

What role does the design of the network equipment play with regard to misconfiguration?

In order to know what is happening on the network, you must have the ability to see the traffic. This means logging. And meaningful logging is log data that is sent to a logging server and retained for a period of time allowing for analysis and reporting. Devices that do not support this functionality, or configurations that have not been set up this way are an indication of misconfiguration.

If you, the owner of the network equipment, decline the service agreement from your provider that includes logging and monitoring, realize that you may be contributing to your own misconfiguration. If you have your own IT staff, then you should have your own logging server setup, and your staff should be trained on how to work with the log data.

Refer to the section on Failure of common setups for more examples of the role of network design in misconfiguration.

SOHO devices

Lastly, SOHO routers are not security appliances. Please see my article on SOHO routers for more detail on why they are not acceptable in today's landscape of dynamic threats.

Dynamic threat landscape

One of the first things I do with an IT manager that I'm newly working with is to help them to see and interpret the traffic occurring inside their network, the traffic leaving (egress), and the traffic coming in or attempting to (ingress). A person really gets an appreciation for security appliances as soon as they get to see the real-time logging data.

A quick story

Several years ago I was working with a new client to take out their Cisco SOHO router that didn't have the firewall feature turned on, and put in a WatchGuard firebox as the center of the network and perimeter device. As soon as I started looking at the logs, I found that one of the accounting PCs was constantly leaking data to Czechoslovakia. I quickly asked the IT manager if they did business with anyone in CZ, and the answer was no. So I wrote a quick policy in the Firebox that stopped all egress traffic from that PC. We then went to investigate.

After getting rid of the useless AVG software on the computer, and installing Trend Worry-Free Business Security, Trend found 26 viruses on scan and removed them.

So one wonders how much of the company's accounting records had leaked to CZ. It is a prime example of how not knowing what is happening on the network can be disastrous. It is also an example of what happens when you use inadequate host-based security software.

New attacks with each published vulnerability

Now you may be thinking, "well then why don't they just stop publishing them?" Published by who is something you need to consider. The black market is laden with hack and crack toolsets that are available for purchase on an annual subscription model. Some hackers maintain these toolkits, and others use them. Sometimes a vulnerability is known on the black market first, then the software vendors have to scramble to issue a patch. Sometimes a whitehat tells the software vendor about the vulnerability, then the software vendor releases a patch.

As an example, as soon as it was published that there was a viable backdoor in massive numbers of SOHO routers on port 33434, I started seeing attacks all over on this port. I've been recently seeing attacks on port 808, but I'm not sure what that's associated with yet.

In terms of zero day vulnerabilities, these are often exploited by hackers before software vendors release a patch. So the question is what mechanism do you have in place to mitigate those risks? If you are employing a strategy of proxying web traffic and using the full inspection capabilities of a security subscription-based security appliance, then it is likely that there will be a dynamic protection available to you in the mean time.

Realize that the keepers of the security subscription content can quickly update their stuff to extend the protection to their subscribers. This can be deployed in a matter of hours compared with days, weeks, or months that it can take to release a tested software patch.

Ultimately, we live in a dynamic threat landscape, so if your security solution doesn't use dynamic update protection methodologies, then you are lacking protection against these attacks.

Annual cost for a reasonable security setup is about $738 per year for a residential scenario. The question you have to ask yourself is what is the cost of an outage, potential banking or identity theft, potential data breach, or potential busted computers in comparison to a controlled annual cost. Obviously, it is up to you. My intent in writing this article was to educate you as always.