

Re: HIPAA and firewalls

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-05/0713.html>

From: Jeff Liebermann (jeffl_at_comix.santa-cruz.ca.us)

Date: 05/10/04

Date: Sun, 09 May 2004 19:45:49 -0700

On 9 May 2004 17:47:13 -0700, ebct@yahoo.com (Irwin) wrote:

*>Hello all. I was trying to connect a few radiology offices in a HIPAA
>compliant manner using VPN. We were considering hardware firewalls
>from Watchguard, Netgear, SonicWall, just read something about
>NetScreen, don't know anything yet about HP.*

I'll assume that you want to terminated the VPN with a VPN router and not a server. It would be nice to know the number of machines at each end of the VPN as many vendor license their routers based upon the number of "users".

*>The offices are connected
>using 768k upload DSL, which I presume is the bottleneck.*

Yep. The slowest speed at BOTH ends of the link is the limiting factor. For a while, the local DSL was 1500/128 kbits/sec. Two of these DSL lines resulted in performance identical to 128/128 ISDN lines. Recently, this has been increased to 1500/256 kbits/sec. Where did you find an xxxx/768 kbits/sec line? ADSL or SDSL?

*> I have read
>previous posts on older equipment, but haven't seen anything
>discussing 2004 equipment. I wondered what you all thought out there?*

Buying the latest greatest often enlists you in the vendors beta test and debugging program. Are you sure you want the latest greatest?

*>1. Which products would be the most cost-effective, given all the
>different plans and service and upgrade stuff?*

Service plans and upgrades imply that you're buying into some kind of service contract. This is the way Watchguard and Sonicwall operate. They license by the number of users, which can be increased from the base 10 user system to whatever your budget can afford. You need to purchase an annual contract to obtain updates and support. While this may have been a proper way to fund development in the past, methinks this is a bad and expensive method of purchasing a router. You need

an "appliance", not a relationship.

*>2. Why do the little boxes cost so darn much? They cost way more than
>the computers you are trying to protect. I guess the data is
>invaluable, but still...*

Trivia: If you find the data sheet online, and it takes more than a dozen clicks to find the price, they're not interested in selling you a product. They're selling a relationship or re-selling the relationship through an authorized dealer.

There's no reason for such VPN routers to be expensive. The need to fund development and for the vendor to pay license fees to technology owners, was the prime culprit in the past. There's nothing magic about IPSec VPN's that justify the current level of pricing other than users continue to pay high prices for user count based licenses.

There are several VPN routers that do not count users and are quite economical. Details to follow.

*>3. What do you experts think about those arrangements where you buy
>hours of telephone tech support to walk you through an install
>yourself? Much cheaper than an on-site install. Is the end result as
>reasonable? Or at least satisfactory?*

If the router requires a tech support walk through on installation, then the manual is badly written (Sonicwall), the web based configuration is overly obfuscated (Watchguard), or the router is infested with features of dubious value (Cisco). I've purchased support services from Sonicwall, Watchguard, and a Cisco reseller in the past. Only the Cisco reseller was worth the expense.

What I do is setup all the routers in my palatial office on a dedicated LAN. I temporarily assign fixed IP addresses to the WAN side of each router so they can communicate without the internet being involved. I connect various laptops, junk PC's, and IP configurable junk laying around the office for testing on each router. I do the configuration, and test the hell out of it. It's important to be sure that various Windoze services (master browser) function. When happy, I ship the routers pre-configured to the remote offices for installation.

I will confess that I did read the manual, an un-natural act that I only perform under duress and only after first blundering through the VPN configuration exercise through Learn By Destroying(tm). It's somewhat complicated, but once the buzzwords and technology is understood, it's fairly simple.

Here's a sample configuration for a Dlink DI-804HV VPN router:

http://support.dlink.com/faq/view.asp?prod_id=1295

http://support.dlink.com/faq/view.asp?prod_id=1383

Think you can handle that yourself?

Basically, the VPN is setup in 5 steps.

1. Setup the WAN side for whatever DSL connection you're using.
2. Setup the LAN side for local connectivity. Test for internet access. This is the same as any non-VPN router.
3. Setup the method of key exchange (IKE). I prefer pre-shared keys because of the simplicity. Each tunnel should have a different pre-shared key to avoid confusion.
4. Setup the method of encryption. DES and Triple DES are the usual choices.
5. Setup the method of authentication. MD5 and SHA are the common choices.
6. Setup the miscellaneous options such as passing NETBIOS broadcasts.
7. Test by pinging the opposite private LAN. Test for windoze (NETBIOS) connectivity with:
net view
\\server_name
Network neighborhood

If you approach the setup from the top down, in the above order, life will be easier.

Incidentally, one potential screwup is to assign the same Class C network IP block to both sides of the VPN tunnel. Don't do that. Use different blocks such as:

- 192.168.1.xxx one end of tunnel
- 192.168.2.xxx other end of tunnel

This way, it's obvious where a machine is located and also avoids duplicate IP address headaches. That means do NOT use the default IP address for the LAN side of the router as supplied by the manufacturer.

>4. There are all of these different kinds of authentication – user, >login, certificate. What do I really need? Different vendors all give >you different information.

Sigh. Keep it simple. You don't need certificates unless your into the ultimate in security. Pre-shared keys are good enough. I do use certificates for mobile and hostile sites (don't ask), where hacking is a potential problem. However, I've had more security issues with copies of the certificates being "borrowed" than with pre-shared keys that cannot be extracted from the router configuration.

For encryption, I'm partial to DES instead of 3DES because it's generally less overhead. If you ping a workstation through the tunnel and compare performance between DES and 3DES, there's usually a few milliseconds difference. If you're worried about someone sniffing your traffic, and decrypting it, go for 3DES. If your router supports AES, that's even better (and slower).

comp.security.firewalls: Re: HIPAA and firewalls

Authentication method is just a hash code. I use MD5 because everyone supports it. Same with mobile IPSec clients. SHA-1 is probably more secure.

Routers that do NOT have a user license limit are my preference. That means:

Linksys

<http://www.linksys.com/products/group.asp?grid=34&scid=29>

Dlink

<http://www.dlink.com/products/category.asp?cid=9>

Netgear

<http://www.netgear.com/products/routers/firewallvpn.php>

None of the above (to the best of my knowledge) have user license counts and additional user count charges. However, they do have limited number of tunnels and users. Generally, 253 users and 8-32 tunnels are common. Make sure you obtain these limits from the vendor before buying. You'll need at least 1 tunnel between each office and one additional tunnel for mobile (remote admin or home) users.

I've used Linksys BEFVP41 (\$90) , DLink DI-804HV (\$50), Netgear FVS318 (\$140) and some others. I do NOT consider these to be expensive. When I had a performance problem with BEFVP41 routers and determined it to be a firmware issue, I simply purchased a different pair of routers until Linksys could fix things (which they did after about 3 months).

Compare those prices with the Sonicwall TELE3, which costs \$500 for 10 users to start, costs approx \$50/user to upgrade (ouch), but does have some nifty features (V.90 modem fallback). However, to keep the user count low, you need to subnet your LAN's, keeping the print servers outside the routers LAN netmask or they will be counted as a user.

--

Jeff Liebermann jeffl@comix.santa-cruz.ca.us
150 Felker St #D 831-336-2558
Santa Cruz CA 95060 AE6KS