

Re: Authentication on PIX, WatchGuard, Safe@Office & SonicWall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-12/0679.html>

From: Leythos (void_at_nowhere.com)

Date: 12/11/03

Date: Thu, 11 Dec 2003 22:38:10 GMT

In article <irkhtv8gao2otkig4mk0gd36n9lcfbd2hj@4ax.com>, kennisonCUTITOUT@goodnet.com says...

>

> *Kind of a long post (preliminary set up w/questions at the end),*

> *please bear with me.*

>

> *I am looking to purchase a new firewall appliance to replace a Linksys*

> *Firewall/Router. I am evaluating (strictly from online literature and*

> *downloading the manuals) the following:*

>

> *Cisco PIX 506E*

> *WatchGuard Firebox III 500*

> *Checkpoint Safe@Office 225*

> *SocicWall Pro 230*

>

> *The firewall will sit between the Internet and Windows Small Business*

> *Server 2003 (Standard) with 10 XP workstations on the Network. I want*

> *this firewall to provide a strong authentication/authorization*

> *mechanism when accessing the local net remotely (I don't care about*

> *authenticating going from the inside out).*

>

> *I am currently providing Remote Access using the Remote Web Workspace*

> *that comes with SBS 2003 (which works great btw). This provides a*

> *simple alternative to VPN, and is more of a remote control service*

> *that allows remote users access to their desktop, network drives, and*

> *all their programs at work.*

>

> *This setup requires me to open ports 443 (https), 444 (Windows*

> *Sharepoint Service), and 4125. (Remote Web Workplace). My reason for*

> *wanting a strong authentication/authorization mechanism on the*

> *firewall is that I am concerned about an exploit being developed that*

> *will directly attack these ports on my server.*

Why not do it the simple easy way – let them VPN into the firewall, once in the firewall, they can access the network on all ports from the encrypted tunnel.

- > *However, as I start to look at the above firewalls I run into the*
- > *following issues (based on reading, no first hand experience):*
- [snip]
- > *With the WatchGuard Firebox III 500 it looks good until I read in the*
- > *User Guide (Pg 165–6) that when setting up users for remote access,*
- > *one of the steps is to provide their remote IP address. The whole*
- > *point of me using a user name mechanism is so I don't have to specify*
- > *a specific IP. The users can log on from any number of locations,*

That's not what it means – they are talking about remote users as in branch offices. If you get the 700 series it comes with VPN software that allows you to pre-package the VPN services and give the install disk to each person. You could also have them use aggressive mode and setup a Linksys at their homes, and create an IPSEC tunnel between the linksys (BEFVP41 unit) and the 700 so that they don't need anything on their computers. It would be 'nice' if they had fixed IP's, but with aggressive mode it will work with the remote offices (users) on a Dynamic connection.

- Am I missing something here with regards to the issues with these
- > *firewalls? (for example, does the WatchGuard not require me to*
 - > *specify an IP for the remote user, or that Safe@Office can*
 - > *authenticate on ports other than VPN)?*

I have a bunch of WG firewalls – for branch offices we use fixed IP's so that the tunnels between the offices are maintained 24/7 – even use some of the Linksys BEFVP41 units to create the remote offices side. You can also have remote users (individual ones) use the VPN software that is provided by WG – I think it's optional on the 500, but comes with 50 licenses on the 700.

- > *Should I be looking at some other method for authentication, such as*
- > *certificates (remembering that I want the authentication to take place*
- > *first on the firewall itself, and I don't want to restrict it to only*
- > *certain remote IP addresses)?*
- >
- > *Am I being too paranoid about having these ports (443, 444, 4125)*
- > *open? I do require complex passwords, but I am worried about exploits*
- > *on these ports that will negate the authentication taking place on the*
- > *server.*

Never open these ports (80/443 are ok) to the outside, there is no reason. If you do a VPN they can access everything inside the company network (if you build the firewall rules to allow it).

- > *Should I be looking at another product or solution? I do want to try*
- > *and keep the cost under \$1500.*

You could also just, and this is not the best idea, get a couple Linksys VPN units, and provide your 10 people with these pre-configured to allow IPsec back into the office. I would rather you do the firewall route.

My other idea, why are you not wanting to use ISA that comes with SBS?
(I don't use it either).

- > *Are there any remote client side issues that are going to be*
- > *problematic? (I hear people complain about WatchGuard's Java applet*
- > *having to be left open, but I can live w/ something like that)*

That's only if you want to authenticate going outbound on the firewall,
has nothing to do with VPN's.

- >
- > *Any other comments or suggestions would be appreciated.*
- >
- > *Thanks*
- > *Tracy Kennison*
- >
- >

--
--

spamfree999@rrohio.com
(Remove 999 to reply to me)