

Re: Site VPN failed between Checkpoint AI R55 gateways

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-04/0766.html>

From: Shekar (csekar21_at_yahoo.com)

Date: 04/20/04

Date: 20 Apr 2004 04:36:46 -0700

csekar21@yahoo.com (Shekar) wrote in message
news:<5e014759.0404071732.ed1fb91@posting.google.com>...
> rick@bcm.tmc.edu (Richard H Miller) wrote in message
news:<c4s3kn\$79m@gazette.corp.bcm.tmc.edu>...
>> Shekar (csekar21@yahoo.com) wrote:
>> : No problem with SIC, In fact i can push the policies without any problem.
>>
>>
>>
>>
>> : "Beoweolf" <Beoweolf@pacbell.net> wrote in message
news:<TPVbc.45983\$rB4.3033@newssvr25.news.prodigy.com>...
>> : > SIC? has it been established between the FW and Nokia?
>> : >
>> : >
>> : > "Shekar" <csekar21@yahoo.com> wrote in message
>> : > news:5e014759.0404040414.4795cfa@posting.google.com...
>> : > > Hi All,
>> : > >
>> : > > We are configuring new firewall in our local and remote office.
>> : > > Check point AI R55 with HFA-02
>> : > > Nokia IPSO 3.7.1
>> : > > Windows 2000 SP4
>> : > >
>> : > > Local vpn-1 pro enforcement module - Nokia IP 350
>> : > > Local checkpoint express smart center server - Windows 2000
>> : > > (Statically NATed and enabled control connection located in LAN)
>> : > >
>> : > > Remote vpn-1 pro enforcement module - Nokia IP 130
>> : > >
>> : > > We can push the policies no problem. But we are not getting log from
>> : > > remote module.
>> : > > Site vpn also failed even the time sync is correct.
>> : > > We have the following error in local log file - IKE: phase 1 received
>> : > > notification from peer, invalid certificate.
>> : > > Remote firewall module log shows the following error message.

comp.security.firewalls: Re: Site VPN failed between Checkpoint AI R55 gateways

> > : > > *IKE : Main mode validation timed out.*
> >
> >
> >
> > *Ok*
> >
> > *1) Did you define a rule in both modules policy to allow IKE. This will be before any encryption rules*
> > *and allows the two module to exchange key information*
> >
> > *2) Did you export your CA information and install a certificate on the remote box and setup the*
> > *appropriate*
> > *trust for the cert's [From the error message it looks like you have the vpn define as a cert]. Is there a*
> > *reson to use this instead of shared secret?*
> >
> > *3) Have you setup a rule to allow the enforcement module to completly talk with the management server*
> >
> > *Richard H. Miller, MCSE, CCSE+*
> > *Information Security Manager*
> > *Information Technology Security and Compliance*
> > *Information Technology – Baylor College of Medicine*
>
> *1. VPN comuunity rule allows from any and all service. Installed both*
> *firewalls*
> *2. I do not have export option since both firewalls are internally*
> *managed*
> *3. My first rule allows any service from remote firewall to management*
> *server*
>
> *My setup is like this,*
> *Local Firewall*
> *Nokia IP 350 – Enforcement Module (IPSO 3.7.1) (CP AI – R55 with*
> *HFA–2)*
> *Int interface – 10.65.16.1*
> *DMZ interface – 10.65.8.98*
> *Ext interface – 209.20.128.60.198*
>
> *Local Managment server*
> *Windows 2000 sp4 – Smart center (CP AI – R55 with HFA–2)*
> *IP address – 10.65.16.19 (Enabled static nat with ip address –*
> *209.20.128.199) (Also enabled the control connection)*
>
> *Remote firewall*
> *Nokia IP 130 – Enforcement Module (IPSO 3.7.1) (CP AI – R55 with*
> *HFA–2)*
> *Int interface – 10.86.16.1*
> *DMZ interface – 10.86.6.2*
> *Ext interface – 211.158.158.220*
>
> *First rule allows remote firewall to access management server (Service*
> *– ANY)*
> *also VPN community rule for site to site vpn (service – ANY)*

comp.security.firewalls: Re: Site VPN failed between Checkpoint AI R55 gateways

- > *Remote gateway & local gateway is the member of community.*
- > *Management server is also a Certificate authority. (Default)*
- >
- > *I can do SIC and push policies to remote firewall. But when I try to*
- > *ping remote internal ip address, It is trying to establish the tunnel.*
- > *But error msg shows (IKE phase 1 – received notification from*
- > *peer.invalid certificate) Even i am not receiving log from remote*
- > *firewall.*
- > *Both firewalls hosts file has the name and public IP address of*
- > *firewall and management server. So no problem with name resolution.*
- > *Date & time is correct in firewalls and management server.*

Hi,

My problem has been resolved by doing the following.

1) Install a NAT rule on the Remote module

- * Original Source: Remote module
- * Original Destination: INTERNAL IP address of the mgmt server
- * Original Service: ANY
- * Translated Source: original
- * Translated Destination: EXTERNAL IP address of the mgmt server
- * Translated service: original

2) Disable client side NATting for manual NAT rules

Policy – Global properties – NAT – Uncheck 'Translate destination on client side'