

RE: [fw-wiz] PIX to PIX IPSEC VPN IKE Phase 2 problem

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-02/msg00102.html>

- *From:* "Horvath, Kevin M." <KEVIN.M.HORVATH@XXXXXXXX>
 - *Date:* Tue, 7 Feb 2006 15:55:12 -0500
-

isakmp key ***** address xxx.yyy.191.66 netmask 255.255.255.255

Verify that the you can reach the HQ ip from the 501 via udp 500 and verify that the key matches what you have in the 501 config.....reset both keys to (no spaces either) the same passphrase and try again.

Kevin M. Horvath
CISSP,CCSP,INFOSEC,CCNA

From: firewall-wizards-admin@XXXXXXXXXXXXXXXXXXXXX
[<mailto:firewall-wizards-admin@XXXXXXXXXXXXXXXXXXXXX>] On Behalf Of Joe Keegan
Sent: Monday, February 06, 2006 12:37 PM
To: firewall-wizards@XXXXXXXXXXXXXXXXXXXXX
Subject: [fw-wiz] PIX to PIX IPSEC VPN IKE Phase 2 problem

I am trying to setup a branch office with a site-to-site VPN to our HQ office. The HQ PIX is a 515E with an existing VPN to an existing router at another site. The branch office has a PIX 501.
The debug crypto isakmp looks ok on the 501 except it looks to me that it is not completing IKE Phase 2.
ISAKMP (0): processing SA payload. message ID = 3634014145
ISAKMP : Checking IPsec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 3600
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-SHA
ISAKMP: key length is 128
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): SA not acceptable!
ISAKMP (0): sending NOTIFY message 14 protocol 0

RE: [fw-wiz] PIX to PIX IPSEC VPN IKE Phase 2 problem

```
return status is IKMP_ERR_NO_RETRANS
ISAKMP: No cert, and no keys (public or pre-shared) with remote peer
aa.bbb.194.253
VPN Peer:ISAKMP: Peer Info for aa.bbb.194.253/500 not found – peers:1
I believe this would be caused by an issue in a mismatched transform-set,
but everything looks OK to me.
Pertinent config info is below. Any help or ideas would be great. thanks!
HQ PIX 515E
access-list VPN-IRL remark Prevent any VoIP traffic to be routed over the
VPN to IRL
access-list VPN-IRL deny ip 10.10.0.0 255.255.0.0 172.18.0.0 255.255.0.0
access-list VPN-IRL remark Allow VPN connection to IRL
access-list VPN-IRL permit ip 10.0.0.0 255.192.0.0 172.18.0.0 255.255.0.0
access-list VPN-HIL remark Allow VPN connection to HIL
access-list VPN-HIL permit ip 10.0.0.0 255.192.0.0 172.20.0.0 255.255.0.0
access-list NO-NAT remark Don't NAT traffic sent to IRL
access-list NO-NAT permit ip 10.0.0.0 255.192.0.0 172.18.0.0 255.255.0.0
access-list NO-NAT remark Don't NAT traffic sent to HIL
access-list NO-NAT permit ip 10.0.0.0 255.192.0.0 172.20.0.0 255.255.0.0
nat (inside) 0 access-list NO-NAT
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
crypto ipsec security-association lifetime seconds 3600
crypto map VPN 100 ipsec-isakmp
crypto map VPN 100 match address VPN-IRL
crypto map VPN 100 set peer ccc.dd.154.114
crypto map VPN 100 set transform-set ESP-AES-SHA
crypto map VPN 200 ipsec-isakmp
crypto map VPN 200 match address VPN-HIL
crypto map VPN 200 set peer xxx.yyy.191.66
crypto map VPN 200 set transform-set ESP-AES-SHA
crypto map VPN interface outside
isakmp enable outside
isakmp key ***** address ccc.dd.154.114 netmask 255.255.255.255
isakmp key ***** address xxx.yyy.191.66 netmask 255.255.255.255
isakmp identity address
isakmp policy 100 authentication pre-share
isakmp policy 100 encryption aes
isakmp policy 100 hash sha
isakmp policy 100 group 2
isakmp policy 100 lifetime 3600
Branch PIX 501
access-list VPN permit ip 172.20.0.0 255.255.0.0 10.0.0.0 255.192.0.0
access-list NO-NAT permit ip 172.20.0.0 255.255.0.0 10.0.0.0 255.192.0.0
nat (inside) 0 access-list NO-NAT
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
crypto ipsec security-association lifetime seconds 3600
crypto map VPN 100 ipsec-isakmp
crypto map VPN 100 match address VPN
crypto map VPN 100 set peer aa.bbb.194.253
```

RE: [fw-wiz] PIX to PIX IPSEC VPN IKE Phase 2 problem

RE: [fw-wiz] PIX to PIX IPSEC VPN IKE Phase 2 problem

```
crypto map VPN 100 set transform-set ESP-AES-SHA
crypto map VPN interface outside
isakmp enable outside
isakmp key ***** address aa.bbb.194.253 netmask 255.255.255.255
isakmp identity address
isakmp policy 100 authentication pre-share
isakmp policy 100 encryption aes
isakmp policy 100 hash sha
isakmp policy 100 group 2
isakmp policy 100 lifetime 3600
```

I can post the entire debug session from both firewalls if it will help.

IP's for the two devices are as follows

HQ PIX IP = aa.bbb.194.253

Branch PIX IP = xxx.yyy.191.66

Thanks

Joe

Joe Keegan IT Systems Architect
(415) 330-2676 jkeegan@xxxxxxxxxxxxxxxxxx