

## Re: [fw-wiz] PIX split tunneling

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-02/0002.html>

---

**From:** Dave Mitchell ([dmitchell@viawest.net](mailto:dmitchell@viawest.net))

**Date:** 02/13/03

From: Dave Mitchell <[dmitchell@viawest.net](mailto:dmitchell@viawest.net)>

To: Malte von dem Hagen <[DocValde@gmx.de](mailto:DocValde@gmx.de)>

Date: Thu, 13 Feb 2003 13:58:26 -0700

Malte,

You need to apply access list (both directions) to the tunnel access in order for this to work properly. These will be the "Proxy Networks" negotiated in IKE phase 2.

i.e.

```
access-list RAS-IPSEC permit ip inside-net 255.255.255.0 ras-client-net 255.255.255.0
access-list RAS-IPSEC permit ip ras-client-net 255.255.255.0 inside-net 255.255.255.0
```

The easiest way to make this cleaner is to assign an IP from a pool to the VPN client during negotiation. The below will be the addresses to fill in the "ras-client-net" in the above access lists.

```
ip local pool vpn-pool 10.1.88.x-10.1.88.x
```

You also need to make sure you don't NAT for your pool space.

```
nat (outside) 0 access-list RAS-IPSEC
```

Finally, configure your tunnel group.

```
vpngroup rasvpn address-pool vpn-pool
vpngroup rasvpn dns-server x.x.x.x
vpngroup rasvpn default-domain blah.com
vpngroup rasvpn split-tunnel RAS-IPSEC
vpngroup rasvpn idle-time 3600
vpngroup rasvpn password *****
```

Hope that helps.

-dave

On Thu, Feb 13, 2003 at 06:45:52PM +0100, Malte von dem Hagen wrote:

> *Hi there again,*

>

> *i want to realize a VPN from a host with the Cisco VPN Client*

Re: [fw-wiz] PIX split tunneling

Firewall-Wizards: Re: [fw-wiz] PIX split tunneling

> to a PIX 525. I need split tunneling, so that only the traffic  
> to the secured subnet is encrypted. I just want to get that  
> baby running, it drives me insane. Maybe some of you could help  
> me, please.

>  
> With kind regards and thanks in advance,

>  
> Malte von dem Hagen

>  
>  
> See all information i could get so far:

>  
> Network Design:

> -----

>  
> Host\_B\_Services

> | 10.153.88.2

> |

> | 10.153.88.0/24

> |

> | 10.153.88.1 [inside]

> Cisco\_PIX\_525 Host\_A\_VPN\_Client

> | 172.23.78.9 [outside] | 153.100.79.34

> ||

> | 172.23.78.0/23 | 153.100.79.0/25

> ||

> | 172.23.78.5 | 153.100.79.1

> Router\_B Router\_A

> ||

> +-----+

> [Transfer network]

>

> Goal: Run a vpn tunnel from Host\_A to PIX with split tunneling

>

> Routing is working:

>

> The PIX is configured "permit any any" in both directions to

> make it easier :-) Of course this will change later.

>

>

> -----

> ' Without VPN:

> |

> | PING from Host\_A to Host\_B is working.

> | PING from Host\_A to PIX\_inside is not working.

> | PING from Host\_A to PIX\_outside is working.

> | PING from Host\_A to Router\_B is working.

> | PING from Host\_A to Router\_A is working.

> |

> | PING from Host\_B to PIX\_inside is working.

> | PING from Host\_B to PIX\_outside is not working.

Re: [fw-wiz] PIX split tunneling

Firewall-Wizards: Re: [fw-wiz] PIX split tunneling

```
> | PING from Host_B to Router_B is working.
> | PING from Host_B to Router_A is working.
> | PING from Host_B to Host_A is working
> `-----
>
> `After connecting to the PIX, the VPN Client's Logfile says:
> |
> | 1 14:33:05.405 02/13/03 Sev=Warning/3 IKE/0xA3000058
> | Received malformed message or negotiation no longer active
> | (message id: 0xE5FB86DE)
> `-----
>
> `With VPN:
> |
> | PING from Host_A to Host_B is not working.
> | VPN_Client Statistics say: Packets discarded
> |
> | PING from Host_A to PIX_inside is not working.
> | VPN_Client Statistics say: Packets discarded
> |
> | PING from Host_A to PIX_outside is not working.
> | VPN_Client Statistics say: Packets encyrpted
> |
> | PING from Host_A to Router_B is working.
> | VPN_Client Statistics say: Packets bypassed
> |
> | PING from Host_A to Router_A is working.
> | VPN_Client Statistics say: Packets bypassed
> |
> |
> | PING from Host_B to PIX_inside is working.
> | PING from Host_B to PIX_outside is not working.
> | PING from Host_B to Router_B is working.
> | PING from Host_B to Router_A is working.
> | PING from Host_B to Host_A is not working.
> | PING from Host_B to Host_A_virtualIP is not working.
> `-----
>
>
> =====<PIX Config>=====
> testpix# sh run
> : Saved
> :
> PIX Version 6.2(2)
> nameif ethernet0 outside security0
> nameif ethernet1 inside security100
> nameif ethernet2 intf2 security10
> nameif ethernet3 intf3 security15
> nameif ethernet4 intf4 security20
```

## Firewall-Wizards: Re: [fw-wiz] PIX split tunneling

```
> nameif ethernet5 intf5 security25
> enable password 8Ry2YjIyt7RRXU24 encrypted
> passwd 2KFQnbNIdI.2KYOU encrypted
> hostname testpix
> domain-name test.local
> fixup protocol ftp 21
> fixup protocol http 80
> fixup protocol h323 h225 1720
> fixup protocol h323 ras 1718-1719
> fixup protocol ils 389
> fixup protocol rsh 514
> fixup protocol rtsp 554
> fixup protocol smtp 25
> fixup protocol sqlnet 1521
> fixup protocol sip 5060
> fixup protocol skinny 2000
> names
> access-list testgroup_splitTunnelAcl permit ip 10.153.88.0 255.255.255.0 any
> access-list inside_outbound_nat0_acl permit ip 10.153.88.0 255.255.255.0 10.153.88.128 255.255.255.128
> access-list outside_cryptomap_dyn_20 permit ip any 10.153.88.128 255.255.255.128
> access-list outside_access_in permit ip any any
> pager lines 24
> interface ethernet0 10baset
> interface ethernet1 100full
> interface ethernet2 auto shutdown
> interface ethernet3 auto shutdown
> interface ethernet4 auto shutdown
> interface ethernet5 auto shutdown
> mtu outside 1500
> mtu inside 1500
> mtu intf2 1500
> mtu intf3 1500
> mtu intf4 1500
> mtu intf5 1500
> ip address outside 172.23.78.9 255.255.254.0
> ip address inside 10.153.88.1 255.255.255.0
> ip address intf2 127.0.0.1 255.255.255.255
> ip address intf3 127.0.0.1 255.255.255.255
> ip address intf4 127.0.0.1 255.255.255.255
> ip address intf5 127.0.0.1 255.255.255.255
> ip audit info action alarm
> ip audit attack action alarm
> ip local pool ippool 10.153.88.129-10.153.88.254
> no failover
> failover timeout 0:00:00
> failover poll 15
> failover ip address outside 0.0.0.0
> failover ip address inside 0.0.0.0
> failover ip address intf2 0.0.0.0
> failover ip address intf3 0.0.0.0
> failover ip address intf4 0.0.0.0
```

Re: [fw-wiz] PIX split tunneling

Firewall-Wizards: Re: [fw-wiz] PIX split tunneling

```
> failover ip address intf5 0.0.0.0
> pdm location 10.153.88.2 255.255.255.255 inside
> pdm history enable
> arp timeout 14400
> nat (inside) 0 access-list inside_outbound_nat0_acl
> nat (inside) 0 0.0.0.0 0.0.0.0 0 0
> access-group outside_access_in in interface outside
> route outside 0.0.0.0 0.0.0.0 172.23.78.1 1
> timeout xlate 3:00:00
> timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
> timeout uauth 0:05:00 absolute
> aaa-server TACACS+ protocol tacacs+
> aaa-server RADIUS protocol radius
> aaa-server LOCAL protocol local
> http server enable
> http 10.153.88.2 255.255.255.255 inside
> no snmp-server location
> no snmp-server contact
> snmp-server community public
> no snmp-server enable traps
> floodguard enable
> sysopt connection permit-ipsec
> no sysopt route dnat
> crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
> crypto dynamic-map outside_dyn_map 20 match address outside_cryptomap_dyn_20
> crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-SHA
> crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
> crypto map outside_map interface outside
> isakmp enable outside
> isakmp policy 20 authentication pre-share
> isakmp policy 20 encryption 3des
> isakmp policy 20 hash sha
> isakmp policy 20 group 2
> isakmp policy 20 lifetime 86400
> vpngroup testgroup address-pool ippool
> vpngroup testgroup split-tunnel testgroup_splitTunnelAcl
> vpngroup testgroup idle-time 1800
> vpngroup testgroup password *****
> telnet timeout 5
> ssh timeout 5
> terminal width 80
> Cryptochecksum:e2eb6019c28b0147d625aba4926f2f13
> : end
> testpix#
>
> =====</PIX Config>=====
>
>
> =====<VPN Client Config>=====
> [main]
```

Firewall-Wizards: Re: [fw-wiz] PIX split tunneling

```
> Description=test
> Host=172.23.78.9
> AuthType=1
> GroupName=testgroup
> GroupPwd=
>
enc_GroupPwd=3D26A9C73AF4B09AAB6233B1F9A46C2F9D5E01345835100AD955BB6180D0FBB100FFD2A2D
> EnableISPConnect=0
> ISPConnectType=1
> ISPConnect=
> ISPCommand=
> Username=
> SaveUserPassword=0
> UserPassword=
> enc_UserPassword=
> NTDomain=
> EnableBackup=0
> BackupServer=
> EnableMSLogon=1
> MSLogonType=0
> EnableNat=0
> TunnelingMode=0
> TcpTunnelingPort=10000
> CertStore=0
> CertName=
> CertPath=
> CertSubjectName=
> CertSerialHash=00000000000000000000000000000000
> SendCertChain=0
> VerifyCertDN=
> DHGroup=2
> ForceKeepAlives=0
> PeerTimeout=90
> EnableLocalLAN=1
> EnableSplitDNS=1
> ForceNetLogin=0
> =====</VPN Client Config>=====
>
> --
> Malte von dem Hagen
>
> DocValde@gmx.de
> http://www.docvalde.net/
>
> _____
> firewall-wizards mailing list
> firewall-wizards@honor.icsalabs.com
> http://honor.icsalabs.com/mailman/listinfo/firewall-wizards
--
-----
```

Firewall-Wizards: Re: [fw-wiz] PIX split tunneling

Dave Mitchell  
Network Engineer, ViaWest  
[dmitchell@viawest.net](mailto:dmitchell@viawest.net)  
(720) 891-1045  
-----

---

firewall-wizards mailing list  
[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>