

## Cisco PIX Firewall and VPN example

Contributed by John Nikolatos  
Tuesday, 09 January 2007

Here is a general example trying to explain how to set up a PIX firewall for site to site VPN and block all inbound traffic except for MAIL and WEB traffic to a specific host.

The inside IP addresses are in the range 172.16.254.X

The outside IP addresses are in the range of 161.53.124.X

The Remote network trying to site-to-site VPN into the primary location is 192.168.20.X

Add an access-list so you do not NAT VPN pool ip addresses or remote network (192.168.20.x) ip addresses

```
access-list 100 permit ip  
172.16.254.0 255.255.255.0 192.168.20.0 255.255.255.0
```

```
access-list 100 permit  
ip 172.16.254.0 255.255.255.0 192.168.15.0 255.255.255.0
```

add  
access-list for interesting site to site VPN traffic to bring up tunnel and route packets to remote network.

```
access-list 110 permit ip 172.16.254.0  
255.255.255.0 192.168.20.0 255.255.255.0
```

Add access-list for email and web -inbound

```
access-list OUTSIDE-EMAIL permit tcp any host 161.53.124.14 eq 25
```

```
access-list OUTSIDE-EMAIL permit tcp any host 161.53.124.14 eq 80
```

```
ip address inside 172.16.254.1 255.255.0.0
```

Set an outside IP address for the mail and web server at 172.16.254.6

```
static (inside,outside) 161.53.124.14 172.16.254.6 netmask 255.255.255.0 0
```

Allow email and web traffic in-bound by calling access-list

```
access-group OUTSIDE-EMAIL in interface outside
```

Call the access list 100 so you do not NAT traffic to other networks, use Interface0 IP address for all outside communications.

```
global (outside) 1 interface
```

```
nat (inside) 0 access-list 100
```

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

You need to define a IPPOOL for client software VPN's to get an IP address:

```
ip local pool VPN-IP-Pool 192.168.15.1-192.168.15.30
```

Here is config for OPEN Site to Site VPN : "DES" encryption - call access-list to define interestign traffic (must be different access-list than others!!!) 0.0.0.0 address below allows any

IP address with the correct password to terminate VPN connections.

```
sysopt
connection permit-ipsec

no sysopt route dnat

crypto ipsec transform-set
myset esp-des esp-md5-hmac

crypto dynamic-map dynmap 30 set transform-set
myset

crypto map newmap 20 ipsec-isakmp dynamic dynmap

crypto map newmap
20 match address 110

crypto map newmap interface outside

isakmp enable
outside

isakmp key MAKE-SOME-PASSWORD-HERE address 0.0.0.0 netmask
0.0.0.0

isakmp identity address

isakmp policy 10 authentication
pre-share

isakmp policy 10 encryption des

isakmp policy 10 hash
md5

isakmp policy 10 group 1

isakmp policy 10 lifetime 86400

isakmp
policy 20 authentication pre-share

isakmp policy 20 encryption des

isakmp
policy 20 hash md5

isakmp policy 20 group 2

isakmp policy 20 lifetime
86400
```

This is for client software VPN termination for group called "vpn3000"

```
vpngroup vpn3000 address-pool ippool

vpngroup vpn3000
dns-server 10.1.1.2

vpngroup vpn3000 wins-server 10.1.1.2
```

```
vpngroup vpn3000  
default-domain cisco.com
```

```
vpngroup vpn3000 split-tunnel 101
```

```
vpngroup  
vpn3000 idle-time 1800
```

```
vpngroup vpn3000 password  
MAKE-SOME-PASSWORD-HERE
```

Allow SSH in-bound from specific IP address  
example 66.3.3.3 or anyone

```
ssh 66.3.3.3 255.255.255.255 outside
```

```
ssh  
0.0.0.0 0.0.0.0 outside
```

Copyright John Nikolatos NIKTEK LLC