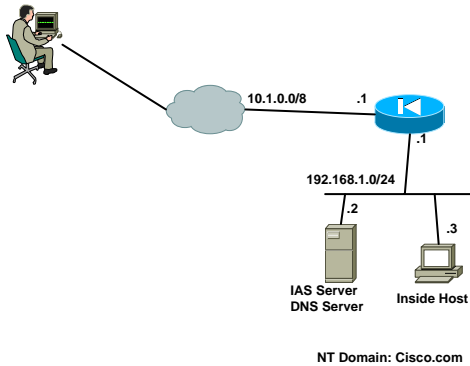


Access VPN cheat sheet



1- Prepare system for VPN

```
pix(config)#isakmp enable outside
pix(config)#sysopt connection permit-ipsecc
```

2- Create ISAKMP policy

```
pix(config)#isakmp identity address
pix(config)#isakmp policy 10 authentication pre-share
pix(config)#isakmp policy 10 encryption 3des
pix(config)#isakmp policy 10 hash sha
pix(config)#isakmp policy 10 lifetime 84600
pix(config)#isakmp policy 10 group 2
pix(config)#isakmp nat-traversal 20
```

3- Create IPSEC transform-set

```
pix(config)#ipsec transform-set remote esp-3des esp-sha-hmac
```

4- Create dynamic crypto map

```
pix(config)#dynamic-map remote 10 set transform-set remote
```

5- Create static map and apply to interface

```
pix(config)#map dialin 65535 ipsec-isakmp dynamic remote
pix(config)#map dialin interface outside
```

6- Create remote client address pool

```
pix(config)#ip local pool remote 192.168.2.1-192.168.2.254
```

7- Create ACL (nat 0)

```
pix(config)#access-list vpn permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
pix(config)#nat (inside) 0 access-list vpn
```

In case of MORE THAN ONE ACCESS VPN:

```
pix(config)#access-list multivpn permit ip any 192.168.2.0 255.255.255.0
pix(config)#dynamic-map remote 20 match address multivpn
```

8- Create VPN Group

```
pix(config)#vpngroup remote address-pool remote
pix(config)#vpngroup remote password cisco
pix(config)#vpngroup remote dns-server 192.168.1.2
pix(config)#vpngroup remote default-domain cisco.com
pix(config)#vpngroup remote split-dns cisco.com
pix(config)#vpngroup remote split-tunnel vpn
```

9- Authentication

```
pix(config)#aaa-server IAS protocol radius
pix(config)#aaa-server (inside) host 192.168.1.2 fns123
pix(config)#map dialin client authentication IAS
```

client authentication is global, remember to use no-xauth at the end of the key setting on the isakmp policy for site-to-site VPNs

```
pix(config)#isakmp key FNS123 address 10.1.0.1 netmask 255.0.0.0 no-xauth
```