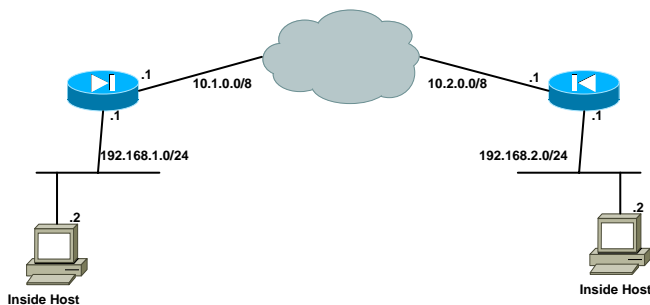


Site-to-Site VPN cheat sheet



PIX (10.1.0.1)

1- Prepare system for VPN

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

2- 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
```

3- Create ISAKMP policy

```
pix(config)#isakmp identity address
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 policy 10 authentication pre-share
pix(config)#isakmp key FNS123 address 10.2.0.1 netmask 255.255.255.255
```

4- Create IPSEC transform-set

```
pix(config)#ipsec transform-set site2site esp-3des esp-sha-hmac
```

5- Create static map and apply to interface

```
pix(config)#map site2site 10 ipsec-isakmp
pix(config)#map site2site 10 set peer 10.2.0.1
pix(config)#map site2site 10 set transform-set site2site
pix(config)#map site2site 10 match address vpn
pix(config)#map site2site interface outside
```

PIX (10.2.0.1)

1- Prepare system for VPN

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

2- Create ACL (nat 0)

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

3- Create ISAKMP policy

```
pix(config)#isakmp key FNS123 address 10.1.0.1 netmask 255.0.0.0
pix(config)#isakmp identity address
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 policy 10 authentication pre-share
```

4- Create IPSEC transform-set

```
pix(config)#ipsec transform-set site2site esp-3des esp-sha-hmac
```

5- Create static map and apply to interface

```
pix(config)#map site2site 10 ipsec-isakmp
pix(config)#map site2site 10 set peer 10.1.0.1
pix(config)#map site2site 10 set transform-set site2site
pix(config)#map site2site 10 match address vpn
pix(config)#map site2site interface outside
```