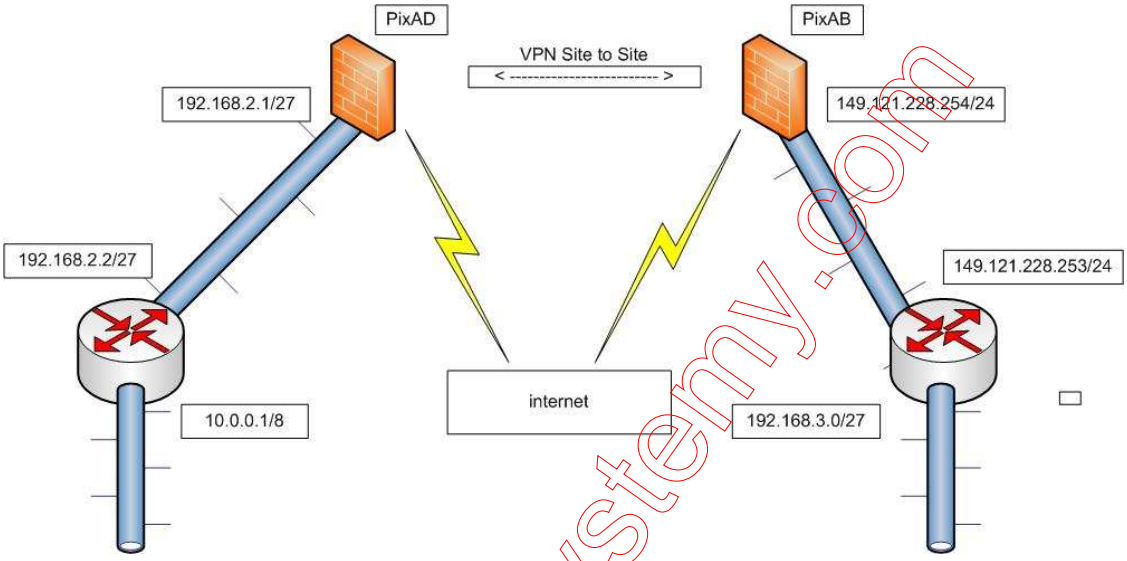
VPN SITE-TO-SITE

Pre-share key authentication

This manual was prepared using pix501 and pix516.



1. Create an isakmp policy – policy should be identical on each pix(type following commands on both):

- isakmp enable outside
- isakmp policy 1 authentication pre-share
- isakmp policy 1 encrypt aes-256
- isakmp policy 1 hash sha
- isakmp policy 1 group 1
- isakmp policy 1 lifetime 86400
- isakmp key our_key address PixIP(ip of remote pix)

2. Enable ipsec (PixAD and PixAB)

- sysopt connection permit-ipsec

3. Create access-lists which map traffic sending via tunnel

- (on PixAD)

access-list PixAB line 1 permit ip 10.0.0.0 255.0.0.0 192.168.3.0 255.255.255.224

access-list PixAB line 2 permit ip 10.0.0.0 255.0.0.0 149.121.228.0 255.255.255.0

access-list PixAB line 3 permit ip 192.168.2.0 255.255.255.224 192.168.3.0 255.255.255.224

access-list PixAB line 4 permit ip 192.168.2.0 255.255.255.224 149.121.228.0 255.255.255.0

- (on PixAB) – do a mirror of access-list

access-list PixAD line 1 permit ip 192.168.3.0 255.255.255.224 10.0.0.0 255.0.0.0

access-list PixAD line 2 permit ip 149.121.228.0 255.255.255.0 10.0.0.0 255.0.0.0

access-list PixAD line 3 permit ip 192.168.3.0 255.255.255.224 192.168.2.0 255.255.255.224

access-list PixAD line 4 permit ip 149.121.228.0 255.255.255.0 192.168.2.0 255.255.255.224

4. Create a transform-set(on both pixes)
- crypto ipsec transform-set ADDA esp-aes-256 esp-sha-hmac

5. Create a crypto map
- on PixAD

crypto map AD2AB 10 set transform-set ADDA
crypto map AD2AB 10 set peer “IP-remote PIX”
crypto map AD2AB 10 match address PixAB
crypto map AD2AB 10 ipsec-isakmp
crypto map AD2AB interface outside

- on PixAB

crypto map AB2AD 10 set transform-set ADDA
crypto map AB2AD 10 set peer "IP-remote PIX"
crypto map AB2AD 10 match address PixAD
crypto map AB2AD 10 ipsec-isakmp
crypto map AB2AD interface outside

6. If necessary disable vpn traffic from nat
- nat (inside) 0 access PixAB – on PixAD
- nat (inside) 0 access PixAD – on PixAB

Tunnel between localizations will be established when first packet is matched by PixAD or PixAB access-list.

Helpful commands:
clear crypto isakmp sa – delete security associations
clear crypto ipsec sa – delete security associations
debug crypto isakmp – in case of problems
debug crypto ipsec – in case of problems

dzbanek