

Cisco Secure PIX and NetScreen ScreenOS 2.5

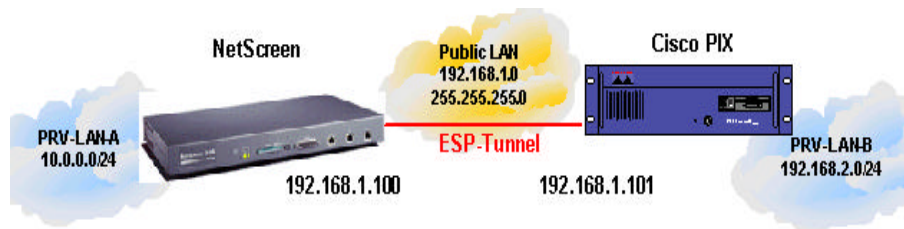
Introduction

This document shows examines basic configuration of a Cisco Secure PIX Firewall running Cisco IOS 5.2 for IPSec Interoperability with the NetScreen product line using ScreenOS 2.5. Basic configuration is defined as "gateway to gateway, main mode IPSec with IP Address identities"

Note: Without hardware acceleration on the Cisco PIX 3DES ciphers are extremely processor intensive. For this reason we will use DES-SHA1 transforms for IPSec.

Topology

In the example below the Cisco PIX is used as a gateway device and wishes to talk to a NetScreen for gateway-gateway access to another LAN. Preshared key IKE negotiation is used during Phase I and ESP Tunnel mode IPSec for Phase II.



The Solution

The NetScreen and the PIX must be configured to establish tunnel mode IPSec connections between each other. PRV-LAN-A, a 10.0.0.0/24 subnet wishes to talk to PRV-LAN-B 192.168.2.0/24 via this tunnel, same holds true for traffic in the other direction. This has been tried and tested with both NetScreen's ScreenOS 2.0 and 2.5 code as well as Cisco PIX 5.1 and 5.2 code with IPSec add-ons.

Below is the configuration used from both the NetScreen and Cisco PIX firewalls. Comments which have been added are marked by a "#" mark.

NetScreen Configuration:

- 2.01r5 Firmware
- set admin sys-ip 0.0.0.0
- set interface trust ip 10.0.0.1 255.255.255.0
- set interface untrust ip 192.168.1.100 255.255.255.0
- set address untrust "PRV-LAN-B" 192.168.2.0 255.255.255.0
- set address trust "PRV-LAN-A" 10.0.0.0 255.255.255.0
- set ike gateway "PIX" ip 192.168.1.101 Main preshare "1234567" proposal "pre-g2-des-sha"
- set ike accept-all-proposal
- set vpn "PIX" gateway "PIX" no-replay proposal "g2-esp-des-sha"
- set ike id-mode subnet
- set policy id 2 outgoing "PRV-LAN-A" "PRV-LAN-B" "ANY" Encrypt vpn-tunnel "PIX" log

Cisco PIX Configuration:

- PIX Version 5.2(1)
- nameif ethernet0 outside security0
- nameif ethernet1 inside security100
- hostname pix
- access-list vpn permit ip 192.168.2.0 255.255.255.0 10.0.0.0 255.255.255.0
- #an access list must be added, this is the information used during IKE negotiation
- interface ethernet0 auto
- interface ethernet1 auto
- icmp permit any outside
- icmp permit any inside
- icmp permit 192.168.2.0 255.255.255.0 inside
- mtu outside 1500
- mtu inside 1500
- ip address outside 192.168.1.101 255.255.255.0
- ip address inside 192.168.2.100 255.255.255.0
- ip audit info action alarm
- arp timeout 14400
- nat (inside) 0 access-list vpn
- route outside 0.0.0.0 0.0.0.0 192.168.1.5 1
- timeout xlate 3:00:00
- timeout conn 0:05:00 half-closed 0:10:00 udp 0:01:00 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
- no snmp-server location
- no snmp-server contact
- snmp-server community public
- no snmp-server enable traps
- floodguard enable
- sysopt connection permit-ipsec
- #Unconditionally trust the IPsec connection
- sysopt ipsec pl-compatible
- no sysopt route dnat
- crypto ipsec transform-set netscreen esp-des esp-sha-hmac
- #DES-SHA proposal
- crypto map netscreen 10 ipsec-isakmp
- crypto map netscreen 10 match address vpn
- crypto map netscreen 10 set peer 192.168.1.100
- #Peer NetScreen's untrusted IP Address
- crypto map netscreen 10 set transform-set netscreen
- crypto map netscreen interface outside
- isakmp enable outside
- # we want the tunnel terminated on the PIX's outside interface
- isakmp key 1234567 address 192.168.1.100 netmask 255.255.255.255
- # "1234567" represents the plain-text Preshared key used
- isakmp identity address
- isakmp policy 10 authentication pre-share
- isakmp policy 10 encryption des
- isakmp policy 10 hash sha
- isakmp policy 10 group 2
- isakmp policy 10 lifetime 14400