



Netopia VPN Application Note

Document Number 0000000-00-01

IPSec w/ IKE to a Cisco PIX Firewall

Written by: Jeff Linam
Date: {08-02-01}
Revised: None

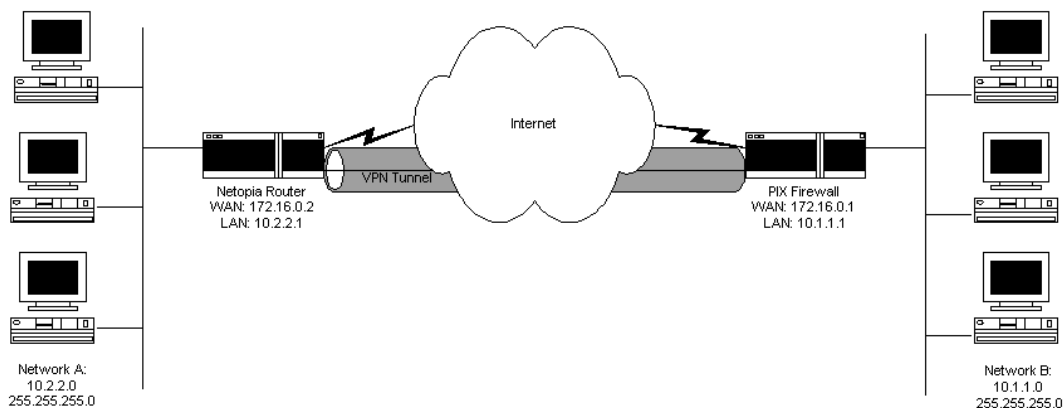
This application note describes the process of configuring the Netopia router to establish an IPSec tunnel using IKE to a Cisco PIX firewall.

Introduction

This document describes the configuration of an IPSec tunnel using IKE between a Netopia r-series router and a Cisco PIX firewall. Although implementation is essentially identical across the Netopia product line, the example configuration is based on an r9100 router and a PIX 506 firewall w/ VPN. The Netopia must have at a minimum firmware version 4.9, and the PIX must have at least 6.0 firmware. This example uses DES encryption with MD5 authentication, and operates in 'Main Mode' with shared secrets, although other options are also possible. In order to provide a detailed step-by-step configuration, a number of assumptions must be made about the configuration options used, particularly regarding the non-IPSec portions of the configuration. These options can be changed as desired or needed, but may lead to incompatible configurations.

Assumptions: This application note is for reference purposes only; it will need to be modified to suit individual needs, and thus a general working knowledge of the equipment used is assumed. It is further assumed that both the Netopia router and the PIX firewall are already configured for internet access, and that there are no access lists, firewalls, proxy servers, or NAT in place upstream from devices in question preventing access between the devices for UDP port 500 (IKE), protocol 50 (ESP) and protocol 51 (AH).

In this example the Netopia and the PIX are configured as follows:



	Netopia Router	PIX Firewall
LAN IP Address	10.2.2.1	10.1.1.1
LAN Subnet Mask	255.255.255.0	255.255.255.0
WAN IP Address	172.16.0.2	172.16.0.1
WAN Subnet Mask	255.255.0.0	255.255.0.0

Note that this makes the **network** address of the PIX's inside interface 10.1.1.0 and the **network** address of the Netopia's Ethernet interface 10.2.2.0 -- the network addresses will be used on several occasions during the configuration.

Configuration

Notes: This application note will first cover the creation of the phase1 (IKE) profile and the phase2 (IPSec) profile in the Netopia, and then proceed to the PIX configuration. In the Netopia, all connections are managed in a 'connection profile' that contains all the pertinent information and options for that connection. To change an IPSec profile that has already been created, go to WAN Configuration -> Change Connection Profile, and select the appropriate profile. To change an IKE profile that has already been created, go to WAN Configuration -> IPSec configuration. Do not make changes to settings not referenced in the configuration. Unlike other connection types, there is no need to establish an IPSec connection; once the profile is configured, the tunnel is automatically and transparently active. However, depending on hardware configuration, encryption options and etc. it can take up to two minutes for the tunnel to complete authentication and begin relaying traffic. Please bear this fact in mind when testing the tunnel connectivity with ping and other diagnostic tools. This configuration assumes that both sides of the VPN have static, valid Internet IP address on their WAN interfaces, and that NAT is not used in the VPN tunnel itself, though it may be used on the Internet connection.

Netopia Step-by-Step Configuration:

- 1) Telnet or Console into the router.
- 2) Go to WAN Configuration, Add Connection Profile
- 3) Give the Profile a Descriptive name, e.g. VPN to PIX, etc.
- 4) Set Data Link Encapsulation to IPSec
- 5) Select Data Link Options and hit ENTER
- 6) Key Management should be set to IKE.
- 7) Select IKE Phase 1 Profile, ADD PH1 PROFILE
- 8) Give the IKE Profile a Descriptive Name
- 9) Leave Mode at Main Mode
- 10) Set Local Identity Type to IPv4 Address
- 11) Set the Local Identity Value to the Local WAN address of your Netopia, e.g. 172.16.0.2
- 12) Set Remote Identity Type to IPv4 Address
- 13) Set the Remote Identity Value to the OUTSIDE address of the PIX, e.g. 172.16.0.1
- 14) Authentication Method should be set to Shared Secret
- 15) Enter the agreed upon pass phrase in the Shared Secret field. In our example, this is IlikeIkeButElvisIsKing. Note that this string is case sensitive, and that letters, numbers, spaces and wildcard characters all count as valid characters.
- 16) Set Encryption Algorithm to DES and Hash Algorithm to MD5
- 17) Leave Diffie-Hellman Group to Group 2 (1024 bits)
- 18) Leave the Advanced IKE Phase 1 Options alone and select ADD IKE PHASE 1 PROFILE. You will be back in the Data Link Options of the IPSec profile.
- 19) Make certain that the IKE Phase 1 Profile is set to the name of the profile you just created.
- 20) Set Encapsulation to ESP
- 21) Set ESP Encryption Transform to DES. If you have the VPN Accelerator card, you may also opt to use 3DES for higher security (you will need to adjust the PIX example configuration accordingly).
- 22) Set ESP Authentication Transform to HMAC-MD5-96. You may also opt to use HMAC-SHA1-96 for higher security (you will need to adjust the PIX example configuration accordingly).
- 23) Leave Compression Type to None and leave the Advanced IKE Options alone.
- 24) Hit ENTER on COMMIT. You will be back at the main screen of the IPSec Profile.
- 25) Select IP Profile Parameters
- 26) Set Remote Tunnel Endpoint to the Outside interface IP address of the PIX, e.g. 172.16.0.1
- 27) Set Remote Member Format to Subnet

- 28) Set Remote Member Address to the Inside interface's **network** address on the PIX -- in the example, 10.1.1.0 is the **network** address of the PIX's internal interface.
- 29) Set Remote Member Mask to the mask used on the PIX's Inside interface, e.g. 255.255.255.0
- 30) Set Local Member Format to Subnet
- 31) Set Local Member Address to the Netopia's LAN interface network address – 10.2.2.0 in the example.
- 32) Set the Local Member Mask to the mask used on the Netopia's LAN interface, e.g. 255.255.255.0
- 33) Leave Address Translation enabled set to no and Filter Set as None.
- 34) Leave the Advanced IP Profile Options alone and hit ENTER on COMMIT
- 35) COMMIT again to complete the profile.

This completes the Netopia portion of the configuration.

PIX Step-by-Step Configuration:

- 1) Go into enable mode by typing **enable** and entering the enable password
- 2) Go into config mode by typing **config t**
- 3) We need to permit the IPSec traffic by creating an access list with the following command:
- 4) **access-list ipsec permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0**
- 5) NAT should not be applied to the VPN tunnel. Enter the following commands:
- 6) **access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0**
- 7) **nat (inside) 0 access-list nonat**
- 8) **nat (inside) 1 10.1.1.0 255.255.255.0 0 0**
- 9) Next we need to configure the policies and transform set for the IPSec tunnel. The IPSec transform set in this example is called **netopiavpn** and the crypto map is called **r9100**. The example uses ESP encapsulation, DES encryption and MD5 as the hashing algorithms illustrated in the following commands:
- 10) **sysopt connection permit-ipsec**
- 11) **crypto ipsec transform-set netopiavpn esp-des esp-md5-hmac**
- 12) **crypto map r9100 21 ipsec-isakmp**
- 13) **crypto map r9100 21 match address ipsec**
- 14) **crypto map r9100 21 set peer 172.16.0.2**
- 15) **crypto map r9100 21 set transform-set netopiavpn**
- 16) **crypto map r9100 interface outside**
- 17) Finally, we set the IKE configuration. In this example, we are using a pre-shared key (**ILikeIkeButElvisIsKing**), DES encryption, MD5 hashing algorithm, Diffie-Hellman group2 and a key lifetime of 28800 seconds. We also specify that the IPSec peer is identified by a single IP address (172.16.0.2). Note the use of the all 255's net mask to identify a single IP address:
- 18) **isakmp enable outside**
- 19) **isakmp key ILikeIkeButElvisIsKing address 172.16.0.2 netmask 255.255.255.255**
- 20) **isakmp identity address**
- 21) **isakmp policy 21 authentication pre-share**
- 22) **isakmp policy 21 encryption des**
- 23) **isakmp policy 21 hash md5**
- 24) **isakmp policy 21 group 2**
- 25) **isakmp policy 21 lifetime 28800**

This completes the PIX configuration.

At this point, you are ready to test the configuration. Bear in mind that the tunnel can take upwards of 90 seconds to authenticate, so if you are testing using ping, send at least 100 packets.