Configuring a PC to Remotely Administer a Cisco Router Using the Router Console

This document details the remote client configuration for establishing an IPSec VPN tunnel from a PC running Windows 2000/XP and the SafeNet High Assurance Remote VPN client to a Cisco router. This is a companion document to "Configuring a Cisco Router for Remote Administration Using the Router Console", which describes how to configure the router side for remote administration with IPSec.

The SafeNet High Assurance Remote VPN client software can be obtained by following the instructions at the "US Government Customers Security Download Center" link at the **http://www.safenet-inc.com** web site (look for the USA flag in the upper right side of the web page). This configuration was verified for software version 1.7.6 (Build 4).

Network Setup

For this configuration, there will be a Cisco router to be managed and one management PC. The management PC will have IP address 192.168.45.67 and the Cisco router will be managed through its interface with IP address 192.168.45.100. Ideally, only administrators would use the management PC and that PC would not connect to external networks or be used for tasks such as email or web browsing. See Figure 1.

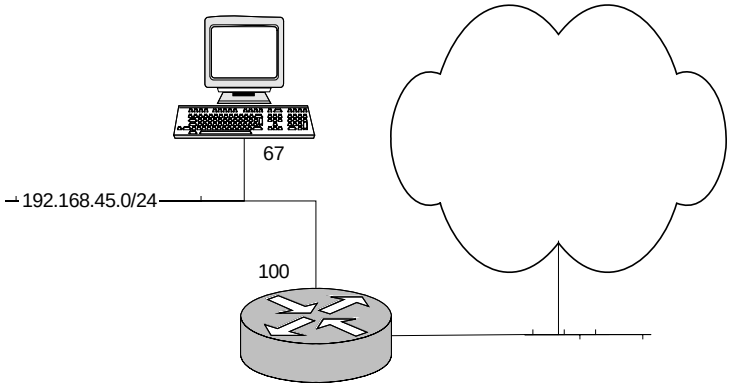

Figure 1: Network Diagram

The ISAKMP Policy and Security Association

The ISAKMP policy parameters:

- Triple DES as the encryption algorithm.
- SHA-1 as the hash algorithm.
- Diffie-Hellman Group 5.
- Pre-shared keys.

The IPSec Security Association parameters:

- Triple DES as the encryption algorithm.
- SHA-1 as the hash algorithm.
- Transport mode.

Configuration of the IPSec Parameters in the SafeNet VPN Client

The SafeNet High Assurance Remote client will be used in the "Specified Connection" mode. This mode is selected via "Secure" in the "Options" pull-down menu. Once in "Specified Connection" mode, add a new connection under "My Connections". The initial option menu has sections "Connection Security" and "Remote Party Identity and Addressing". Set the following options:

- Under "Connection Security" the "Secure" option should be checked (default).
- Under "Remote Party Identity and Addressing", set the "ID Type" to "IP Address" and enter the IP address of the router interface (192.168.45.100). "Protocol" set to "All" and "Connect using" should NOT be checked (defaults).

Expand the initial option menu to reveal the "My Identity" and "Security Policy" sub-menus. Click on "My Identity" to reveal the associated options. Set the following options:

- Set "Select Certificate" to "None". This will reveal the "Pre-shared Key" button.
- Click on the "Pre-shared Key" button and enter the pre-shared key matching that entered in the router configuration.
- Set the "ID Type" to "IP Address".
- At the bottom in the "Internet Interface" area, set "Name" to the network device associated with the PC's IP address. This will automatically enter the IP address into the "IP Addr" field below "Name" as well as below "ID Type" (IP Address).

Click on "Security Policy". The default settings should be in effect which are "Main Mode" selected for the "Phase 1 Negotiation Mode", "PFS" NOT checked, and "Enable Replay Detection" checked.

Expand the "Security Policy" submenu to reveal the "Authentication" and "Key Exchange" submenus. Expand the "Authentication" submenu to reveal "Proposal 1". Click on "Proposal 1" to reveal its settings. Change the settings to the following:

- "Pre-shared Key" for the "Authentication Method".
- "Triple DES" for the "Encrypt Alg".
- "SHA-1" for the "Hash Alg".
- Leave "SA Life" as "Unspecified".
- "Diffie-Hellman Group 5" for the "Key Group".

Expand the "Key Exchange" submenu to reveal "Proposal 1". Click on "Proposal 1" to reveal its settings. Change the settings to the following:

- Leave "SA Life" as "Unspecified" and "Compression" as "None".
- "Encapsulation Protocol (ESP)" should be checked (default).
- "Triple DES" for the "Encrypt Alg".
- "SHA-1" for the "Hash Alg.
- "Transport" for the "Encapsulation".
- "Authentication Protocol (AH)" should NOT be checked (default).

Save the settings.

Once the router is configured using the companion document "Configuring a Cisco Router for Remote Administration Using the Router Console", the VPN tunnel can be established. This will provide a secure connection for administrating the router using, for example, a telnet connection.