Configuring a Cisco Router for Remote Administration Using the Router Console

A secure channel is necessary for remote administration of Cisco routers. Cisco provides support for SSH and IPSec as a means for such a channel. However, at the time of this writing, Cisco's implementation of SSH cannot be recommended as their router IOS only supports Diffie-Hellman group 1 for the authentication group. Use of an IPSec VPN tunnel with Diffie-Hellman group 5 as the authentication group is recommended for high value networks with a migration strategy towards Diffie-Hellman group 14 as it becomes available.

This document details the router configuration for establishing an IPSec VPN tunnel from a PC running Windows 2000/XP and the SafeNet High Assurance Remote VPN client. The companion document, "Configuring a PC to Remotely Administer a Cisco Router Using the Router Console", details the associated remote client configuration.

Note: The router configuration requires an IOS build that supports 3DES (triple-DES).

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. See Figure 1.

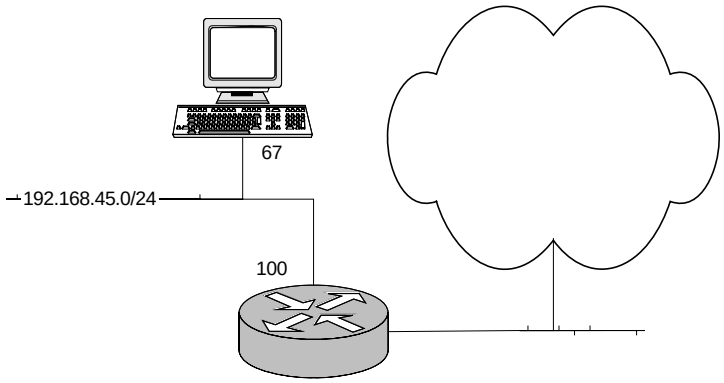

Figure 1: Network Diagram

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 on the Cisco Router

The following commands will add the ISAKMP parameters to the ISAKMP policy list:

```
router# config t
router (config)# crypto isakmp policy 20
router (config-isakmp)# encr 3des
router (config-isakmp)# hash sha
router (config-isakmp)# authentication pre-share
router (config-isakmp)# group 5
router (config-isakmp)# exit
router (config)#
```

The pre-shared key is set using the following command:

```
router (config)# crypto isakmp key 0 thepassphrase address 192.168.45.67
```

This will produce a pre-shared key with value “thepassphrase”. Replace “thepassphrase” with a random alphanumeric (a-z, A-Z, 0-9) string that is minimally 19 characters long.

The IPSec Security Association is added with the following command:

```
router (config)# crypto ipsec transform-set admin_3des esp-3des esp-sha-hmac
router (cfg-config-trans)# mode transport
router (cfg-config-trans)# exit
router (config)#
```

Finally, a crypto map must be created and then applied to the appropriate router interface. The crypto map uses an ACL to indicate which outgoing traffic is to be encrypted. This will be traffic from the router to the administration PC and the following commands create this ACL:

```
router (config)# access-list 192 permit ip host 192.168.45.100 host 192.168.45.67
```

The crypto map can now be created using the following commands:

```
router (config)# crypto map ADMIN_MAP 10 ipsec-isakmp
router (config-crypto-map)# set peer 192.168.45.67
router (config-crypto-map)# set transform-set admin_3des
router (config-crypto-map)# match address 192
router (config-crypto-map)# exit
router (config)#
```

The crypto map is applied to the appropriate interface using the following commands:

```
router (config)# interface fastethernet 0/1
router (config-if)# crypto map ADMIN_MAP
router (config-if)# exit
router (config)# exit
router#
```

Once the management PC is configured using the companion document “Configuring a PC to Remotely Administer a Cisco Router 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.

The crypto operation can be verified using the following command:

```
router# show crypto ipsec sa
```