Configuring IPSec − Wild−card Pre−shared Keys with Cisco Secure VPN Client and No−mode Config

Document ID: 14148

Cisco Secure VPN Client 1.x is End−of−Life. For details, refer to Product Bulletins 938.

Contents

Introduction

This sample configuration illustrates a router configured for wild−card pre−shared keys all PC clients share a common key. A remote user enters the network, keeping its own IP address; data between the PC of a remote user and the router is encrypted.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco IOS® Software Release 12.2.8.T1
- Cisco Secure VPN Client version 1.0 or 1.1 End−of−Life
- Cisco router with DES or 3DES image

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

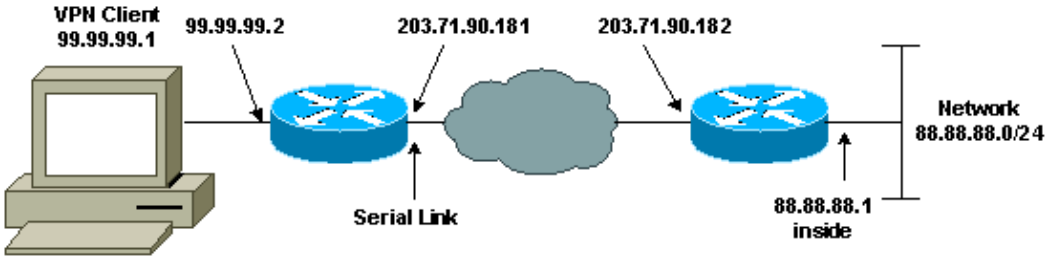
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses the network setup shown in the diagram below.



Configurations

This document uses the configurations shown below.

- Router Configuration
- VPN Client Configuration

Router Configuration

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
```

```
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

VPN Client Configuration

```
Network Security policy:


1- Myconn
    My Identity
         Connection security: Secure
         Remote Party Identity and addressing
         ID Type: IP subnet
         88.88.88.0
         255.255.255.0
         Port all Protocol all


    Connect using secure tunnel
         ID Type: IP address
         203.71.90.182


    Authentication (Phase 1)
    Proposal 1

        Authentication method: Preshared key
        Encryp Alg: DES
        Hash Alg: MD5
        SA life:  Unspecified
        Key Group: DH 1

    Key exchange (Phase 2)
    Proposal 1
        Encapsulation ESP
```

```
        Encrypt Alg: DES
        Hash Alg: MD5
        Encap: tunnel
        SA life: Unspecified
        no AH

2- Other Connections
       Connection security: Non-secure
       Local Network Interface
         Name: Any
         IP Addr: Any
         Port: All
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show crypto isakmp sa** Shows Phase 1 security associations.
- **show crypto ipsec sa** Shows Phase 1 security associations and proxy, encapsulation, encryption, decapsulation, and decryption information.
- **show crypto engine connections active** Shows current connections and information regarding encrypted and decrypted packets.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

Note: You must clear security associations on both peers. Perform the router commands in non−enable mode.

Note: You must run these debugs on both IPSec peers.

- **debug crypto isakmp** Displays errors during Phase 1.
- **debug crypto ipsec** Displays errors during Phase 2.
- **debug crypto engine** Displays information from the crypto engine.
- **clear crypto isakmp** Clears the Phase 1 security associations.
- **clear crypto sa** Clears the Phase 2 security associations.

Related Information

- **IPSec Support Page**
- **VPN 3000 Client Support Pages**
- **Technical Support − Cisco Systems**

Updated: Jan 19, 2006 Document ID: 14148