Configuring Router Mode−config, Wild−card, Pre−shared Keys, no NAT

Document ID: 14135

Contents

Introduction

In this sample configuration, a router is configured for mode configuration (get an IP address from the pool), wild−card, pre−shared keys (all PC clients share a common key), without Network Address Translation (NAT). An off−site user can enter the network and have an internal IP address assigned from the pool. To users, it appears that they are inside the network. Devices inside the network are set up with routes to the un−routable 10.2.1.x pool.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software 12.0.7T or later
- Hardware that supports this software revision
- CiscoSecure VPN Client 1.0/1.0.A or 1.1 (shown as 2.0.7/E or 2.1.12, respectively, go to **Help** > **About** to check)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

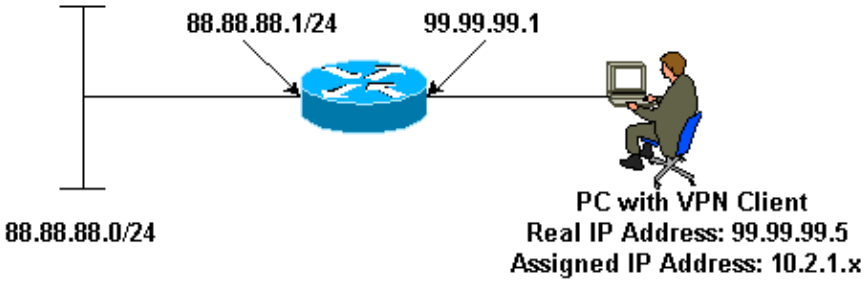
Configure

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 this network setup:



Configurations

This document uses these configurations:

- VPN Client
- Router

VPN Client

```
Network Security policy:

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

                Connect using secure tunnel
                        ID Type: IP address
                        99.99.99.1
                        Pre-shared key = cisco123

        Authentication (Phase 1)
        Proposal 1
                Authentication method: pre-shared 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
```

Router

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
enable password ww
!
username cisco password 0 cisco
!
clock timezone EST -5
ip subnet-zero
cns event-service server
!

crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local ourpool
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
 set transform-set trans1
crypto map intmap client configuration address initiate
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Ethernet0

 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache

 crypto map intmap
!
interface Ethernet1
 ip address 88.88.88.1 255.255.255.0
 no ip directed-broadcast
!

ip local pool ourpool 10.2.1.1 10.2.1.254
ip classless
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
```

```
 password ww
 login
!
end
```

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 engine connections active** Shows the encrypted and decrypted packets.
- **show crypto ipsec sa** Shows the phase 2 security associations.
- **show crypto isakmp sa** Shows the phase 1 security associations.

These debugs must be running on both IPSec routers (peers). Clearing security associations must be done on both peers.

- **debug crypto ipsec** Shows the IPSec negotiations of phase 2.
- **debug crypto isakmp** Shows the the ISAKMP negotiations of phase 1.
- **debug crypto engine** Shows the traffic that is encrypted.
- **clear crypto isakmp** Clears the security associations related to phase 1.
- **clear crypto sa** Clears the security associations related to phase 2.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **VPN 3000 Series Concentrators Product Support**
- **Cisco VPN 3000 Client Product Support**
- **IPSec (IP Security Protocol) Technology Support**
- **Technical Support − Cisco Systems**

Updated: Feb 17, 2005 Document ID: 14135