Konfigurieren von Router Mode-config, Wild Card, Pre-Shared Keys, kein NAT

Inhalt

Einführung

In dieser Beispielkonfiguration wird ein Router für die Moduskonfiguration (IP-Adresse aus dem Pool abrufen), für Platzhalter und vorinstallierte Schlüssel (alle PC-Clients teilen einen gemeinsamen Schlüssel) ohne Network Address Translation (NAT) konfiguriert. Ein externer Benutzer kann das Netzwerk betreten und über eine interne IP-Adresse verfügen, die dem Pool zugewiesen ist. Benutzer scheinen sich im Netzwerk zu befinden. Geräte im Netzwerk werden mit Routen zum nicht routbaren 10.2.1.x-Pool eingerichtet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Software 12.0.7T oder höher
- Hardware, die diese Softwareversion unterstützt
- CiscoSecure VPN Client 1.0/1.0.A oder 1.1 (als 2.0.7/E bzw. 2.1.12 angezeigt): Gehen Sie zu **Hilfe > Info**, um zu überprüfen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions .

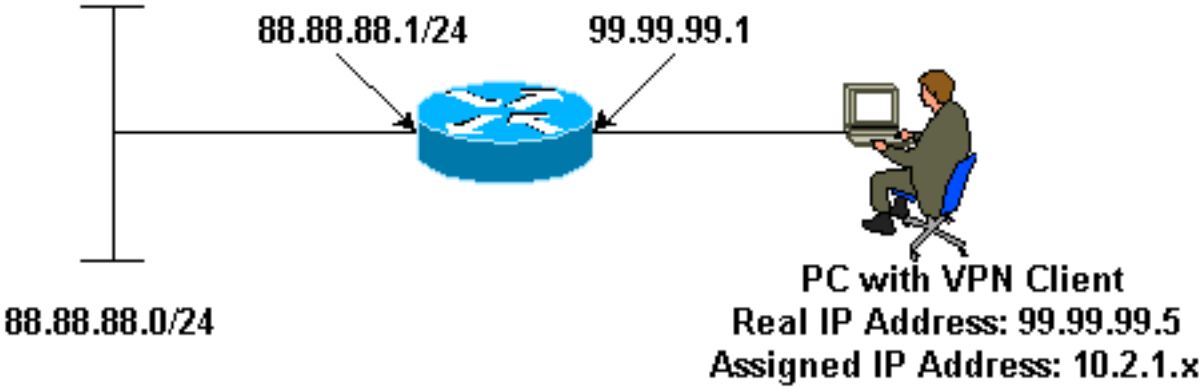
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- 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
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto engine connections active** - Zeigt die verschlüsselten und entschlüsselten Pakete an.
- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1.

Diese Debugger müssen auf beiden IPSec-Routern (Peers) ausgeführt werden. Das Löschen von Sicherheitszuordnungen muss auf beiden Peers erfolgen.

- **debug crypto ipsec** —Zeigt die IPSec-Verhandlungen von Phase 2.
- **debug crypto isakmp** - Zeigt die ISAKMP-Verhandlungen von Phase 1.
- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **clear crypto isakmp** : Löscht die Sicherheitszuordnungen für Phase 1.
- **clear crypto sa** —Löscht die Sicherheitszuordnungen für Phase 2.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Produktunterstützung für VPN Concentrators der Serie 3000
- Produkt-Support für Cisco VPN 3000-Clients
- IPSec (IP Security Protocol)-Technologieunterstützung
- Technischer Support - Cisco Systems