Konfiguration von IPSec - Vorinstallierte Wild-Card-Schlüssel mit Cisco Secure VPN Client und No-Mode-Konfiguration

Inhalt

Einführung

In dieser Beispielkonfiguration wird ein Router veranschaulicht, der für vorinstallierte Schlüssel von Wildcard konfiguriert ist - alle PC-Clients verwenden einen gemeinsamen Schlüssel. Ein Remote-Benutzer betritt das Netzwerk und behält seine eigene IP-Adresse bei. Daten zwischen dem PC eines Remote-Benutzers und dem Router werden verschlüsselt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco IOS® Softwareversion 12.2.8.T1
- Cisco Secure VPN Client Version 1.0 oder 1.1 - End-of-Life
- Cisco Router mit DES- oder 3DES-Image

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

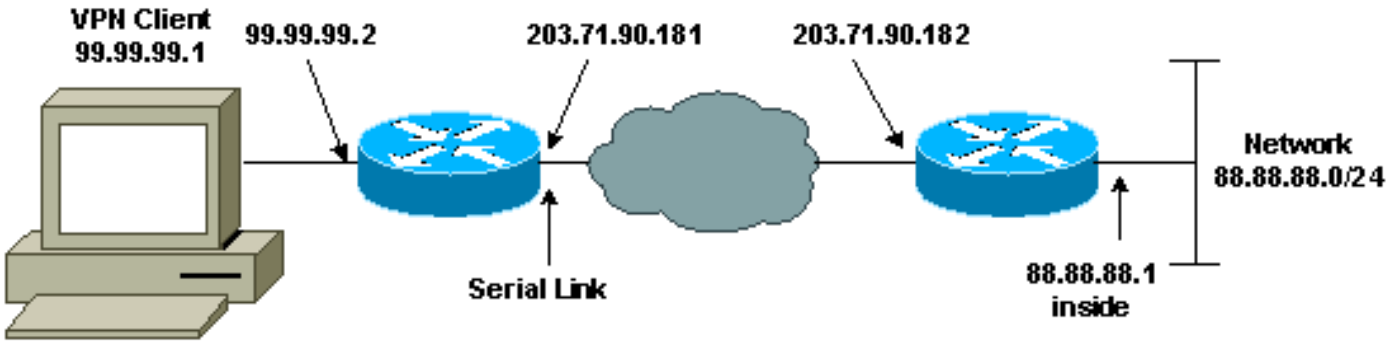
Konfigurieren

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 im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden die unten angegebenen Konfigurationen verwendet.

- Routerkonfiguration
- VPN-Client-Konfiguration

Routerkonfiguration

```
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-Konfiguration

```
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
```

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 isakmp sa** - Zeigt Sicherheitszuordnungen für Phase 1 an.
- **show crypto ipsec sa** - Zeigt Sicherheitszuordnungen für Phase 1 sowie Proxy-, Kapselungs-, Verschlüsselungs-, Entkapselungs- und Entschlüsselungsinformationen.
- **show crypto engine connections active** - Zeigt aktuelle Verbindungen und Informationen über verschlüsselte und entschlüsselte Pakete.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

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

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

Hinweis: Sie müssen die Sicherheitszuordnungen auf beiden Peers löschen. Führen Sie die Router-Befehle im nicht aktivierten Modus aus.

Hinweis: Sie müssen diese Debug auf beiden IPSec-Peers ausführen.

- **debug crypto isakmp** - Zeigt Fehler in Phase 1 an.
- **debug crypto ipsec** - Zeigt Fehler in Phase 2 an.
- **debug crypto engine** - Zeigt Informationen vom Crypto Engine an.
- **clear crypto isakmp** - Löscht die Sicherheitszuordnungen für Phase 1.
- **clear crypto sa** - Löscht die Sicherheitszuordnungen für Phase 2.

Zugehörige Informationen

- IPSec-Support-Seite
- VPN 3000 Client - Support-Seiten
- Technischer Support - Cisco Systems