Configuration d'IPSec - Clés prépartagées par carte générique avec Cisco Secure VPN Client et configuration sans mode

Contenu

Introduction

Cet exemple de configuration illustre un routeur configuré pour les clés pré-partagées de caractères génériques : tous les clients PC partagent une clé commune. Un utilisateur distant entre dans le réseau, en conservant sa propre adresse IP ; les données entre le PC d'un utilisateur distant et le routeur sont chiffrées.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Logiciel Cisco IOS® Version 12.2.8.T1
- Client VPN sécurisé Cisco version 1.0 ou 1.1 - Fin de vie
- Routeur Cisco avec image DES ou 3DES

Les informations présentées dans ce document ont été créées à partir de périphériques dans un

environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

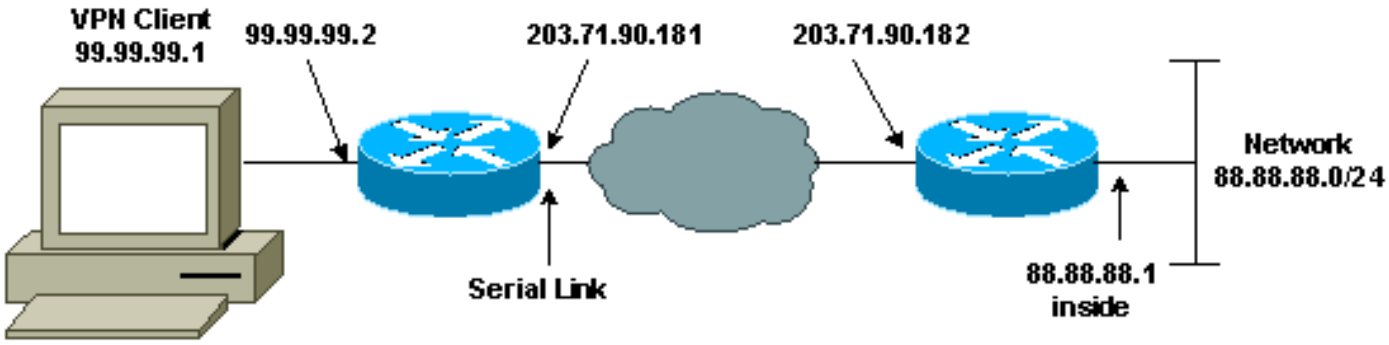
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configurations

Ce document utilise les configurations présentées ci-dessous.

- Configuration du routeur
- Configuration du client VPN

Configuration du routeur

```
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
```

Configuration du client VPN

```
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
```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto isakmp sa** - Affiche les associations de sécurité de la phase 1.
- **show crypto ipsec sa** - Affiche les associations de sécurité de phase 1 et les informations de proxy, d'encapsulation, de chiffrement, de décapsulation et de déchiffrement.
- **show crypto engine connections active** - Affiche les connexions et informations actuelles concernant les paquets chiffrés et déchiffrés.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque : avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

Remarque : vous devez supprimer les associations de sécurité sur les deux homologues. Exécutez les commandes du routeur en mode non actif.

Remarque : Vous devez exécuter ces débogages sur les deux homologues IPSec.

- **debug crypto isakmp** - Affiche les erreurs au cours de la phase 1.
- **debug crypto ipsec** - Affiche les erreurs pendant la phase 2.
- **debug crypto engine** — Affiche des informations du moteur de chiffrement.
- **clear crypto isakmp** : efface les associations de sécurité de phase 1.
- **clear crypto sa** : efface les associations de sécurité de phase 2.

Informations connexes

- Page d'assistance IPsec
- Pages d'assistance client VPN 3000
- Support technique - Cisco Systems