Configuration d'IPSec - Clés pré-partagées de caractère d'ambiguité avec le Cisco Secure VPN Client et le config de NO--mode

Contenu

Introduction

Cette configuration d'échantillon illustre un routeur configuré pour des clés pré-partagées de caractère d'ambiguité — tous les clients PC partagent une clé commune. Un utilisateur distant entre dans le réseau, gardant sa propre adresse IP ; des 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.

Composants utilisés

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

- Version de logiciel 12.2.8.T1 de Cisco IOS®
- Version 1.0 ou 1.1 de Cisco Secure VPN Client — Fin de vie
- Routeur de Cisco avec l'image DES ou 3DES

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

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). 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 utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

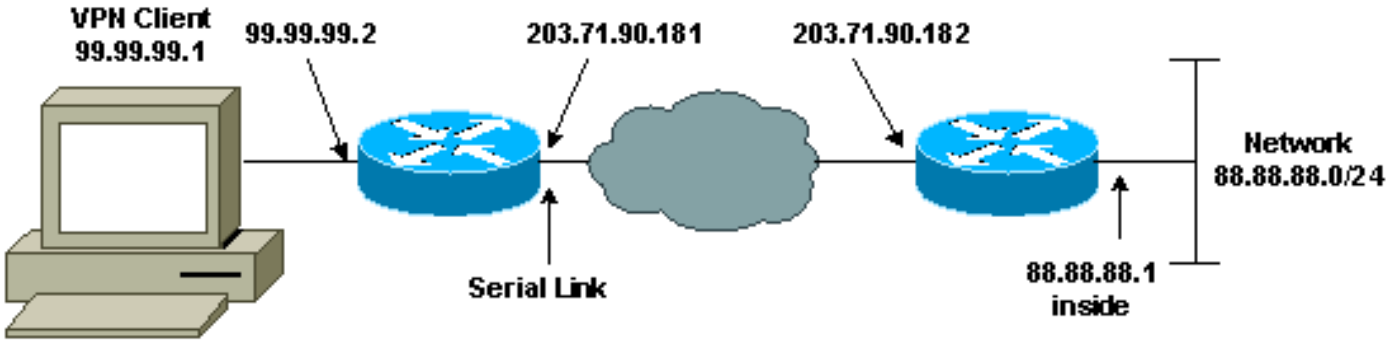
Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés 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

```
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
```

Vérifiez

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** — Associations de sécurité de Phase 1 d'expositions.
- **show crypto ipsec sa** — Associations de sécurité et proxy de Phase 1 d'expositions, encapsulation, cryptage, décapsulage, et informations de déchiffrement.
- **active de connexions de show crypto engine** — Connexions en cours et informations d'expositions concernant les paquets chiffrés et déchiffrés.

Dépannez

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 de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

Remarque: Vous devez autoriser des associations de sécurité sur les deux pairs. Exécutez les commandes de routeur dans le mode non activé.

Remarque: Vous devez exécuter ces derniers met au point sur les deux pairs d'IPSec.

- **debug crypto isakmp** — Affiche des erreurs pendant le Phase 1.
- **debug crypto ipsec** — Affiche des erreurs pendant le Phase 2.
- **debug crypto engine** — Affiche des informations du moteur de chiffrement.
- **clear crypto isakmp** — Autorise les associations de sécurité de Phase 1.
- **clear crypto sa** — Autorise les associations de sécurité de Phase 2.

Informations connexes

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