

Configuration du routeur en configuration de mode, clés génériques pré-partagées, sans NAT

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Dans cette configuration d'échantillon, un routeur est configuré pour la configuration de mode (obtenez une adresse IP du groupe), caractère d'ambiguïté, des clés pré-partagées (tous les clients PC partagent une clé commune), sans Traduction d'adresses de réseau (NAT). Un utilisateur de hors fonction-site peut entrer dans le réseau et avoir une adresse IP interne assignée du groupe. Les utilisateurs pensent qu'ils sont à l'intérieur du réseau. Des périphériques à l'intérieur du réseau sont installés avec des artères au groupe l'ONU-routable 10.2.1.x.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel 12.0.7T de Cisco IOS® ou plus tard
- Matériel qui prend en charge cette révision de logiciel
- Client vpn 1.0/1.0.A ou 1.1 de CiscoSecure (affiché comme 2.0.7/E ou 2.1.12, respectivement, allez **aider > environ** pour vérifier)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

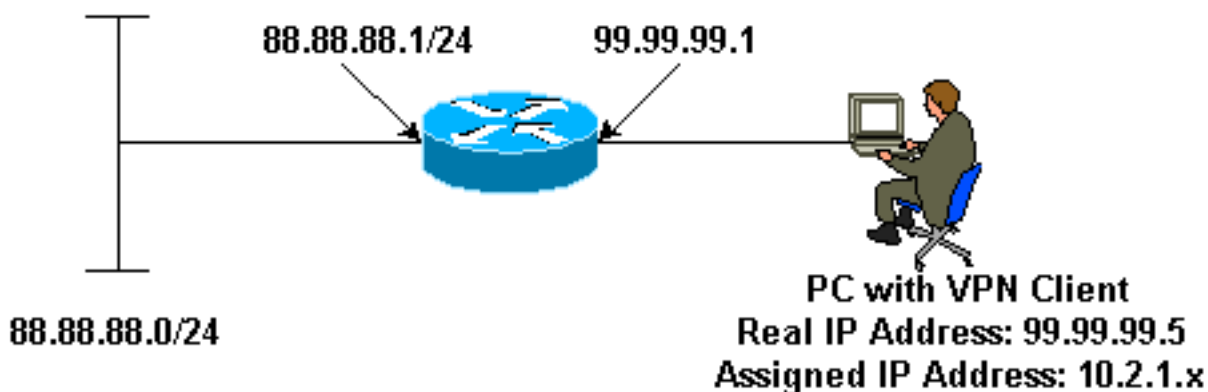
Configurez

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

Note: 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 suivante :



Configurations

Ce document utilise les configurations suivantes :

- [Client VPN](#)
- Routeur

Client VPN

```
.  
.  
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

Routeur

```
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
```

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.

- **active de connexions de show crypto engine** — Affiche les paquets chiffrés et déchiffrés.
- **show crypto ipsec sa** - Montre les associations de sécurisation de phase 2.
- **show crypto isakmp sa** - Montre les associations de sécurisation de phase 1.

Ceux-ci met au point doivent s'exécuter sur les deux Routeurs d'IPSec (pairs). L'autorisation des associations de sécurité doit être faite sur les deux pairs.

- **debug crypto ipsec** — Affiche les négociations IPSecs de la phase 2.
- **debug crypto isakmp** — Affiche les les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Montre le trafic crypté.
- **clear crypto isakmp** — Autorise les associations de sécurité liées à la phase 1.
- **clear crypto sa** — Autorise les associations de sécurité liées à la phase 2.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Support de produit de concentrateurs VPN série 3000](#)
- [Support produit de Cisco VPN 3000 Client](#)
- [Support technique d'IPSec \(protocole de sécurité IP\)](#)
- [Support technique - Cisco Systems](#)