

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Dans cet exemple de configuration, un routeur est configuré pour la configuration du mode (obtenir une adresse IP du pool), des clés génériques pré-partagées (tous les clients PC partagent une clé commune), sans traduction d'adresses réseau (NAT). Un utilisateur hors site peut accéder au réseau et disposer d'une adresse IP interne attribuée à partir du pool. Les utilisateurs pensent qu'ils sont à l'intérieur du réseau. Les périphériques du réseau sont configurés avec des routes vers le pool 10.2.1.x non routable.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Components Used](#)

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

- Logiciel Cisco IOS® 12.0.7T ou ultérieur
- Matériel prenant en charge cette révision logicielle
- Client VPN CiscoSecure 1.0/1.0.A ou 1.1 (indiqué respectivement sur 2.0.7/E ou 2.1.12, accédez à **Aide > Sur le point** de vérifier)

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

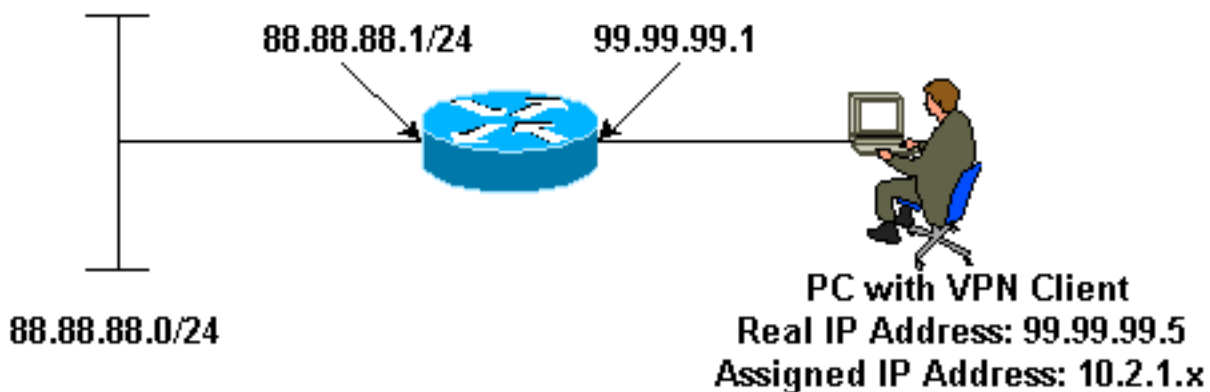
Configuration

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 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
```

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 engine connections active** : 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.

Ces débogages doivent être exécutés sur les deux routeurs IPSec (homologues). La suppression des associations de sécurité doit être effectuée sur les deux homologues.

- **debug crypto ipsec** : Cette commande affiche les négociations IPSec de la phase 2.
- **debug crypto isakmp** —Montre les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Montre le trafic crypté.
- **clear crypto isakmp** : efface les associations de sécurité liées à la phase 1.
- **clear crypto sa** - Efface les associations de sécurité liées à la phase 2.

Dépannage

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

Informations connexes

- [Prise en charge des concentrateurs de la gamme VPN 3000](#)

- [Assistance produit client Cisco VPN 3000](#)
- [Prise en charge de la technologie IPSec \(IP Security Protocol\)](#)
- [Support technique - Cisco Systems](#)