

Comment authentifier un client VPN 5000 sur le concentrateur VPN 5000 à l'aide de CiscoSecure NT version 2.5 et ultérieure (RADIUS)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration Cisco Secure du NT 2.5](#)

[Changer à l'authentification PAP](#)

[Modification du profil RADIUS VPN 5000](#)

[Ajouter l'affectation d'adresse IP](#)

[Ajout de la comptabilité](#)

[Vérifiez](#)

[Dépannez](#)

[Le serveur NT Cisco Secure est inaccessible](#)

[L'authentification échoue](#)

[Le mot de passe de groupe VPN entré par l'utilisateur n'est pas conforme à VPNPassword](#)

[Le nom de groupe envoyé vers le bas par le serveur de RAYON n'existe pas sur le VPN 5000](#)

[Informations connexes](#)

Introduction

Le NT Cisco Secure (CSNT) 2.5 et plus tard (RAYON) est capable de renvoyer le réseau privé virtuel (VPN) 5000 attributs de constructeur-particularité pour que le mot de passe VPN GroupInfo et VPN authentifia un client VPN 5000 au concentrateur VPN 5000. Le document suivant suppose que l'authentification locale fonctionne avant d'ajouter l'authentification de RAYON (par conséquent notre utilisateur, « localuser, » dans le groupe « ciscolocal »). Alors l'authentification est ajoutée au RAYON CSNT pour des utilisateurs n'existant pas dans la base de données locale (l'utilisateur « csntuser » est assigné pour grouper le « csntgroup » en vertu des attributs retournés du serveur de RAYON CSNT).

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 :

- NT Cisco Secure 2.5
- Concentrateur 5.2.16.0005 de Cisco VPN 5000
- Client VPN 5000 de Cisco 4.2.7

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](#).

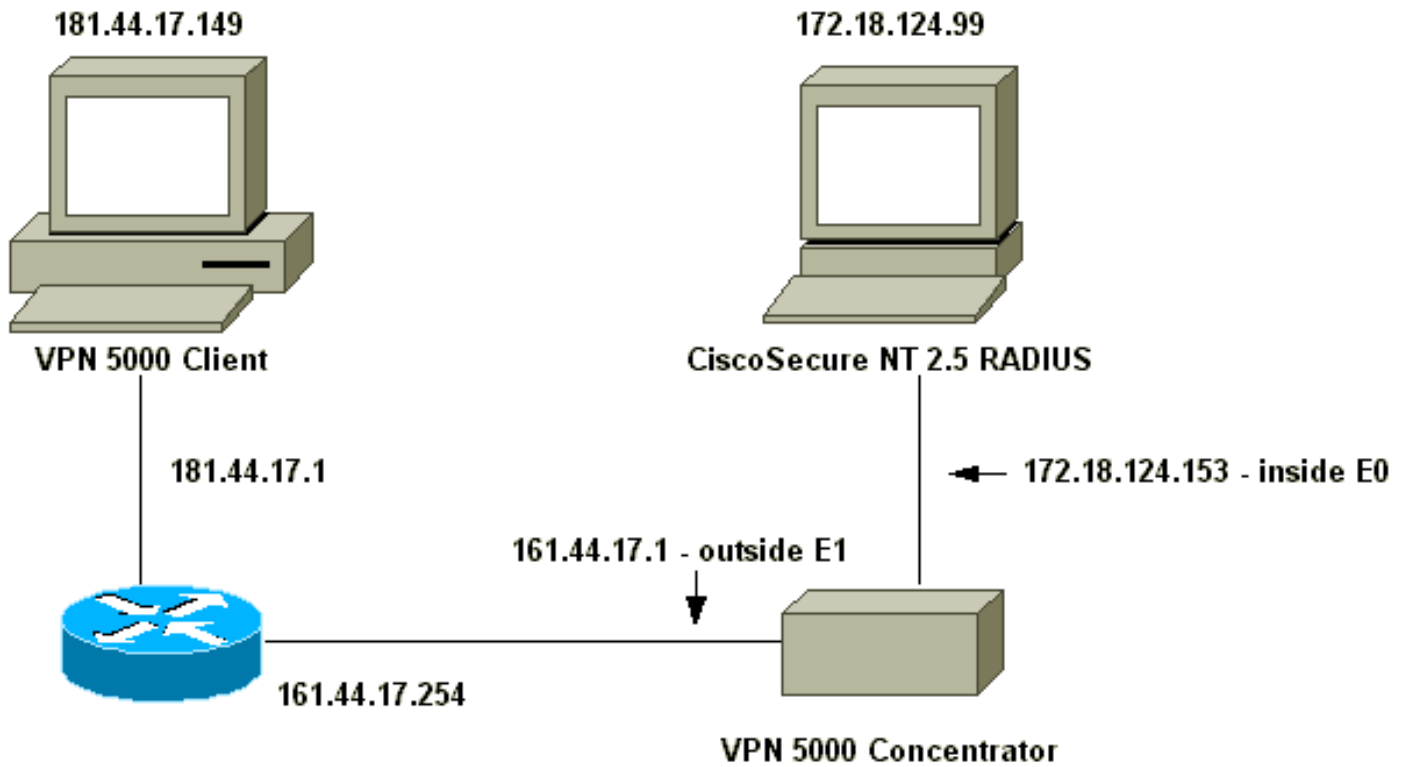
Configurez

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

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 suivante :



Configurations

Ce document utilise les configurations suivantes :

- [Concentrateur VPN 5000](#)
- [Client VPN 5000](#)

Concentrateur VPN 5000

```
[ IP Ethernet 0 ]
SubnetMask          = 255.255.255.0
Mode                = Routed
IPAddress           = 172.18.124.153

[ IP Ethernet 1 ]
Mode                = Routed
SubnetMask          = 255.255.255.0
IPAddress           = 161.44.17.1

[ VPN Group "ciscolocal" ]
IPNet               = 172.18.124.0/24
Transform            = esp(md5,des)
StartIPAddress      = 172.18.124.250
MaxConnections      = 4
BindTo              = "ethernet0"
[ General ]
EthernetAddress     = 00:00:a5:f0:c9:00
DeviceType          = VPN 5001 Concentrator
ConfiguredOn        = Timeserver not configured
ConfiguredFrom      = Command Line, from
172.18.124.99
IPSecGateway        = 161.44.17.254

[ Logging ]
Level               = 7
Enabled              = On
LogToAuxPort        = On
```

```

LogToSysLog           = On
SyslogIPAddress       = 172.18.124.114
SyslogFacility        = Local5

[ IKE Policy ]
Protection            = MD5_DES_G1

[ VPN Users ]
localuser Config="ciscocal" SharedKey="localike"

[ Radius ]
Accounting            = Off
PrimAddress           = "172.18.124.99"
Secret                = "csntkey"
ChallengeType         = CHAP
BindTo                = "ethernet0"
Authentication        = On

[ VPN Group "csnt" ]
BindTo                = "ethernet0"
Transform             = ESP(md5,Des)
MaxConnections        = 2
IPNet                 = 172.18.124.0/24
StartIPAddress        = 172.18.124.245

AssignIPRADIUS        = Off
BindTo                = "ethernet0"
StartIPAddress        = 172.18.124.243
IPNet                 = 172.18.124./24
StartIPAddress        = 172.18.124.242
Transform             = ESP(md5,Des)
BindTo                = "ethernet0"
MaxConnections        = 1

[ VPN Group "csntgroup" ]
MaxConnections        = 2
StartIPAddress        = 172.18.124.242
BindTo                = "ethernet0"
Transform             = ESP(md5,Des)
IPNet                 = 172.18.124.0/24

Configuration size is 2045 out of 65500 bytes.

```

Client VPN 5000

Note: None of the defaults have been changed. Two users were added, and the appropriate passwords were entered when prompted after clicking Connect: username password radius_password -----
localuser localike N/A csntuser grouppass csntpass

[Configuration Cisco Secure du NT 2.5](#)

Suivez cette procédure.

1. Configurez le serveur pour parler au concentrateur

Network Configuration

Access Server Setup For vpn5000

Network

Access Server

IP Address

Key

Authenticate
Using

- Single Connect TACACS+ NAS (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this Access Server
- Log Radius Tunnelling Packets from this Access Server

2. Allez à la **configuration d'interface** > au **RAYON (VPN 5000)** et vérifiez le mot de passe VPN

Group

- * [026/255/000]
CVPN5000-Compatible-Tunnel-Delay
- * [026/255/001]
CVPN5000-Tunnel-Throughput
- * [026/255/002]
CVPN5000-Client-Assigned-IP
- * [026/255/003]
CVPN5000-Client-Real-IP
- [026/255/004]
CVPN5000-VPN-GroupInfo
- [026/255/005]
CVPN5000-VPN-Password
- * [026/255/006] CVPN5000-Echo
- * [026/255/007]
CVPN5000-Client-Real-IP

Submit Cancel

GroupInfo et VPN :

3. Après avoir configuré l'utilisateur (« csntuser ») avec un mot de passe (« csntpass ») dans l'installation utilisateur et la mise de l'utilisateur dans le groupe 13, configurez les attributs VPN 5000 dans le **Group Setup | Groupe 13**

Group Setup

Access Restrictions | IP Address Assignment | IETF Radius

Cisco VPN5000 Radius

Cisco VPN 5000 Concentrator RADIUS Attributes

[255\004] CVPN5000-VPN-GroupInfo

[255\005] CVPN5000-VPN-Password

[Changer à l'authentification PAP](#)

Les travaux arrogants d'authentification de protocole d'authentification CHAP (Challenge Handshake Authentication Protocol), vous pouvez souhaiter changer en le Password Authentication Protocol (PAP), qui te permet d'avoir le mot de passe d'utilisateur CSNT l'utilisation de la base de données de NT.

[Modification du profil RADIUS VPN 5000](#)

```
[ Radius ]
PAPAuthSecret           = "abcxyz"
ChallengeType           = PAP
```

Remarque: CSNT serait également configuré pour utiliser la base de données de NT pour cette authentification d'utilisateur.

Ce que l'utilisateur voit (trois cadres Password) :

```
Shared Secret = grouppass
RADIUS Login box - Password = csntpass
```

RADIUS Login box - Authentication Secret = abcxyz

Ajouter l'affectation d'adresse IP

Si le profil CSNT de l'utilisateur est placé dans « assignez l'adresse IP statique » à une valeur particulière, et si le groupe du concentrateur VPN 5000 est placé pour :

```
AssignIPRADIUS = On
```

Puis, l'adresse IP de RAYON est envoyée vers le bas de CSNT et appliquée à l'utilisateur sur le concentrateur VPN 5000.

Ajout de la comptabilité

Si vous voulez des enregistrements des comptes de session envoyés au serveur Cisco Secure de RAYON, alors ajoutez à la configuration RADIUS du concentrateur VPN 5000 :

```
[ Radius ]
Accounting = On
```

Vous devez utiliser l'**application** et les touches d'écriture, et puis la commande de **démarrage** sur le VPN 5000 pour que cette modification la prenne effet.

Enregistrements des comptes de CSNT

```
11/06/2000,16:02:45,csntuser,Group 13,,Start,077745c5-00000000,,,,,,,,,
268435456,172.18.124.153
11/06/2000,16:03:05,csntuser,Group 13,,Stop,077745c5-00000000,20,,,
104,0,1,0,,268435456,172.18.124.153
```

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.

- **mémoire tampon de log de show system**

```
Info 7701.12 seconds Command loop started from
172.18.124.99
on PTY1

Notice 7723.36 seconds New IKE connection: [181.44.17.149]:1041:csntuser
Debug 7723.38 seconds Sending RADIUS CHAP challenge to
csntuser at 181.44.17.149
Debug 7729.0 seconds Received RADIUS challenge resp. from
csntuser at 181.44.17.149, contacting server
Notice 7729.24 seconds VPN 0 opened for csntuser from 181.44.17.149.
Debug 7729.26 seconds Client's local broadcast address = 181.44.17.255
Notice 7729.29 seconds User assigned IP address 172.18.124.242
```
- **vidage mémoire tout de suivi de vpn**

```
VPN5001_A5F0C900# vpn trace dump all
6 seconds -- stepmngtr trace enabled --
new script: ISAKMP primary responder script for <no id> (start)
manage @ 91 seconds :: [181.44.17.149]:1042 (start)
91 seconds doing irpri_new_conn, (0 @ 0)
91 seconds doing irpri_pkt_1_recd, (0 @ 0)
new script: ISAKMP Resp Aggr Shared Secret script for
[181.44.17.149]:1042 (start)
```



```

    91 seconds doing irsass_process_pkt_1, (0 @ 0)
    91 seconds doing irsass_build_rad_pkt, (0 @ 0)
    91 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 91 seconds :: [181.44.17.149]:1042 (done)
manage @ 93 seconds :: [181.44.17.149]:1042:csntuser (start)
    93 seconds doing irsass_radius_wait, (0 @ 0)
    93 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 93 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
    95 seconds doing irsass_radius_wait, (0 @ 0)
    95 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
    95 seconds doing irsass_radius_wait, (0 @ 0)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
    95 seconds doing irsass_rad_serv_wait, (0 @ 0)
    95 seconds doing irsass_build_pkt_2, (0 @ 0)
    96 seconds doing irsass_send_pkt_2, (0 @ 0)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (start)
    96 seconds doing irsass_check_timeout, (0 @ 0)
    96 seconds doing irsass_check_hash, (0 @ 0)
    96 seconds doing irsass_last_op, (0 @ 0)
end script: ISAKMP Resp Aggr Shared Secret script for
[181.44.17.149]:1042:csntuser, (0 @ 0)
next script: ISAKMP primary responder script for
[181.44.17.149]:1042:csntuser, (0 @ 0)
    96 seconds doing irpri_phase1_done, (0 @ 0)
    96 seconds doing irpri_phase1_done, (0 @ 0)
    96 seconds doing irpri_start_phase2, (0 @ 0)
new script: phase 2 initiator for [181.44.17.149]:1042:csntuser (start)
    96 seconds doing iph2_init, (0 @ 0)
    96 seconds doing iph2_build_pkt_1, (0 @ 0)
    96 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (start)
    96 seconds doing iph2_pkt_2_wait, (0 @ 0)
    96 seconds doing ihp2_process_pkt_2, (0 @ 0)
    96 seconds doing iph2_build_pkt_3, (0 @ 0)
    96 seconds doing iph2_config_SAs, (0 @ 0)
    96 seconds doing iph2_send_pkt_3, (0 @ 0)
    96 seconds doing iph2_last_op, (0 @ 0)
end script: phase 2 initiator for [181.44.17.149]:1042:csntuser, (0 @ 0)
next script: ISAKMP primary responder script for
[181.44.17.149]:1042:csntuser, (0 @ 0)
    96 seconds doing irpri_open_tunnel, (0 @ 0)
    96 seconds doing irpri_start_i_maint, (0 @ 0)
new script: initiator maintenance for [181.44.17.149]:1042:csntuser (start)
    96 seconds doing imnt_init, (0 @ 0)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
<vpn trace dump done, 55 records scanned>

```

[Dépannez](#)

Ce qui suit sont des erreurs possibles que vous pouvez rencontrer.

[Le serveur NT Cisco Secure est inaccessible](#)

Debug VPN 5000

```
Notice 359.36 seconds New IKE connection: [181.44.17.149]:1044:csntuser
Debug 359.38 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 363.18 seconds Received RADIUS challenge resp. From
    csntuser at 181.44.17.149, contacting server
Notice 423.54 seconds <no ifp> (csntuser) reset: RADIUS server never responded.
```

Ce que l'utilisateur voit :

```
VPN Server Error (14) User Access Denied
```

[L'authentification échoue](#)

Le nom d'utilisateur ou mot de passe sur le NT Cisco Secure est mauvais.

Debug VPN 5000

```
Notice 506.42 seconds New IKE connection: [181.44.17.149]:1045:csntuser
Debug 506.44 seconds Sending RADIUS CHAP challenge to csntuser
    at 181.44.17.149
Debug 511.24 seconds Received RADIUS challenge resp. From csntuser
    at 181.44.17.149, contacting server
Debug 511.28 seconds Auth request for csntuser rejected by RADIUS server
Notice 511.31 seconds <no ifp> (csntuser) reset due to RADIUS authentication
failure.
```

Ce que l'utilisateur voit :

```
VPN Server Error (14) User Access Denied
```

Cisco Secure :

Allez aux **états** et à **l'activité**, et les essais ratés se connectent des expositions la panne.

[Le mot de passe de groupe VPN entré par l'utilisateur n'est pas conforme à VPNPassword](#)

Debug VPN 5000

```
Notice 545.0 seconds New IKE connection: [181.44.17.149]:1046:csntuser
Debug 545.6 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 550.6 seconds Received RADIUS challenge resp. From csntuser at 181.44.17.149,
contacting server
```

Ce que l'utilisateur voit :

```
IKE ERROR: Authentication Failed.
```

Cisco Secure :

Allez aux **états** et à **l'activité**, et le log d'essais ratés n'affiche pas la panne.

[Le nom de groupe envoyé vers le bas par le serveur de RAYON n'existe pas sur le VPN 5000](#)

Debug VPN 5000

```
Notice 656.18 seconds New IKE connection: [181.44.17.149]:1047:csntuser
Debug 656.24 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 660.12 seconds Received RADIUS challenge resp. From csntuser at 181.44.17.149,
contacting server
Warnin 660.16 seconds User, "csntuser", has an invalid VPN Group config, "junkgroup"
```

Notice 660.20 seconds (csntuser) reset: connection script finished.
Notice 660.23 seconds -- reason: S_NO_POLICY (220@772)

Ce que l'utilisateur voit :

VPN Server Error (6): Bad user configuration on IntraPort server.

Cisco Secure :

Allez aux **états** et à l'**activité**, et le log d'essais ratés n'affiche pas la panne.

Informations connexes

- [Cisco Secure ACS pour la page d'assistance de Windows](#)
- [Annonce de fin de ventes de Concentrateur VPN de la gamme Cisco 5000](#)
- [Page d'assistance du concentrateur VPN Cisco 5000](#)
- [Page d'assistance du client VPN 5000 de Cisco](#)
- [Page d'assistance IPsec](#)
- [Page d'assistance RADIUS](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)