

Como autenticar o VPN 5000 Client para o VPN 5000 Concentrator com o CiscoSecure NT 2.5 e posterior (RADIUS)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração do Cisco Secure NT 2.5](#)

[Alterando para a autenticação PAP](#)

[Alteração de perfil do VPN 5000 RADIUS](#)

[Adicionando atribuição de endereço IP](#)

[Relatório de adição](#)

[Verificar](#)

[Troubleshoot](#)

[O Cisco Secure NT Server não pode ser alcançado](#)

[Falhas de autenticação](#)

[A senha do grupo VPN digitada pelo usuário não coincide com a senha de VPN](#)

[O nome do grupo enviado pelo servidor RADIUS não existe no VPN 5000](#)

[Informações Relacionadas](#)

Introduction

O Cisco Secure NT (CSNT) 2.5 e posterior (RADIUS) é capaz de retornar atributos específicos de fornecedor da Virtual Private Network (VPN) 5000 para VPN GroupInfo e senha de VPN para autenticar um VPN 5000 Client para o VPN 5000 Concentrator. O documento a seguir pressupõe que a autenticação local está funcionando antes de adicionar a autenticação RADIUS (portanto, nosso usuário, "localuser", no grupo "ciscocal"). Em seguida, a autenticação é adicionada ao CSNT RADIUS para usuários não existentes no banco de dados local (o usuário "csntuser" é atribuído ao grupo "csntgroup" em virtude dos atributos retornados do servidor CSNT RADIUS).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure NT 2.5
- Concentrador Cisco VPN 5000 5.2.16.0005
- Cisco VPN 5000 Client 4.2.7

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](#).

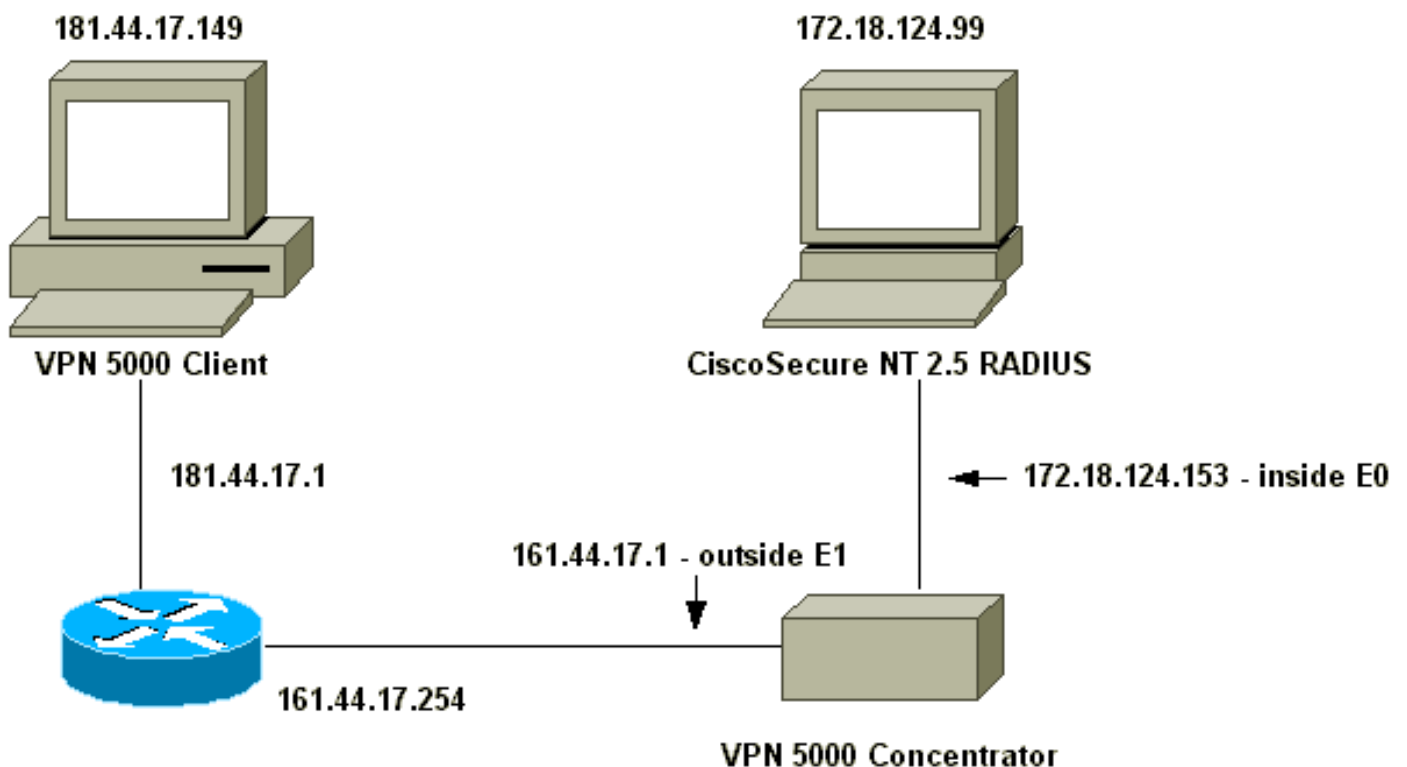
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a [ferramenta Command Lookup Tool](#) (somente clientes [registrados](#)).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- [VPN 5000 Concentrator](#)
- [Cliente VPN 5000](#)

VPN 5000 Concentrator	
[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="ciscolocal" 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.

```

Cliente 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

[Configuração do Cisco Secure NT 2.5](#)

Siga este procedimento.

1. Configure o servidor para falar com o

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

concentrador:

2. Vá para **Interface Configuration > RADIUS (VPN 5000)** e verifique VPN GroupInfo e 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]

Submit Cancel

Password:

3. Depois de configurar o usuário ("csntuser") com uma senha ("csntpass") na Configuração do usuário e colocar o usuário no Grupo 13, configure os atributos do VPN 5000 na **Configuração do grupo | Grupo**

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

13:

[Alterando para a autenticação PAP](#)

Supondo que a autenticação CHAP (Challenge Handshake Authentication Protocol Protocolo de Autenticação de Handshake de Desafio) funcione, você pode desejar alterar para PAP (Password Authentication Protocol Protocolo de Autenticação de Senha), que permite que você faça com que o CSNT use a senha do usuário do banco de dados NT.

[Alteração de perfil do VPN 5000 RADIUS](#)

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

Observação: o CSNT também seria configurado para usar o banco de dados NT para a autenticação desse usuário.

O que o usuário vê (três caixas de senha):

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

Adicionando atribuição de endereço IP

Se o perfil CSNT do usuário estiver definido em "Atribuir endereço IP estático" a um valor específico e se o grupo do VPN 5000 Concentrator estiver definido para:

```
AssignIPRADIUS = On
```

Em seguida, o endereço IP RADIUS é enviado de CSNT e aplicado ao usuário no VPN 5000 Concentrator.

Relatório de adição

Se você deseja que os registros de contabilidade de sessão sejam enviados para o servidor Cisco Secure RADIUS, adicione à configuração RADIUS do VPN 5000 Concentrator:

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

Você deve usar os comandos **apply** e **write** e, em seguida, o comando **boot** no VPN 5000 para que essa alteração entre em vigor.

Registros Contábeis Do 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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.](#)

- **show system log buffer**

```
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
```

- **vpn trace dump all**

```
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_rcvd, (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>

```

[Troubleshoot](#)

A seguir estão possíveis erros que você pode encontrar.

O Cisco Secure NT Server não pode ser alcançado

Debug de 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.
```

O que o usuário vê:

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

Falhas de autenticação

O nome de usuário ou a senha no Cisco Secure NT estão incorretos.

Debug de 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.
```

O que o usuário vê:

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

Cisco Secure:

Vá para **Relatórios e Atividade**, e o registro de tentativas com falha mostra a falha.

A senha do grupo VPN digitada pelo usuário não coincide com a senha de VPN

Debug de 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
```

O que o usuário vê:

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

Cisco Secure:

Vá para **Relatórios e Atividade**, e o registro de tentativas com falha não mostra a falha.

[O nome do grupo enviado pelo servidor RADIUS não existe no VPN 5000](#)

Debug de 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)
```

O que o usuário vê:

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

Cisco Secure:

Vá para **Relatórios e Atividade**, e o registro de tentativas com falha *não* mostra a falha.

[Informações Relacionadas](#)

- [Cisco Secure ACS para página de suporte do Windows](#)
- [Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series](#)
- [Página de suporte do Cisco VPN 5000 Concentrator](#)
- [Página de suporte do Cisco VPN 5000 Client](#)
- [Página de suporte do IPsec](#)
- [Página de suporte RADIUS](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)