CiscoSecure NT 2.5 以降（RADIUS）を使用して VPN 5000 Client から VPN 5000 コンセントレータへの認証を行う方法

内容

概要

Cisco Secure NT(CSNT)2.5以降(RADIUS)では、VPN 5000クライアントをVPN 5000コンセントレータに認証するために、VPN GroupInfoおよびVPN PasswordのVirtual Private Network(VPN)5000ベンダー固有属性をに戻できます。次のドキュメントでは、RADIUS認証を追加する前にローカル認証が機能していることを前提としています（したがって、グループ「ciscolocal」のユーザ「localuser」）。 次に、ローカルデータベースに存在しないユーザの認証がCSNT RADIUSに追加されます（ユーザ「csntuser」は、CSNT RADIUSサーバから返される属性によってグループ「csntgroup」に割り当てられます）。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure NT 2.5
- Cisco VPN 5000コンセントレータ5.2.16.0005
- Cisco VPN 5000 Client 4.2.7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

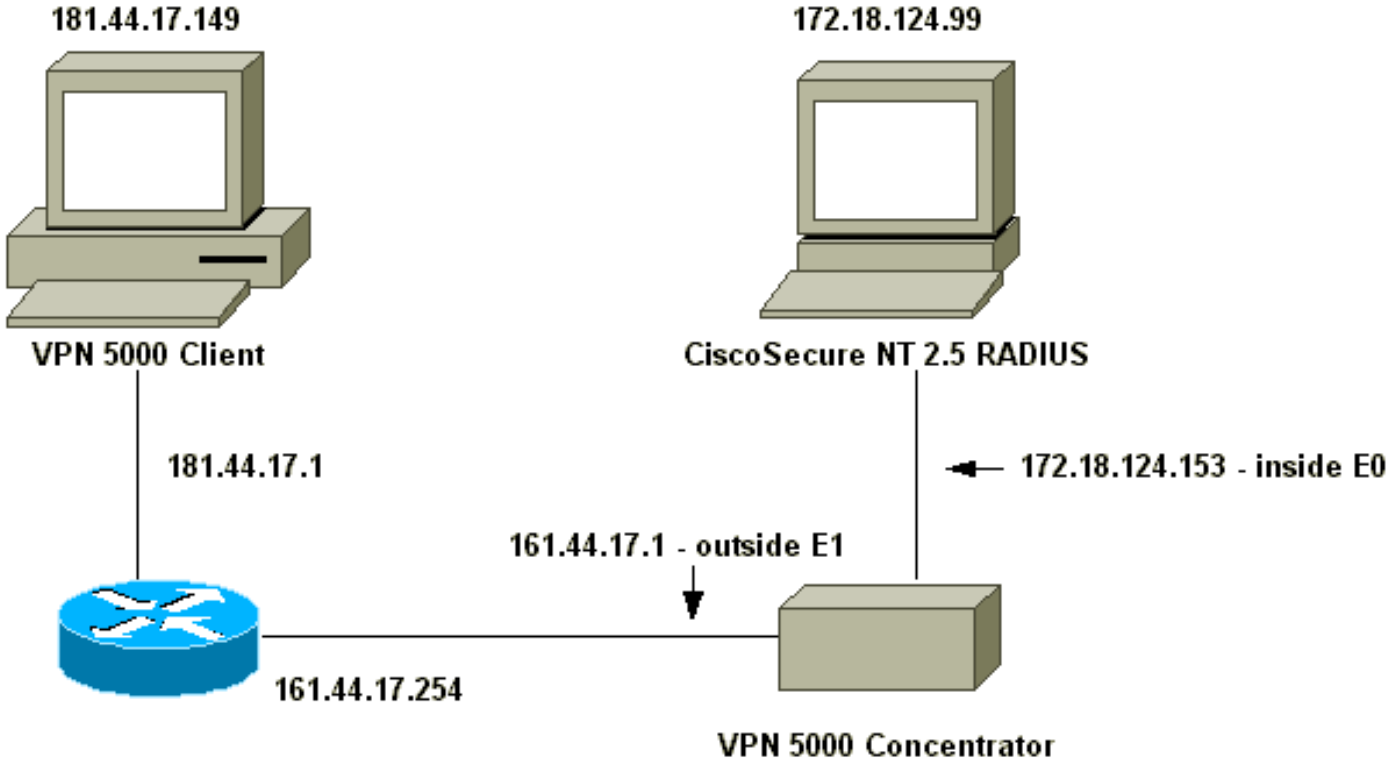
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- VPN 5000 コンセントレータ
- VPN 5000クライアント

VPN 5000 コンセントレータ

```
[ 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.
```

VPN 5000クライアント

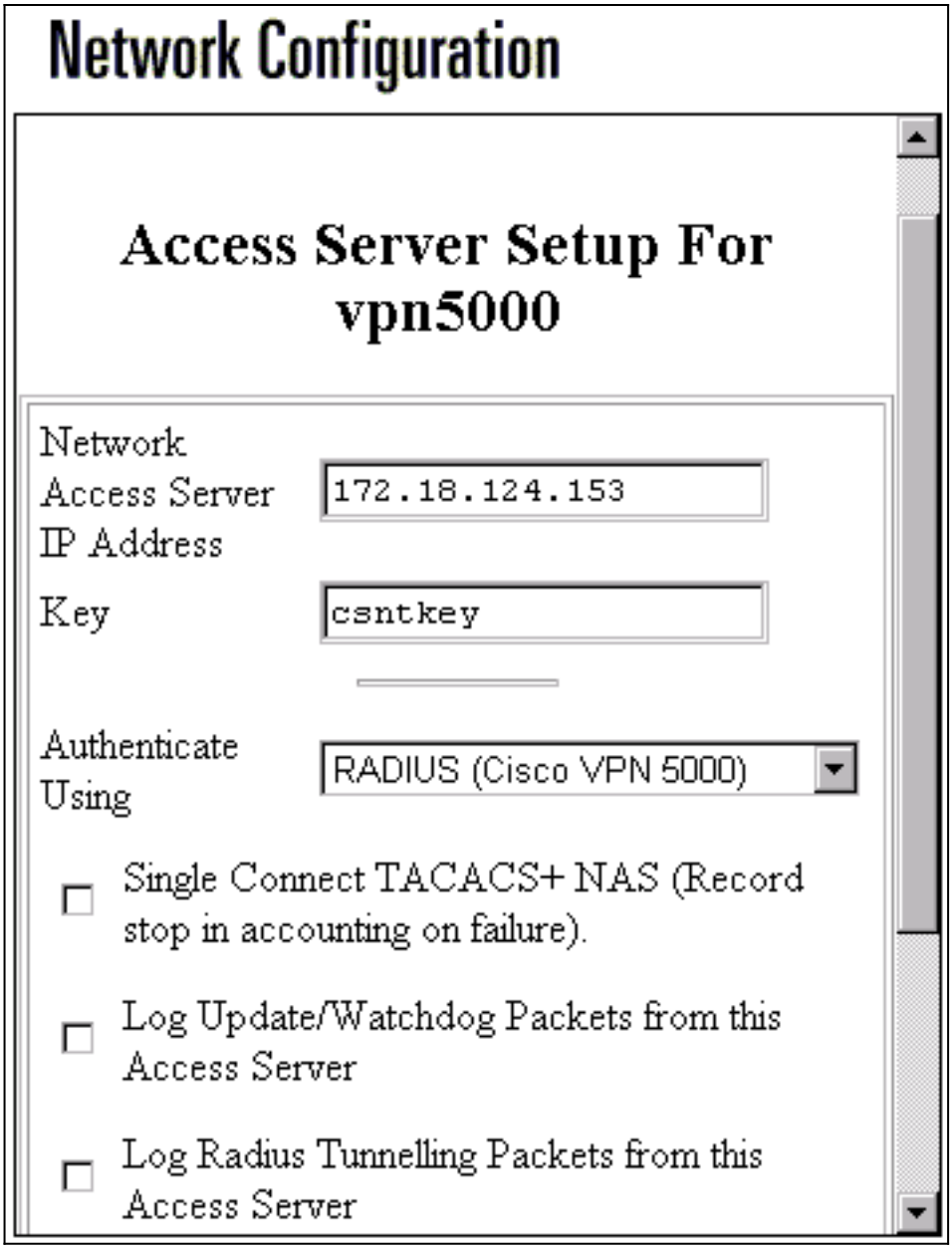
Note: None of the defaults have been changed. Two users were added, and
the appropriate passwords were entered when prompted after clicking Connect:

username	password	radius_password
localuser	localike	N/A
csntuser	grouppass	csntpass

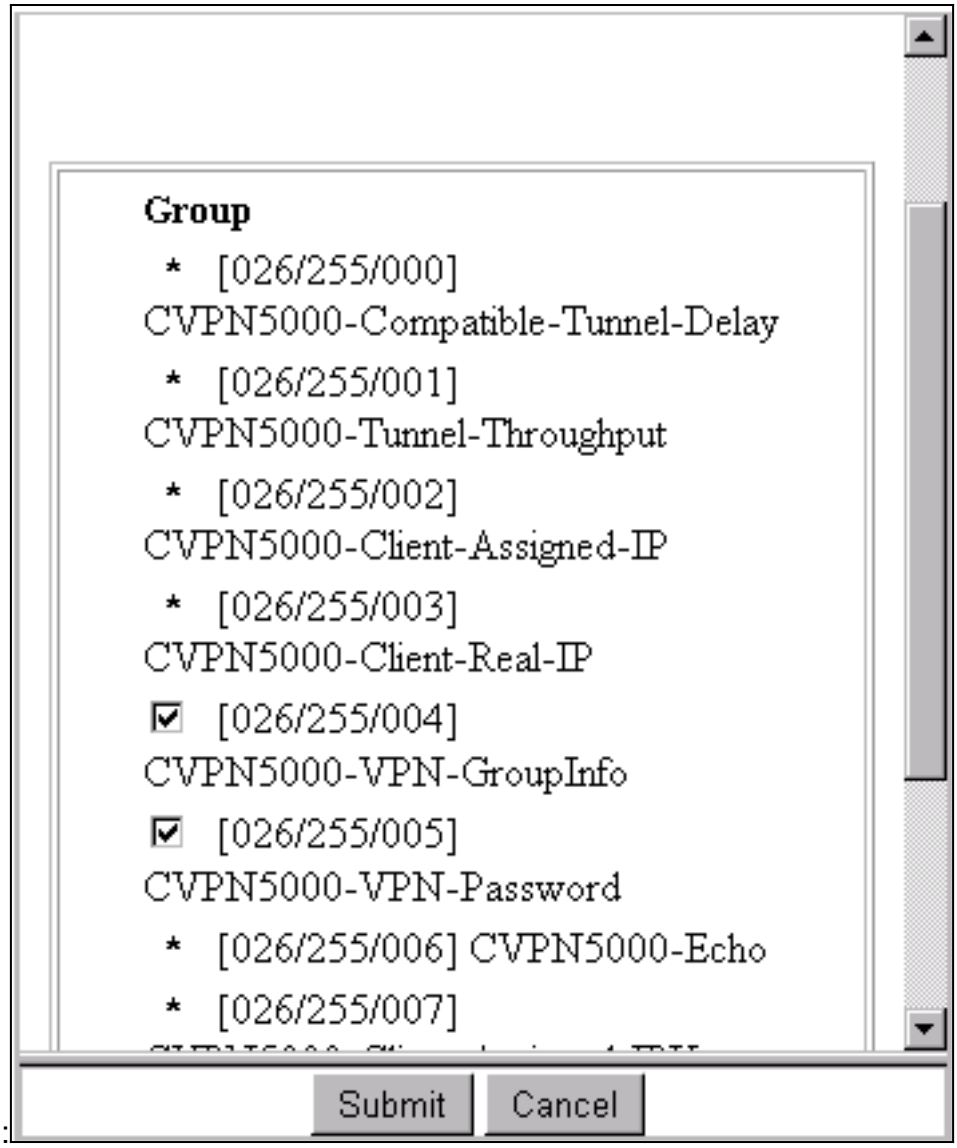
Cisco Secure NT 2.5の設定

次の手順に従います。

1. コンセントレータと通信するようにサーバを設定します。

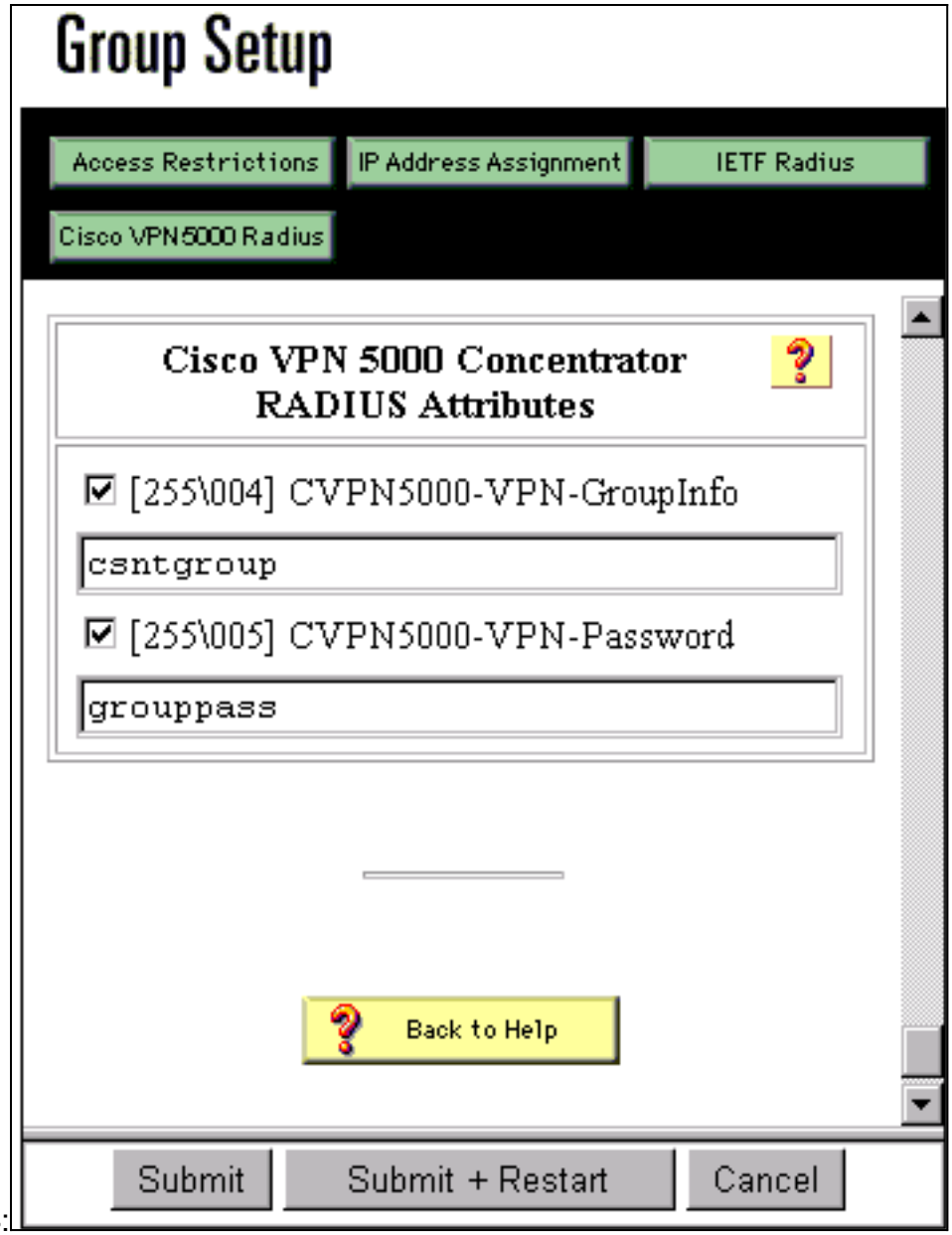


2. [Interface Configuration] > [RADIUS (VPN 5000)] に移動し、[VPN GroupInfo]と[VPN



Password:

3. ユーザ設定でパスワード(「csntpass」)を使用してユーザ(「csntuser」)を設定し、ユーザをグループ13に配置した後、グループセットアップでVPN 5000属性を設定**します |グループ**

13: 

PAP認証の変更

Challenge Handshake Authentication Protocol(CHAP)認証が機能する場合は、Password Authentication Protocol(PAP)に変更する必要があります。これにより、CSNTでNTデータベースからユーザのパスワードを使用できます。

VPN 5000 RADIUSのプロファイル変更

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

注：CSNTは、そのユーザの認証にNTデータベースを使用するように設定されます。

ユーザに表示される内容（3つのパスワードボックス）：

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

```
RADIUS Login box - Authentication Secret = abcxyz
```

IP アドレス割り当ての追加

ユーザのCSNTプロファイルが[Assign static IP Address]で特定の値に設定されている場合、およびVPN 5000コンセントレータグループが次のように設定されている場合。

```
AssignIPRADIUS = On
```

次に、RADIUS IPアドレスがCSNTから送信され、VPN 5000コンセントレータのユーザに適用されます。

アカウンティングの追加

セッションアカウンティングレコードをCisco Secure RADIUSサーバに送信する場合は、VPN 5000コンセントレータのRADIUS設定に追加します。

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

この変更を有効にするには、**apply**コマンドと**write**コマンドを使用してから、**boot**コマンドをVPN 5000で使用する必要があります。

CSNTからのアカウンティングレコード

```
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
```

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **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 -- stepmngr 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>
```

トラブルシュート

発生する可能性のあるエラーは次のとおりです。

Cisco Secure NT サーバが到達不能である場合

VPN 5000 のデバッグ

```
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.
```

ユーザに対する表示:

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

認証失敗

Cisco Secure NTのユーザ名またはパスワードが正しくありません。

VPN 5000 のデバッグ

```
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.
```

ユーザに対する表示:

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

Cisco Secure:

[Reports] と[Activity] に移動し、失敗した試行ログに失敗が表示されます。

ユーザが入力したVPNグループパスワードがVPNPassword と一致しない場合

VPN 5000 のデバッグ

```
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
```

ユーザに対する表示:

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

Cisco Secure:

[Reports] と[Activity] に移動します。失敗した試行ログに失敗が表示されません。

RADIUSサーバによって送信されるグループ名がVPN 5000 にない場合

VPN 5000 のデバッグ

```
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)
```

ユーザに対する表示:

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

Cisco Secure:

[Reports]と[Activity]に移動し、失敗した試行ログに失敗が表示されません。

関連情報

- Cisco Secure ACS for Windows に関するサポート ページ
- Cisco VPN 5000 シリーズ コンセントレータの販売終了のお知らせ
- Cisco VPN 5000 コンセントレータに関するサポートページ
- Cisco VPN 5000 クライアントに関するサポート ページ
- IPSec サポート ページ
- RADIUS に関するサポート ページ
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems