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

目次

概要
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
設定
Cisco Secure NT 2.5の設定
PAP認証の変更
VPN 5000 RADIUSのプロファイル変更
IP アドレス割り当ての追加
アカウンティングの追加
確認
トラブルシューティング
Cisco Secure NT サーバが到達不能である場合
認証失敗
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
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
関連情報

概要

Cisco Secure NT （CSNT） 2.5 および それ以降（RADIUS）は VPN 5000 コンセントレータに VPN 5000 Client を認証するためにバーチャル プライベート ネットワーク （VPN）を戻すことができます VPN GroupInfo および VPN パスワードのための 5000 の vendor-specific属性。 次に挙げるドキュメントはローカル認証が RADIUS認証（それ故に」ciscolocal グループ「のユーザ、「localuser」、追加する）をことを前にはたらいていると仮定します。 それから認証はローカル データベースで存在 して いない ユーザ向けの CSNT RADIUS に追加されます（CSNT RADIUSサーバから戻る属性によって「csntgroup」をグループ化するためにユーザ「csntuser」は割り当てられます）。

前提条件

要件

このドキュメントに関する固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くものです。

- 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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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。

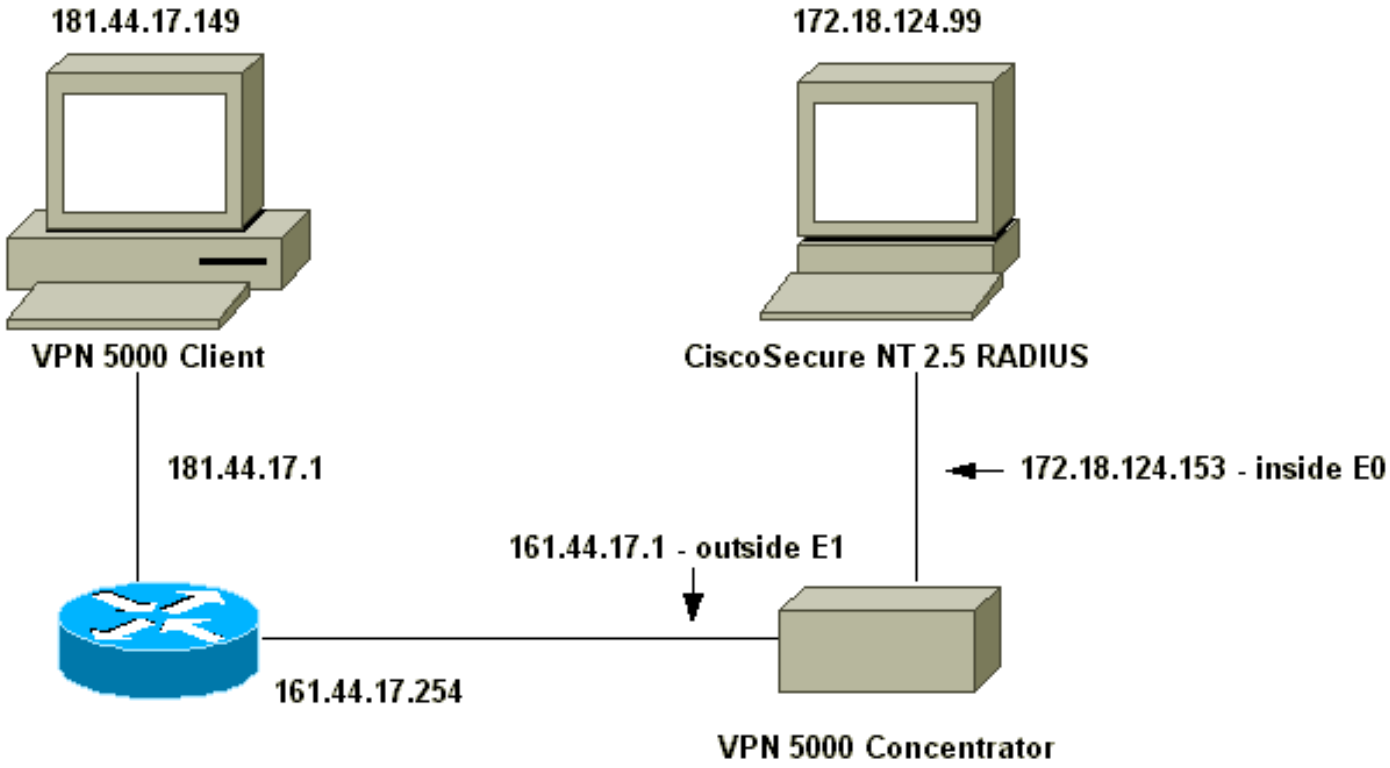
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- VPN 5000 コンセントレータ
- VPN 5000 Client

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.
```

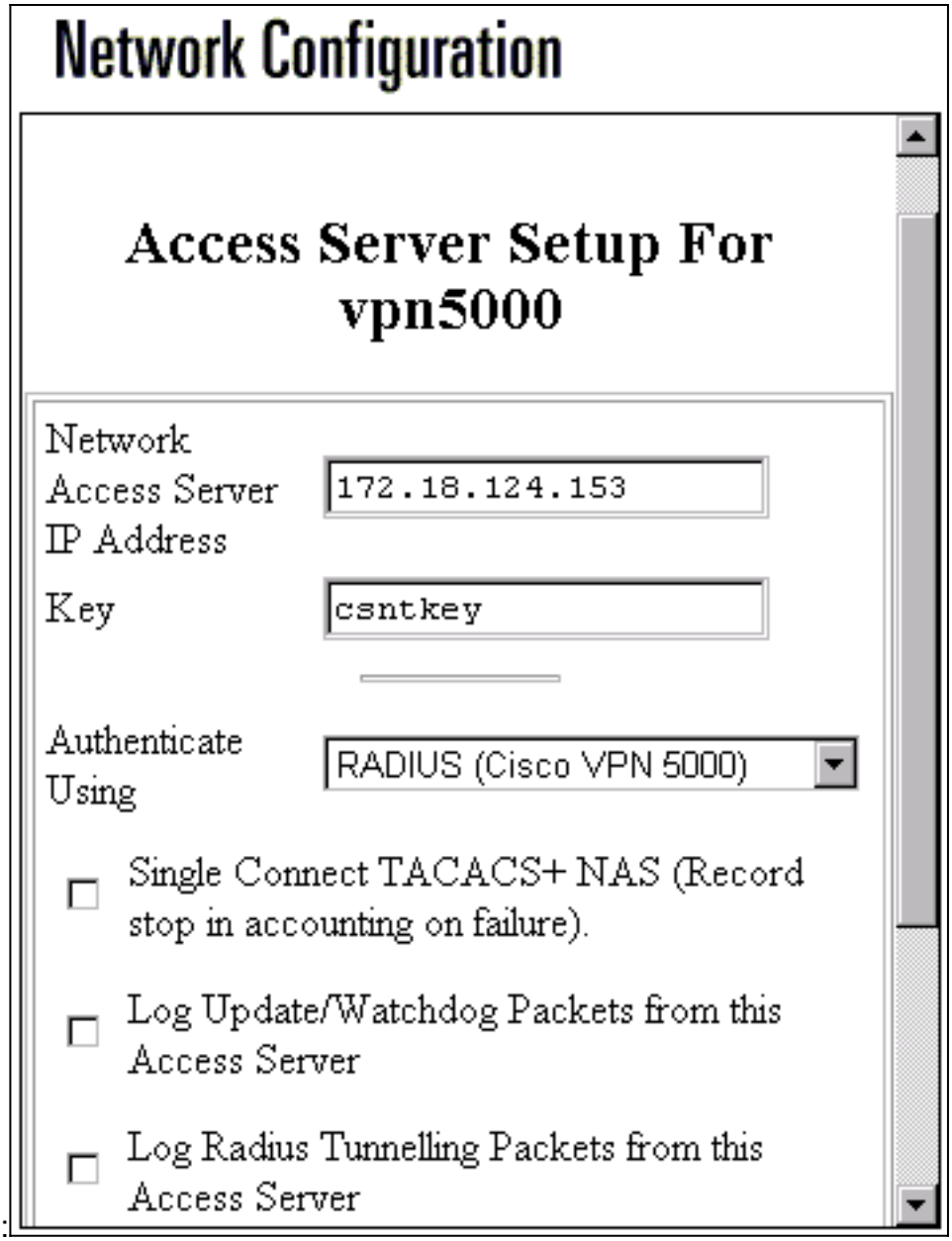
VPN 5000 Client

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

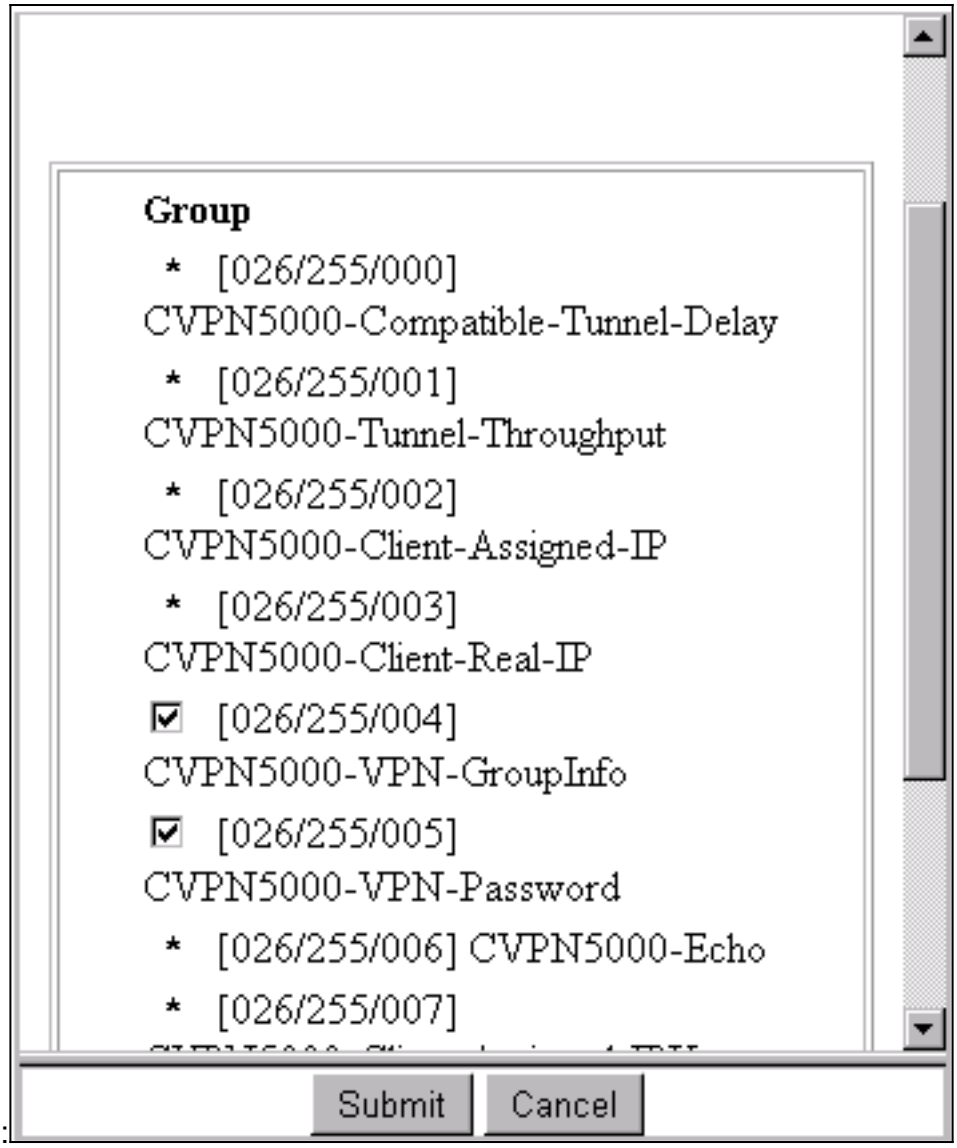
次の手順に従います。

1. コンセントレータに話すためにサーバを設定して下さい



:

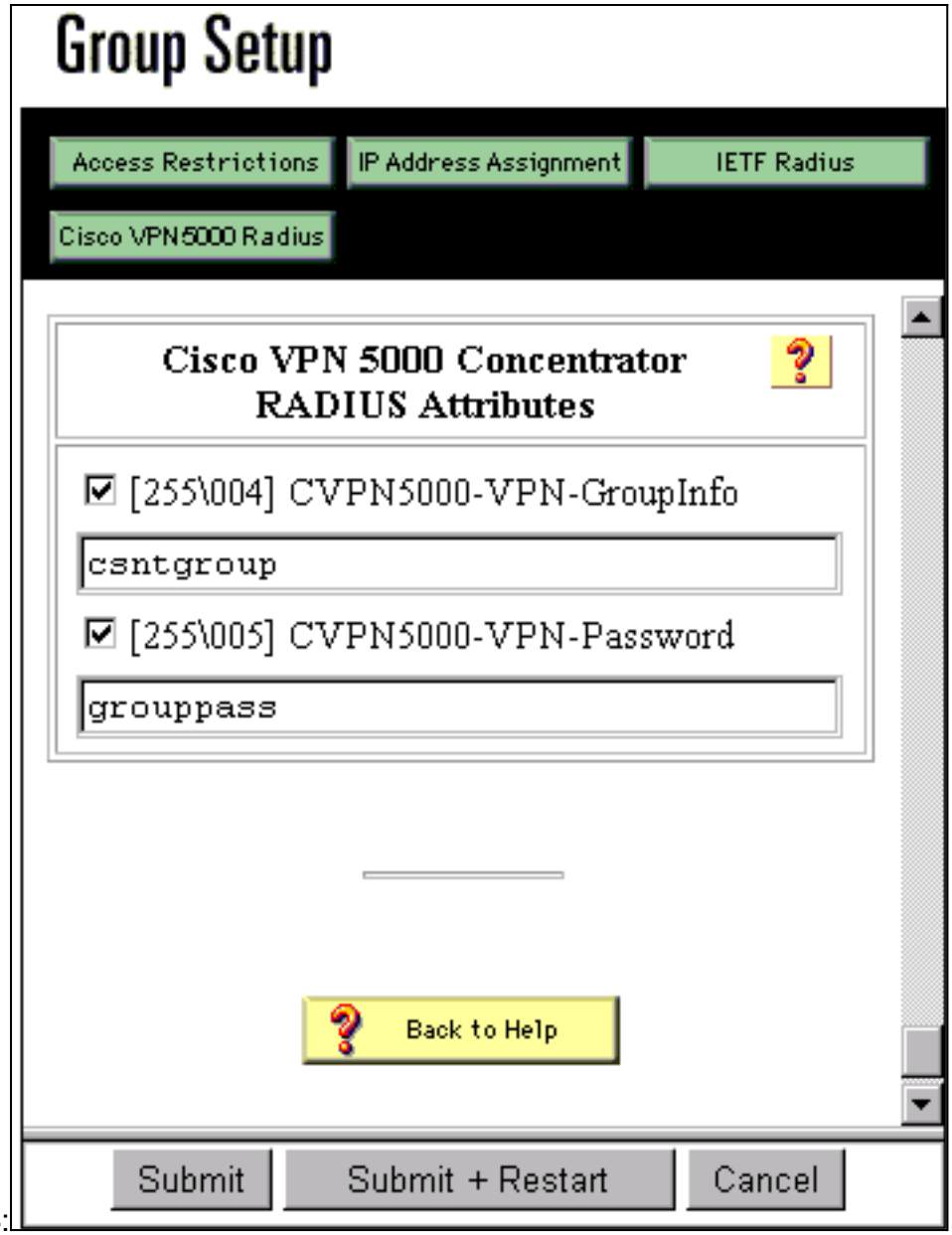
2. **インターフェイスコンフィギュレーション > RADIUS（VPN 5000）**に行き、VPN GroupInfo および VPN パスワードを確認して下さい



:

3. ユーザ (「csntuser」) をユーザセットアップのパスワード (「csntpass」) で設定し、グループ 13 のユーザを置いた後、**グループセットアップ**の VPN 5000 属性を設定して下さい

| グループ 13:



PAP認証の変更

Challenge Handshake Authentication Protocol（CHAP）認証作業を仮定して、CSNT 使用があることを NT データベースからのユーザ パスワード可能にする Password Authentication Protocol（PAP）に変更したい場合もあります。

VPN 5000 RADIUSのプロファイル変更

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

注: CSNT はまたそのユーザ認証のために NT データベースを使用するために設定されます。

ユーザが見る何を（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 プロファイルがで「設定 されたら VPN 5000 コンセントレータ グループがのために設定 される場合特定 の 値に静的IP アドレス」を、そして割り当てて下さい:

```
AssignIPRADIUS = On
```

それから、RADIUS IP アドレスは 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

Cisco Secure RADIUSサーバに送られるセッション アカウンティング レコードがほしいと思う場合 VPN 5000 コンセントレータ RADIUSコンフィギュレーションに追加して下さい:

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

次にこの変更に実施される VPN 5000 の **apply および write コマンド**および **boot コマンドを**使用して下さい。

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

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **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>
```

トラブルシューティング

以下は出会う可能性がある可能性のある エラーです。

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.
```

ユーザが見る何を:

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

認証失敗

ユーザ名かパスワード on Cisco セキュア NT は悪いです。

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.
```

ユーザが見る何を:

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

Cisco Secure:

レポートおよび**アクティビティ**に行けば、試行失敗 ログは失敗を示します。

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
```

ユーザが見る何を:

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

Cisco Secure:

レポートおよび**アクティビティ**に行けば、試行失敗 ログは失敗を示しません。

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)
```

ユーザが見る何を:

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

Cisco Secure:

レポートおよび**アクティビティ**に行けば、試行失敗 ログは失敗を示しません。

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発表
- 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 に関するサポート ページ
- RADIUS に関するサポート ページ
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems