認証プロキシの実装

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[認証プロキシの実装方法](#)
[サーバのプロファイル](#)
[Cisco Secure UNIX(TACACS+)](#)
[Cisco Secure Windows(TACACS+)](#)
[ユーザに対する表示](#)
[関連情報](#)

概要

認証プロキシ（auth-proxy）は、Cisco IOS(R)ソフトウェア ファイアウォール バージョン 12.0.5.T 以降で使用可能であり、発信ユーザまたは着信ユーザ、およびその両方の認証に使用されます。これらのユーザは通常はアクセス リストによってブロックされます。ただし、認証プロキシを使用すると、ユーザはブラウザを起動してファイアウォールを通過し、TACACS+ または RADIUS サーバで認証を受けることができます。このサーバはアクセス リストの追加エントリをルータに渡し、認証後にユーザの通過を許可します。

このドキュメントでは、auth-proxyの実装に関するユーザの一般的なヒントを示し、認証プロキシに関するいくつかのCisco Secureサーバプロファイルを提供し、認証プロキシが使用されている場合のユーザの表示について説明します。

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内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

認証プロキシの実装方法

次のステップを実行します。

1. auth-proxyを設定する前に、トラフィックがファイアウォールを正しく通過することを確認してください。
2. テスト中のネットワークの中断を最小限にするため、既存のアクセス リストを変更して、テスト用のクライアントに対するアクセスを拒否します。
3. テスト用のクライアントがファイアウォールを通過できず、他のホストは通過できることを確認します。
4. コンソールポートまたは仮想タイプ端末(VTY)で**exec-timeout 0 0を使用してデバッグをオン**にし、**auth-proxyコマンドを追加してテスト**します。

サーバのプロファイル

シスコのテストは、Cisco Secure UNIXおよびWindowsで行われました。RADIUS が使用されている場合、RADIUS サーバでベンダー固有の属性（属性 26）がサポートされている必要があります。 具体的な例を次に示します。

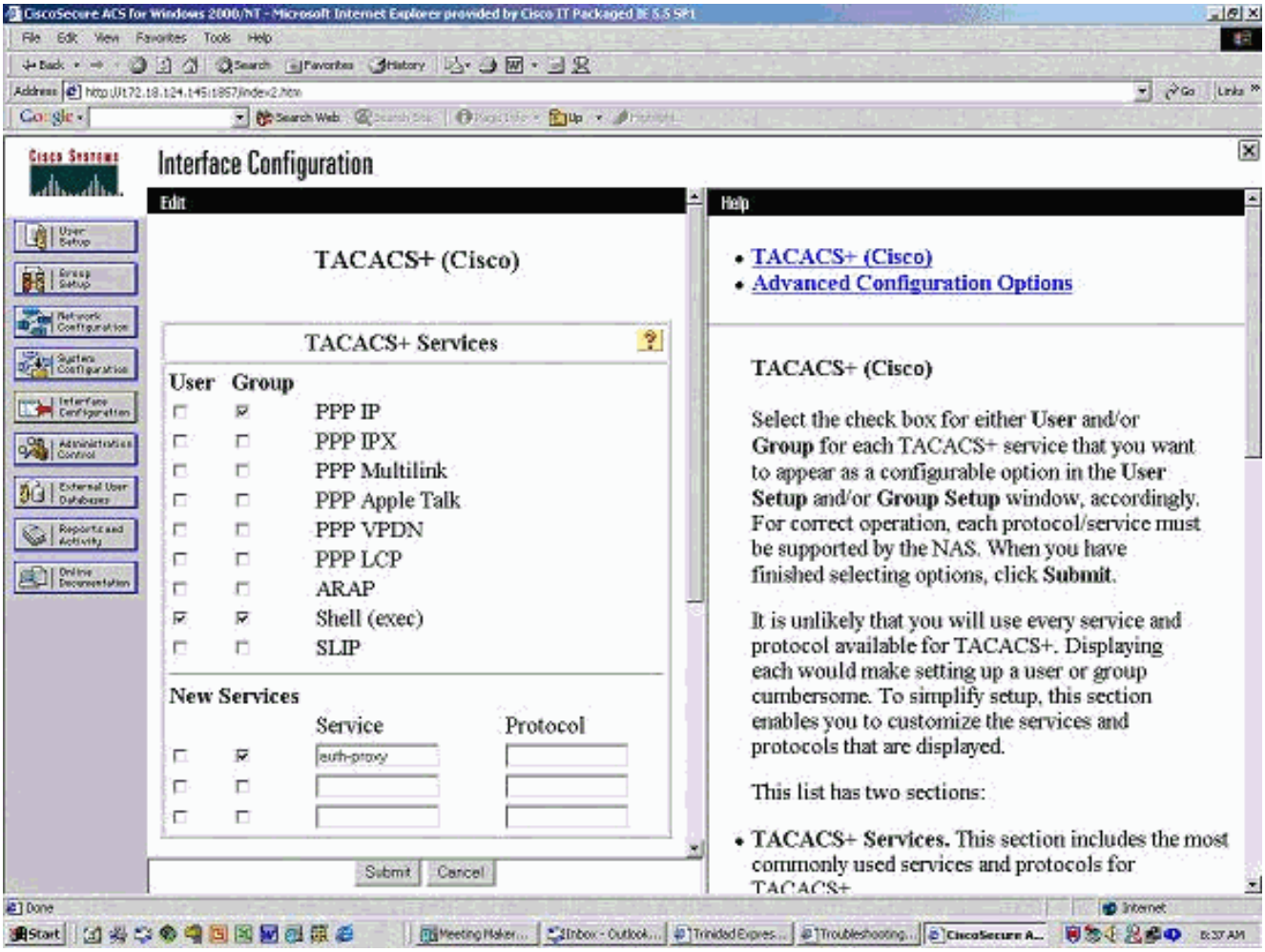
Cisco Secure UNIX(TACACS+)

```
# ./ViewProfile -p 9900 -u proxyonly
User Profile Information
user = proxyonly{
profile_id = 57
set server current-failed-logins = 1
profile_cycle = 2
password = clear "********"
service=auth-proxy {
set priv-lvl=15
set proxyacl#1="permit icmp any any"
set proxyacl#2="permit tcp any any"
set proxyacl#3="permit udp any any"
}
}
```

Cisco Secure Windows(TACACS+)

次の手順に従います。

1. ユーザ名とパスワード（Cisco SecureまたはWindowsデータベース）を入力します。
2. Interface Configuration に対して、TACACS+ を選択します。
3. [新しいサービス]の[グループ]オプションを選択し、[サービス]列にauth-proxyと入力します。Protocol のカラムは空白のままにしておきます。



4. Advanced - 各サービスに対するウィンドウが表示され、属性をカスタマイズします。
5. [Group Settings]で、[auth-proxy]をオンにし、ウィンドウに次の情報を入力します。

```
priv-lvl=15
proxyacl#1=permit icmp any any
proxyacl#2=permit tcp any any
proxyacl#3=permit udp any any
```

Cisco Secure UNIX(RADIUS)

```
# ./ViewProfile -p 9900 -u proxy
User Profile Information
user = proxy{
profile_id = 58
profile_cycle = 1
radius=Cisco {
check_items= {
2="proxy"
}
reply_attributes= {
9,1="auth-proxy:priv-lvl=15"
9,1="auth-proxy:proxyacl#1=permit icmp any any"
9,1="auth-proxy:proxyacl#2=permit tcp any any"
9,1="auth-proxy:proxyacl#3=permit udp any any"
}
}

}
```

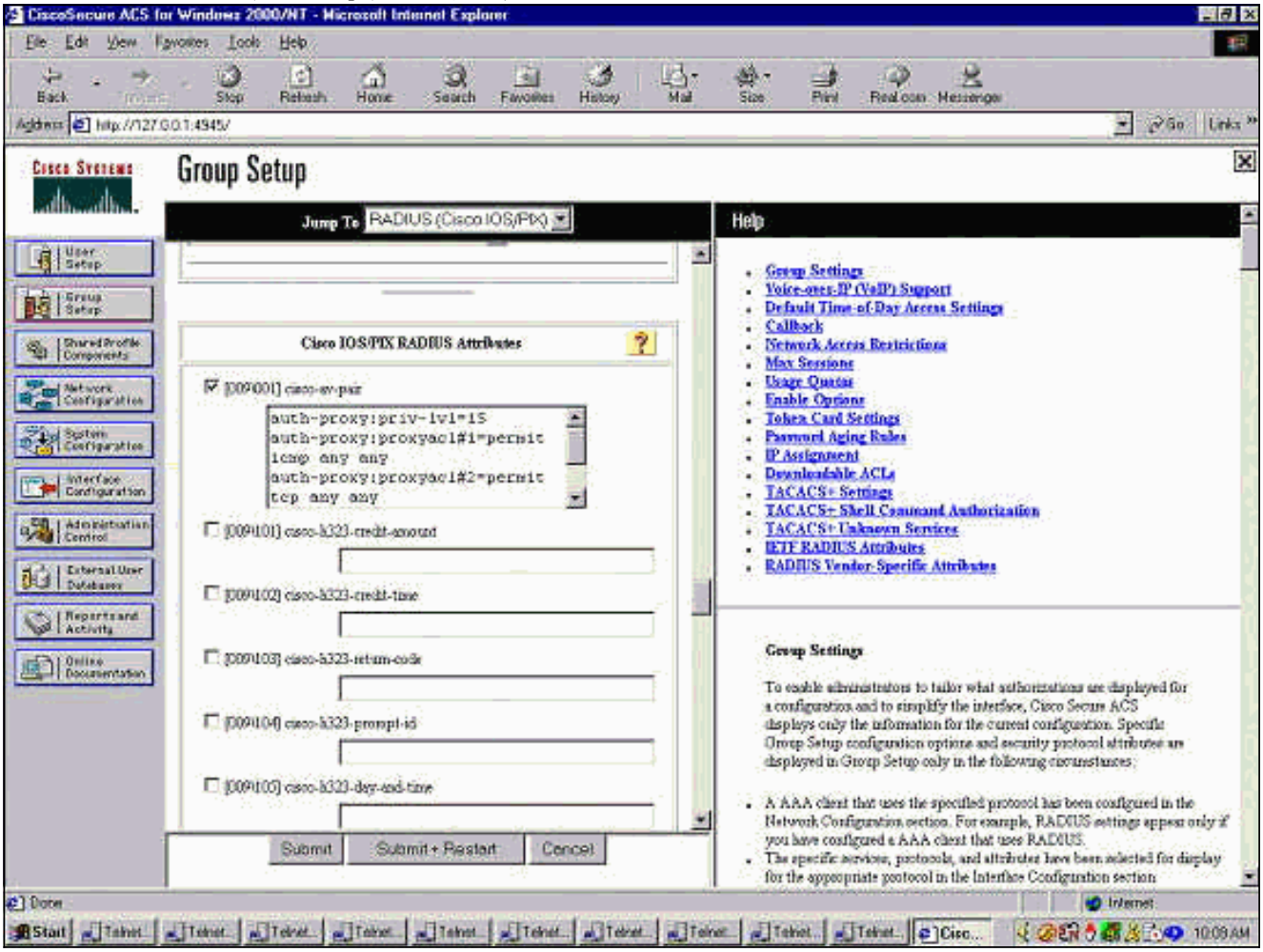
Cisco Secure Windows(RADIUS)

次の手順に従います。

1. Network Configuration を開きます。NAS は Cisco radius であることが必要です。
2. [Interface Configuration RADIUS]が使用可能な場合は、[VSA]ボックス**をオンに**します。
3. User Settings で、Username/password を入力します。
4. Group Settings で、[009/001] cisco-av-pair のオプションを選択します。選択範囲の下のテキストボックスに、次のように入力します。

```
auth-proxy:priv-lvl=15
auth-proxy:proxyacl#1=permit icmp any any
auth-proxy:proxyacl#2=permit tcp any any
auth-proxy:proxyacl#3=permit udp any any
```

このウィンドウは、この手順の例です。



ユーザに対する表示

ユーザがファイアウォールの反対側をブラウズしようとしています。

次のメッセージが表示されたウィンドウが表示されます。

```
Cisco <hostname> Firewall
Authentication Proxy
```

```
Username:
Password:
```

ユーザ名とパスワードに問題がなければ、次のように表示されます。

```
Cisco Systems
Authentication Successful!
```

認証に失敗すると、次のメッセージが表示されます。

```
Cisco Systems
Authentication Failed!
```

関連情報

- IOS ファイアウォールのサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems