

認証プロキシの実装

目次

[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。

この資料は auth-proxy が使用中のときユーザに auth-proxy の実装のための一般的な情報を与え、auth プロキシにいくつかの Cisco Secure サーバ プロファイルを提供し、ユーザが見るものを記述したものです。

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

次の手順を実行します。

1. auth-proxy を設定する前にことをファイアウォールによるトラフィックフローきちんと確かめて下さい。
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. auth-proxy コマンドおよびテストを追加するが、コンソールポートか仮想端末、仮想端末回線 (VTY) の下で `exec-timeout 0 0` とデバッグをつけて下さい。

サーバのプロファイル

テストは Cisco Secure UNIX および Windows によって行われました。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 および パスワードを入力して下さい (Cisco Secure または Windows データベース)。
2. Interface Configuration に対して、TACACS+ を選択します。
3. 新しいサービスの下で、**グループ** オプションを選択し、サービス カラムの **auth-proxy** を入力して下さい。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. グループ設定では、**auth-proxy** をチェックし、ウィンドウでこの情報を入力して下さい:
`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. インターフェイスコンフィギュレーション RADIUS が利用できる場合、VSA ボックスをチェックして下さい。
3. ユーザ設定では、username/password を入力して下さい。
4. Group Settings で、[009/001] cisco-av-pair のオプションを選択します。選択の下のテキストボックスでは、これを入力して下さい：
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ステップの例です。

[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。

ウィンドウはこのメッセージと表示されます：

```
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](#)