# 認証プロキシの実装

### 内容

概要 <u>前提条件</u> 要件 使用するコンポーネント <u>表記法</u> 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

#### <u>概要</u>

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。

### <u>前提条件</u>

<u>要件</u>

このドキュメントに特有の要件はありません。

#### <u>使用するコンポーネント</u>

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。

#### <u>表記法</u>

ドキュメント表記の詳細は、「<u>シスコ テクニカル ティップスの表記法</u>」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。
- 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。

### <u>サーバのプロファイル</u>

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。

Edit View Favorite	-s Took	s Help	sour internet explore provided by the	11 Packaged in a 5 Set		Î
a + + • @ 3	1 3	Search (e.	Favorites Stratory 12 - 3 W -	18		
1 http:///172.18.124	4.1.45118	7, index2, htm			₩ c <sup>2</sup> Go Leta	30
gie •	001-00520	• (* Sea	h Web : @parts for    @Part for +	🛅 Up 🖓 🥒 Provinse 👘	사람들은 아이들에서 전 이렇게 제품가 물건을 통해야 하네.	
a Searcest Int	terfac	e Confi	uration		وا	R
based base	it :				Help	
User Setup Setup	TACACS+ (Cisco)				<u>TACACS+ (Cisco)</u> <u>Advanced Configuration Options</u>	
Retwork Configuration	TACACS+ Services			2		
Configuration	Jser	Group			TACACS+ (Cisco)	
eterface Denfiguration		R	PPP IP		Select the check how for either Hear and/or	
ninistation [	14		PPP IPX		Group for each TACACS+ service that you want	
	3		PPP Multilink		to appear as a configurable option in the User	
d Uber			PPP Apple Talk		Setup and/or Group Setup window, accordingly.	
	-		PPP VPDN		For correct operation, each protocol/service must	
	-		PPP LCP		be supported by the NAS. When you have	
Alen T			ARAP		finished selecting options, click Submit.	
F	2	R	Shell (exec)	1	It is unlikely that you will use every service and	
C	-	Ē.	SLIP		protocol available for TACACS+. Displaying	
	New Services				each would make setting up a user or group	
1	iew c	ervices	Service Deat	100	enables you to customize the services and	
	-		bervice Prov		protocols that are displayed.	
	_	2	leum-proxy			
1		-			This list has two sections:	
÷1	_				• TACACS+ Services This section includes the most	
			21-21	<u> </u>	<ul> <li>FACACS+ Services. This section includes the most commonly used services and protocols for</li> </ul>	
			Submit		TACACS+	-
					😰 internet	

- 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"
}
}
}
```

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。
CiscoSecure ACS for Windows 2000/NT - Wicrosoft Internet Explo
                                                                                                                                                                            18 X
  File Edit View Favorites Tools
                                       Heb
                                                                                                                                                                             100
                                                                                             넢
                              0
                                        10
                                                  Here
                                                              2
                                                                                   3
                                                                                                                           Real cost Hessens
                                                                                                        - (金)
                                                                         -
                                                                                                                   Relie
    Back
 Agidienta 🔄 http://127.0.0.1.4945/

→ 2 Go Links

                                                                                                                                                                               ×
                        Group Setup
    Cesca Systems
     aile.
            فتقلقه
                                          Jump To RADIUS (Cisco IOS/PIX) 💌
                                                                                                       Help
   - User
Setup
                                                                                                  -
                                                                                                            Group Settings
Voice-over-IP (VoIP) Support
  Batep
                                                                                                            Default Time of Day Access Settings
Callback
                                                                                         ?
                                          Cinco IOS/PIX RADRIS Attributes
                                                                                                            Network Access Restrictions
  Shared Profile
Components
                                                                                                            Max Services
                                                                                                            Usage Quatas
Enable Option
                            17 [009001] caso-av-pair
  Autwork
Cealignation
                                                                                                            Token Card Setti
                                     auth-proxy:priv-lv1*15
                                                                                -
                                                                                                               amori Aging Rules
  Sestem
Configuration
                                      auth-proxy:proxyacl#i=permit
                                                                                                            IP Assignment
Develophile ACL
                                     icmp any any
                                      auth-proxy;proxyacl#2=permit
  Condiguration
                                                                                                            TACACS+ Settin
                                     tep any any
                                                                                .
                                                                                                            TACACS+ Shell Command Authorization
  Ado histuatia
                            [ [009101] cisco-k323-credit-enound
                                                                                                            TACACS+ Unknown Services
IETE RADIUS Attributes
                                               f
                                                                                                            RADIUS Vender-Specific Attributes
 Del Defebarer
                            [ [009402] cisco-h323-credit-time
  Activity
                                               I
                                                                                                            Group Settings
                            🖺 (009/103) cisco-5323-retum-code
  Documentation
                                                                                                            To easible administrators to tailor what authorizations are displayed for 
a configuration and to simplify the interface, Cieco Secure ACS 
displays only the information for the current configuration. Specific
                            D09104 circo-h323-prompt-id
                                                                                                            Or one Setup configuration options and accurity protocol attributes are
displayed in Group Setup only in the following corranstances
                            [ [009100] cisto-k323-day-and-time
                                                                                                         . A AAA client that uses the specified protocol has been configured in the
                                                                                                            Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA clear that uses RADIUS.
                                                    Submit + Restart
                                       Submit
                                                                            Cencel
                                                                                                            The specific services, protocols, and attributes have been selected for daplay
                                                                                                            for the appropriate protocol in the Interface Configuration section.
#1 Dote
                                                                                                                                                      in/ernet
 #Statt Tahet Teres Teres
```

## <u>ユーザに対する表示</u>

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。

<sup>Username:</sup> 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!



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