實施身份驗證代理

目錄

簡介

Cisco IOS®軟體防火牆版本12.0.5.T和更新版本中提供的驗證代理(auth-proxy)用於對傳入和/或傳出使用者進行驗證。這些使用者通常被訪問清單阻止。但是，透過驗證代理，使用者會啟動瀏覽器來通過防火牆，並在TACACS+或RADIUS伺服器上進行驗證。伺服器會把其他存取清單專案向下傳遞到路由器，以便在驗證之後允許使用者通過。

本檔案將提供使用者實施驗證代理的一般提示，提供一些適用於驗證代理的思科安全伺服器設定檔，並說明使用者在使用驗證代理時看到的內容。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

如何實作驗證代理

請完成以下步驟：

1. 設定auth-proxy之前，請確保流量正確通過防火牆。
2. 為了使測試期間的網路中斷降至最低，請修改現有訪問清單以拒絕對一個測試客戶端的訪問。
3. 請確保一個測試客戶端無法通過防火牆，並且其他主機可以通過。
4. 在控制檯埠或虛擬型別終端(VTY)下使用**exec-timeout 0 0**開啟debug，同時新增**auth-proxy**命令並進行測試。

伺服器配置檔案

我們的測試是使用Cisco Secure UNIX和Windows完成的。如果正在使用RADIUS，則RADIUS伺服器必須支援廠商專用屬性（屬性26）。 具體伺服器示例如下：

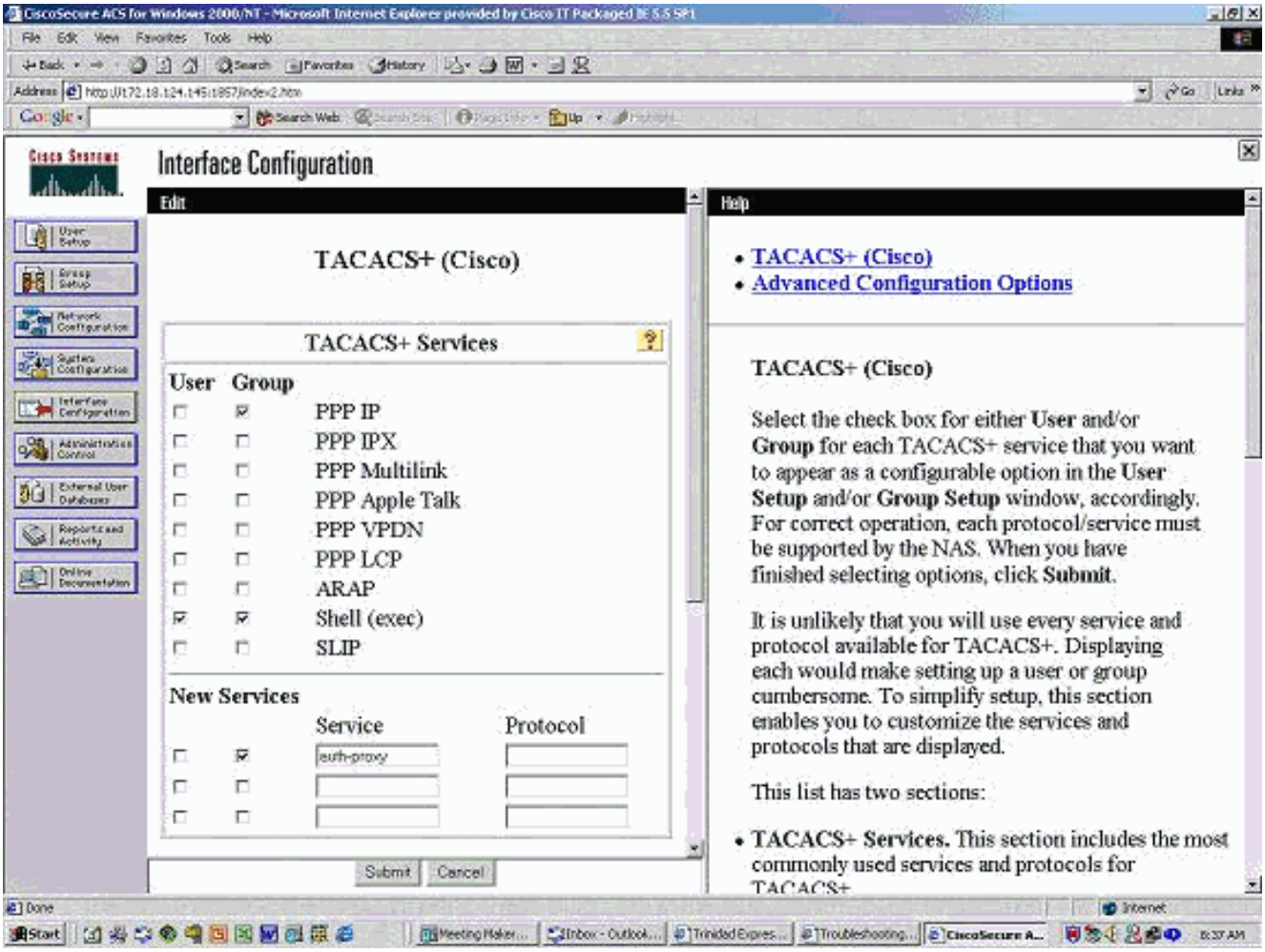
Cisco Secure UNIX(TACACS+)

```
# ./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+)

請按照以下步驟操作。

1. 輸入使用者名稱和密碼（Cisco Secure或Windows資料庫）。
2. 對於介面配置，請選擇**TACACS+**。
3. 在新服務下，選擇**Group**選項，然後在「服務」列中鍵入**auth-proxy**。將「協定」列留空。



4. 高級 — 顯示每個服務的視窗 — 自定義屬性。
5. 在「組設定」中，選中**auth-proxy**，然後在視窗中輸入以下資訊：

```
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"
}
}

}
```

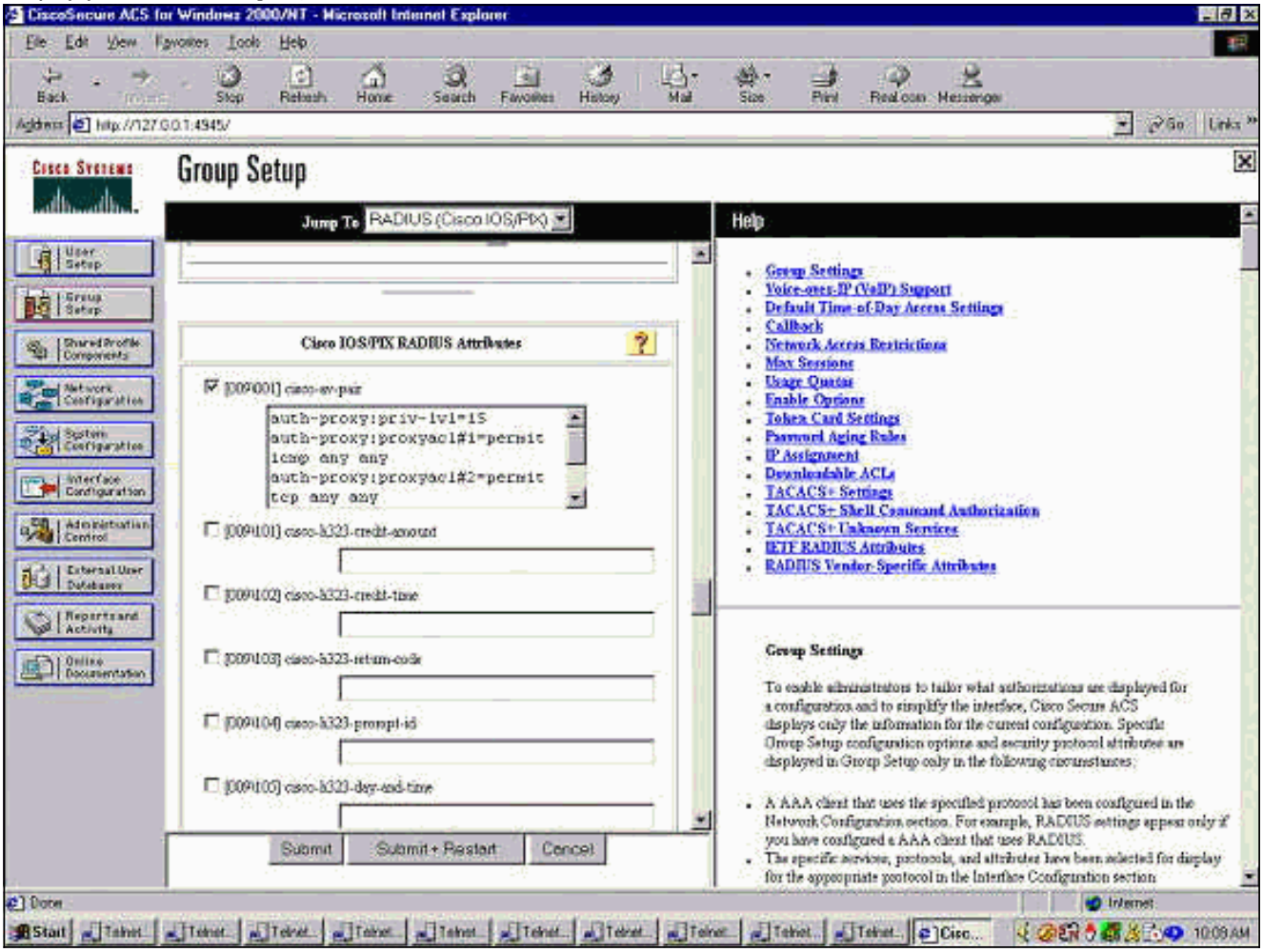
Cisco Secure Windows(RADIUS)

請按照以下步驟操作。

1. 開啟網路配置。NAS應為Cisco RADIUS。
2. 如果介面配置RADIUS可用，請選中**VSA**框。
3. 在使用者設定中，輸入使用者名稱/密碼。
4. 在「組設定」中，選擇**[009/001] cisco-av-pair**的選項。在選定內容下面的文本框中，鍵入以下內容：

```
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
```

此視窗是此步驟的示例。



使用者所看到的內容

使用者嘗試瀏覽防火牆另一端的專案。

將顯示一個視窗，其中顯示以下消息：

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

```
Username:
Password:
```

如果使用者名稱和密碼正確，使用者將看到：

```
Cisco Systems
Authentication Successful!
```

如果驗證失敗，則消息為：

```
Cisco Systems
Authentication Failed!
```

相關資訊

- IOS防火牆支援頁面
- 技術支援與文件 - Cisco Systems