實施身份驗證代理

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>如何實作驗證代理</u> <u>伺服器配置檔案</u> <u>Cisco Secure UNIX(TACACS+)</u> <u>Cisco Secure Windows(TACACS+)</u> <u>使用者所看到的內容</u> <u>相關資訊</u>

<u>簡介</u>

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。

<u>必要條件</u>

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本文件所述內容不限於特定軟體和硬體版本。

<u>慣例</u>

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。

| | Mana . | Grann Grant 13. 3 E. 3 Z | |
|-------------------------|---------------|--------------------------|--|
| ttp:///172.18.124.145/1 | 857)inde-(2.h | tn | 🛫 (2 ² Ga) Linka |
| | - 00 S | arch Web - Og bearch the | <u> </u> |
| Interfa | ce Cont | iguration | |
| Edit | | 3 | El Holo: |
| | | | |
| | | TACACS+ (Cisco) | • TACACS+ (Cisco) |
| | | Sector Sector | Advanced Configuration Options |
| | | | |
| Į | | TACACS+ Services | |
| User | Group |) | TACACS+ (Cisco) |
| | R | PPP IP | Select the check hox for either User and/or |
| 'E' | | PPP IPX | Group for each TACACS+ service that you want |
| E . | | PPP Multilink | to appear as a configurable option in the User |
| | | PPP Apple Talk | Setup and/or Group Setup window, accordingly. |
| E | E. | PPP VPDN | For correct operation, each protocol/service must |
| | | PPP LCP | finished selecting ontions, click Submit |
| | 17 | ARAP | |
| E. | R | Shell (exec) | It is unlikely that you will use every service and |
| | | SLIP | protocol available for TACACS+. Displaying |
| New | Service | 5 | cumbersome. To simplify setup, this section |
| | | Service Protocol | enables you to customize the services and |
| Έ. | R | euth-proxy | protocols that are displayed. |
| Ē | | | This list has two sections: |
| E . | | | |
| | | | TACACS+ Services. This section includes the most |
| | | Salarit Cancal | commonly used services and protocols for |

- 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)

auth-proxy:priv-lvl=15

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。

auth-proxy:proxyacl#1=permit icmp any any

- 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:

| 此視窗是此步 | ▽驟的示例。 | | |
|------------------------------|---|---|--|
| CiscoSecure ACS for | Windows 2000/NT - Wicrosoft Internet Esplorer | 201 | |
| Ele Edi Yew Fav | owes Look Help | | |
| Eack - | Stop Retects Home Search FavoRes History Ma | * ∰* ∰ ₽ 🗶 Size Pint Real.com Hessenae | |
| Agidents 🔄 http://127.00 | 11.4945/ | 🖃 🖉 Go 🛛 Leks | |
| Canes Systems | Groun Sotun | 5 | |
| -alice data | aroup setup | | |
| Relativer to the second | Lings Te, RADIUS (Cisco IOS/PM) | Help | |
| User Setup | | · Green Setting | |
| and Series | | Voice-ores: IP (VoIP) Support | |
| To I Sector | | Callback | |
| Shared Profile Components | Claro IUSTIX RADIUS Attributes | Setwork Access Restrictions Max Sensions | |
| Natwork Configuration | 1009001] ciaco-ev-pair | Usage Quartar Enable Options | |
| Sector a sector part of the | auth-proxy:priv-lv1=15 | Token Card Settings | |
| Contigeration | auth-proxy:proxyacl#1=permit icmp any any | Passignment Passignment | |
| Endineration | auth-proxy(proxyac1#2=permit | Describentable ACLs TACACS - Services | |
| ER Laterstatur | tep any any | TACACS+ Shell Command Authorization | |
| Centrol | 1 . [009101] case-k323-medit-amount | IACAUS+ Unknown Services IETF RADIUS Attributes | |
| External Uper | E | RADIUS Vender Specific Attributes | |
| Con L Report and | [009402] cisco-3323-credit-time | | |
| Activity | | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | |
| Documentation | 🗖 (009/103) cisco-à323-retum-code | Group Settings | |
| | | To easible administrators to tailor what suthermations are displayed for a configuration and to simplify the interface. Given Secure ACS | |
| | 10990040 ctaso-3323 prompt-id | deploys only the information for the current configuration. Specific | |
| | l | Uroup being configuration optime and security protocol altibutes are displayed in Group Setup only in the following circumstances: | |
| | 🗆 (0094005) cisco-h522)-day-and time | | |
| | | A AAA carst that uses the specifies proceed as seen codigited in the Network Configuration section. For example, RADIUS settings appear only if | |
| | Submit Submit+Restart Cencel | you have configured a AAA chest that uses RADUUS. The specific services, protocols, and attributes have been adacted for damlay | |
| 4 | | for the appropriate portocol in the Interface Configuration section | |
| Dote: | | 🔮 internet | |

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:

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!



• IOS防火牆支援頁面

• 技術支援與文件 - Cisco Systems