Authentifizierungsproxy implementieren

Inhalt

Einführung

Der Authentifizierungsproxy (auth-proxy), verfügbar in der Cisco IOS® Software Firewall Version 12.0.5.T und höher, wird zur Authentifizierung ein- und ausgehender Benutzer oder beides verwendet. Diese Benutzer werden normalerweise durch eine Zugriffsliste blockiert. Mit auth-proxy rufen die Benutzer jedoch einen Browser auf, um die Firewall zu durchlaufen und sich auf einem TACACS+- oder RADIUS-Server zu authentifizieren. Der Server übergibt zusätzliche Zugriffslisteneinträge bis zum Router, damit die Benutzer nach der Authentifizierung fortfahren können.

Dieses Dokument enthält allgemeine Tipps für den Benutzer zur Implementierung von auth-Proxy, enthält einige Cisco Secure Server-Profile für den Authentifizierungsproxy und beschreibt, was der Benutzer sieht, wenn auth-proxy verwendet wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips

Conventions.

Implementieren des Authentifizierungsproxys

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Datenverkehr ordnungsgemäß durch die Firewall fließt, bevor Sie den auth-Proxy konfigurieren.
2. Um während des Testens eine minimale Unterbrechung des Netzwerks zu ermöglichen, ändern Sie die vorhandene Zugriffsliste so, dass der Zugriff auf einen Testclient verweigert wird.
3. Stellen Sie sicher, dass der eine Test-Client die Firewall nicht durchlaufen kann und dass die anderen Hosts durchkommen können.
4. Aktivieren Sie das Debuggen mit **exec-timeout 0 0** unter dem Konsolenport oder den Virtual Type Terminals (VTYs), während Sie die **auth-Proxy-**Befehle und den Test hinzufügen.

Serverprofile

Die Tests wurden mit Cisco Secure UNIX und Windows durchgeführt. Wenn RADIUS verwendet wird, muss der RADIUS-Server anbieterspezifische Attribute unterstützen (Attribut 26). Hier einige Beispiele für Server:

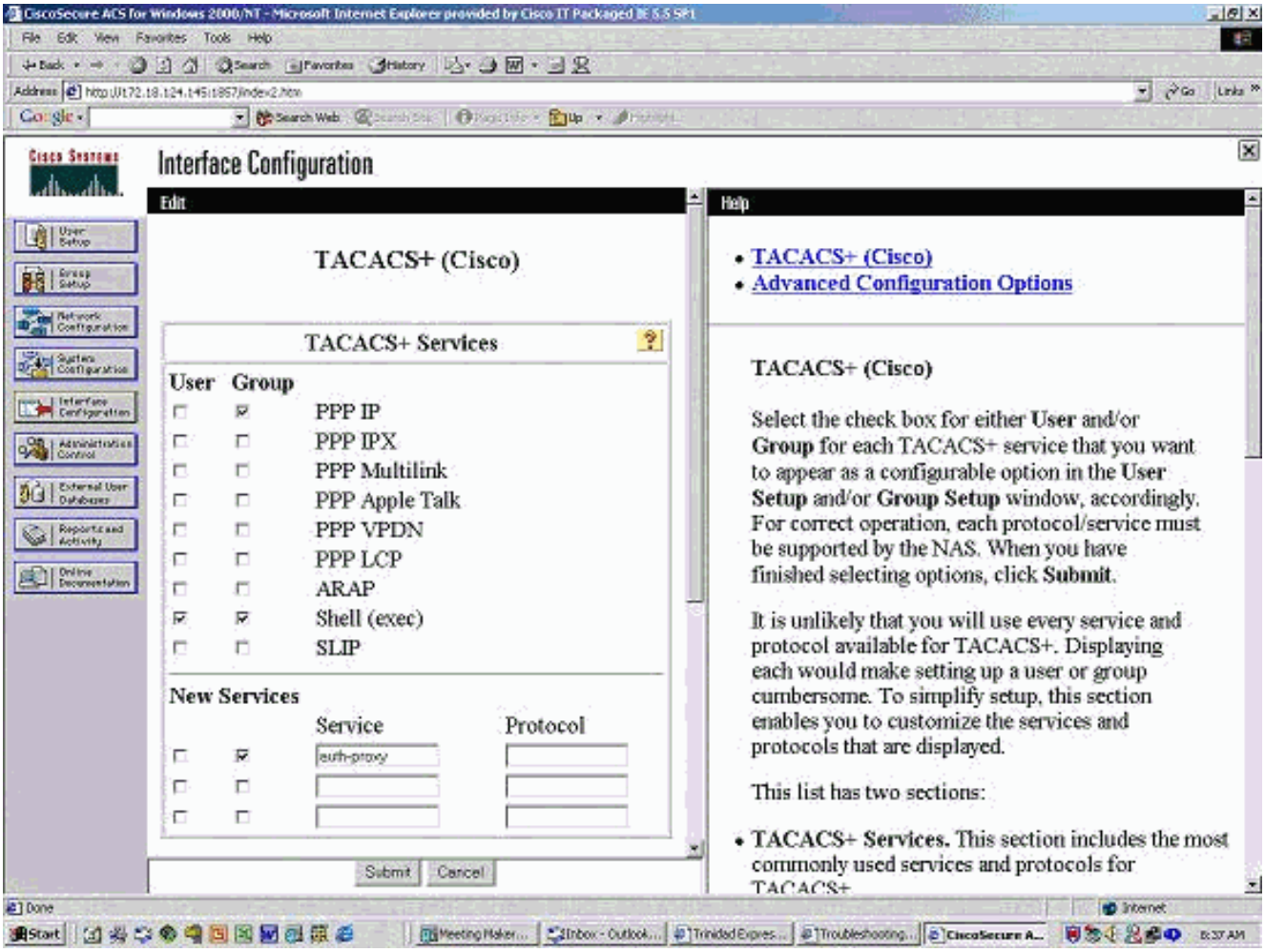
Cisco Secure UNIX (TACACS+)

```
# ./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+)

Befolgen Sie dieses Verfahren.

1. Geben Sie den Benutzernamen und das Kennwort ein (Cisco Secure oder Windows-Datenbank).
2. Wählen Sie als Schnittstellenkonfiguration **TACACS+** aus.
3. Wählen Sie unter Neue Dienste die Option **Gruppe** aus, und geben Sie **auth-proxy** in die Spalte Service ein. Lassen Sie die Spalte Protokoll leer.



4. Erweitert - Fenster für jeden Service anzeigen - benutzerdefinierte Attribute.
5. Aktivieren Sie unter Gruppeneinstellungen die Option **auth-proxy**, und geben Sie diese Informationen im Fenster ein:

```
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"
}
}
```

}

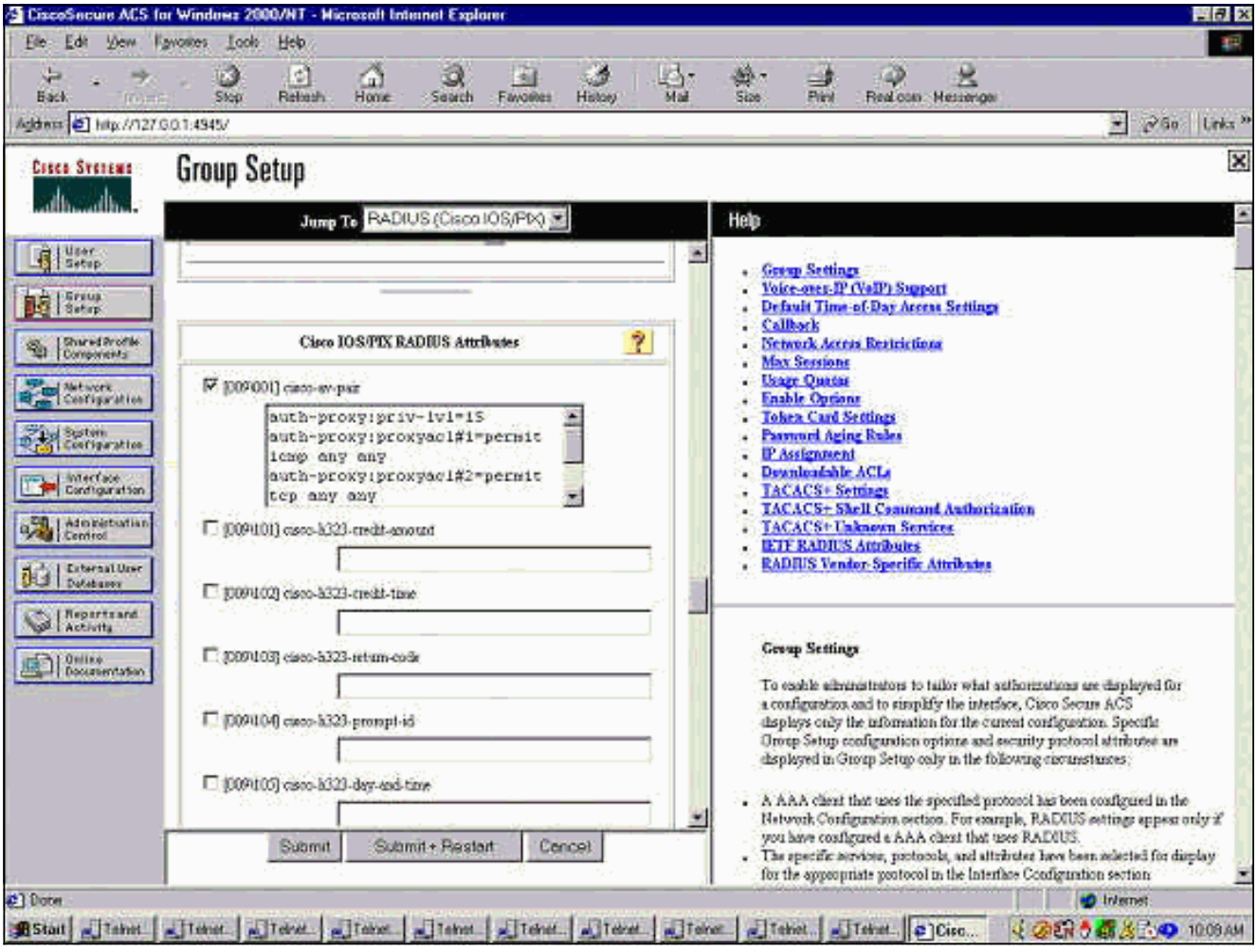
Cisco Secure Windows (RADIUS)

Befolgen Sie dieses Verfahren.

1. Öffnen Sie die Netzwerkkonfiguration. NAS sollte Cisco RADIUS sein.
2. Wenn die Schnittstellenkonfiguration RADIUS verfügbar ist, aktivieren Sie die **VSA-**Kontrollkästchen.
3. Geben Sie unter User Settings (Benutzereinstellungen) den Benutzernamen/das Kennwort ein.
4. Wählen Sie unter "Gruppeneinstellungen" die Option für **[009/001] cisco-av-pair aus**. Geben Sie in das Textfeld unter der Auswahl Folgendes ein:

```
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
```

Dieses Fenster ist ein Beispiel für diesen Schritt.



Was der Benutzer sieht

Der Benutzer versucht, etwas auf der anderen Seite der Firewall zu durchsuchen.

Es wird ein Fenster mit dieser Meldung angezeigt:

```
Cisco <hostname> Firewall
Authentication Proxy
Username:
Password:
```

Wenn Benutzername und Kennwort gut sind, sieht der Benutzer Folgendes:

```
Cisco Systems
Authentication Successful!
```

Wenn die Authentifizierung fehlschlägt, lautet die Meldung:

```
Cisco Systems
Authentication Failed!
```

Zugehörige Informationen

- Support-Seite für IOS-Firewall
- Technischer Support und Dokumentation - Cisco Systems