Verificatieproxy uitvoeren

Inhoud

Inleiding

Verificatieproxy (verificatie-proxy), beschikbaar in Cisco IOS® Software Firewall versie 12.0.5.T en hoger, wordt gebruikt om inkomende of uitgaande gebruikers of beide voor verificatie te zorgen. Deze gebruikers worden normaal gesproken geblokkeerd door een toegangslijst. Maar met auth-proxy halen de gebruikers een browser op om door de firewall te gaan en op een TACACS+ of RADIUS-server te authenticeren. De server passeert extra ingangen van de toegangslijst tot de router toe om de gebruikers door te staan na authenticatie.

Dit document geeft de gebruiker algemene tips voor de implementatie van proxy, biedt een aantal Cisco Secure-serverprofielen voor automatische proxy en beschrijft wat de gebruiker ziet wanneer de auth-proxy wordt gebruikt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Verificatieproxy implementeren

Voer de volgende stappen uit:

1. Zorg ervoor dat het verkeer goed door de firewall stroomt voordat u de automatische proxy instelt.
2. Voor minimale verstoring van het netwerk tijdens het testen, wijzig de bestaande toegangslijst om toegang tot één testclient te ontzeggen.
3. Zorg ervoor dat de ene testclient niet door de firewall kan komen en dat de andere hosts doorheen kunnen.
4. Schakel deze optie in met **exec-timeout 0 0** onder de console poort of virtuele type terminals (VTYs), terwijl u de **auth-proxy** opdrachten en test toevoegt.

serverprofielen

Onze tests zijn uitgevoerd met Cisco Secure UNIX en Windows. Als RADIUS in gebruik is, moet de RADIUS-server de leverancierspecifieke eigenschappen ondersteunen (eigenschap 26). Specifieke servervoorbeelden volgen:

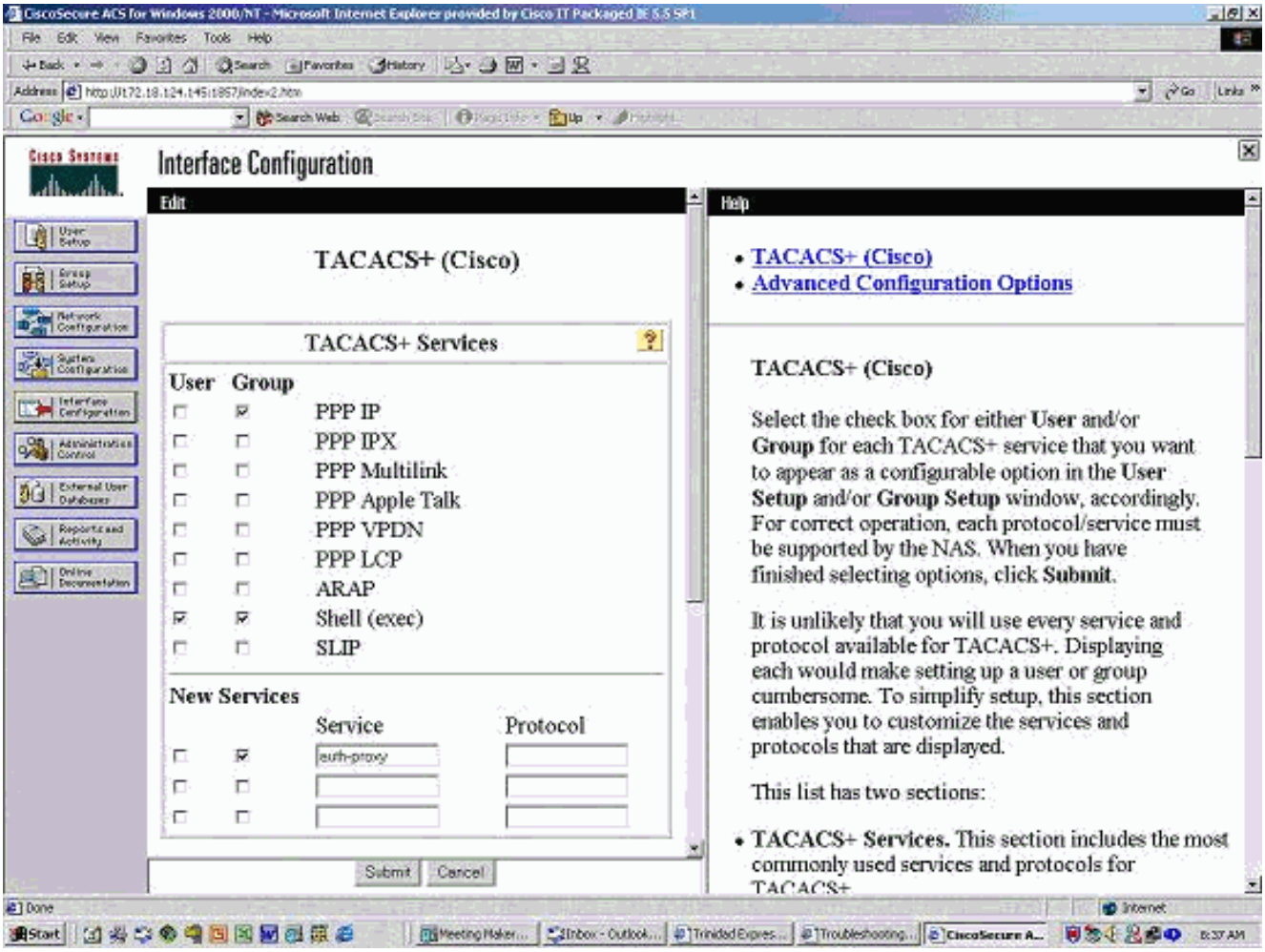
Cisco Secure UNIX (TACACS+)

```
# ./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+)

Volg deze procedure.

1. Voer de gebruikersnaam en het wachtwoord in (Cisco Secure of Windows database).
2. Selecteer voor interfaceconfiguratie de optie **TACACS+**.
3. Selecteer onder New Services de optie **Group** en type **auth-proxy** in de Service kolom. Laat de kolom Protocol
   leeg.



4. Geavanceerd - weergavevenster voor elke op service gerichte eigenschappen.
5. In groepinstellingen controleert u **de proxy-**en voert u deze informatie in het venster in:

```
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"
}
}

}
```

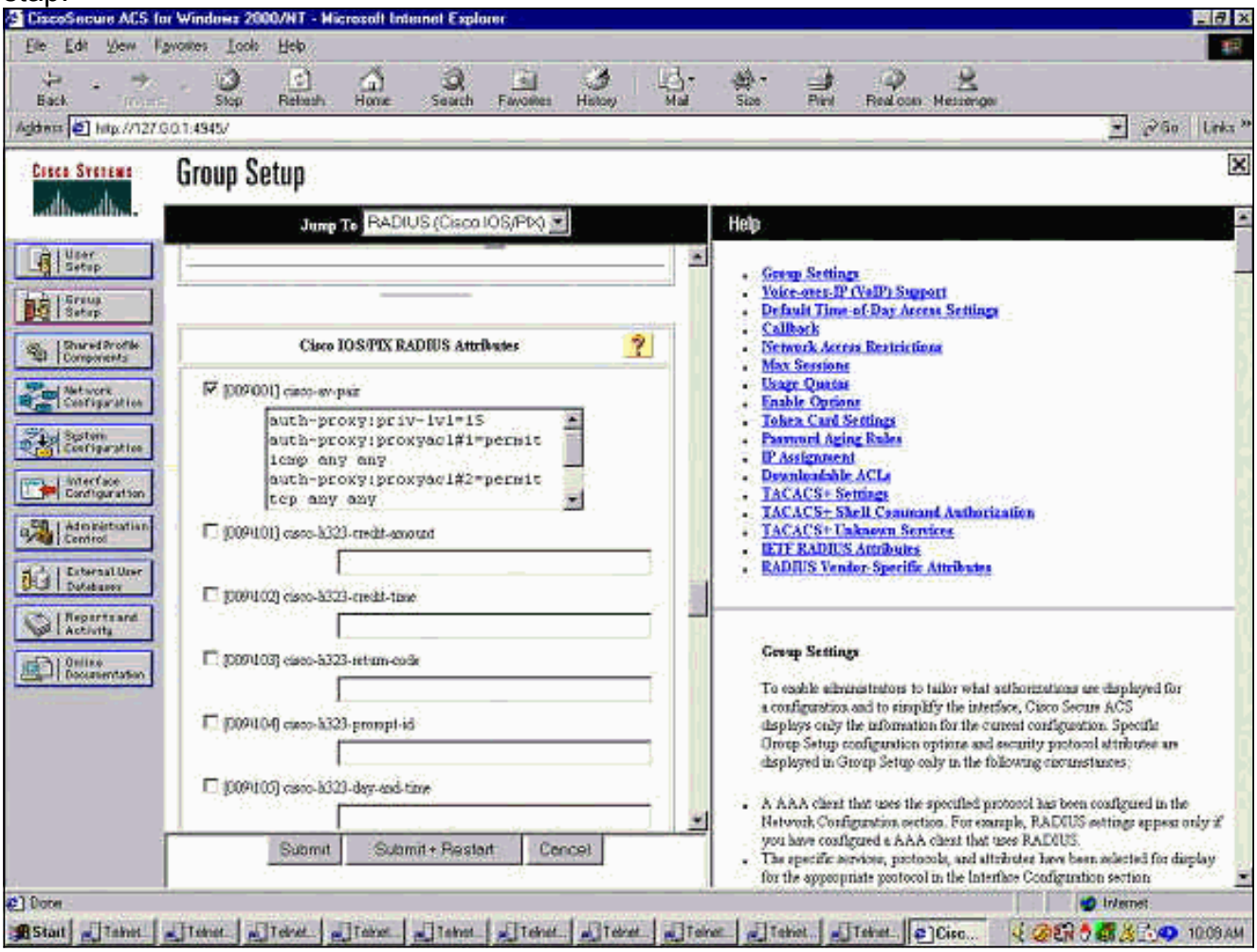
Cisco Secure Windows (RADIUS)

Volg deze procedure.

1. Netwerkconfiguratie openen. NAS moet Cisco RADIUS zijn.
2. Als de RADIUS van de interfaceconfiguratie beschikbaar is, controleert u de **VSA**-vakjes.
3. Voer in de gebruikersinstellingen de gebruikersnaam/het wachtwoord in.
4. Selecteer in groepsinstellingen de optie voor **[009/001] cisco-av-paar**. Typ in het tekstvak onder de selectie het volgende:

```
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
```

Dit venster is een voorbeeld van deze stap.



Wat de gebruiker ziet

De gebruiker probeert iets aan de andere kant van de firewall te bladeren.

Dit bericht wordt in een venster weergegeven:

```
Cisco <hostname> Firewall
```

```
Authentication Proxy
Username:
Password:
```

Als de gebruikersnaam en het wachtwoord goed zijn, ziet de gebruiker:

```
Cisco Systems
Authentication Successful!
```

Als authenticatie mislukt, is het bericht:

```
Cisco Systems
Authentication Failed!
```

Gerelateerde informatie

- IOS-ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems