인증 프록시 구현

목차

소개

Cisco IOS® Software Firewall 버전 12.0.5.T 이상에서 사용 가능한 인증 프록시(auth-proxy)는 인바운드 또는 아웃바운드 사용자 또는 둘 모두를 인증하는 데 사용됩니다.이러한 사용자는 일반적으로 액세스 목록에 의해 차단됩니다.그러나 auth-proxy를 사용하여 사용자는 방화벽을 통과하고 TACACS+ 또는 RADIUS 서버에서 인증하기 위해 브라우저를 불러옵니다.서버는 인증 후 사용자가 통과할 수 있도록 추가 액세스 목록 항목을 라우터로 전달합니다.

이 문서에서는 인증 프록시 구현에 대한 사용자 일반 팁을 제공하고, 인증 프록시에 대한 일부 Cisco 보안 서버 프로필을 제공하며, 인증 프록시가 사용 중일 때 사용자에게 표시되는 내용을 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

인증 프록시 구현 방법

다음 단계를 완료하십시오.

1. auth-proxy를 구성하기 전에 트래픽이 방화벽을 통해 제대로 이동하는지 확인합니다.
2. 테스트 중에 네트워크 중단을 최소화하려면 기존 액세스 목록을 수정하여 하나의 테스트 클라이언트에 대한 액세스를 거부합니다.
3. 한 테스트 클라이언트가 방화벽을 통과할 수 없고 다른 호스트가 통과할 수 있는지 확인하십시오.
4. **auth-proxy** 명령 및 테스트를 추가하는 동안 콘솔 포트 또는 VTY(virtual type terminals)에서 exec-**timeout 0**을 사용하여 디버그를 설정합니다.

서버 프로파일

테스트는 Cisco Secure UNIX 및 Windows에서 수행되었습니다.RADIUS를 사용 중인 경우 RADIUS 서버는 공급업체별 특성(특성 26)을 지원해야 합니다. 특정 서버 예는 다음과 같습니다.

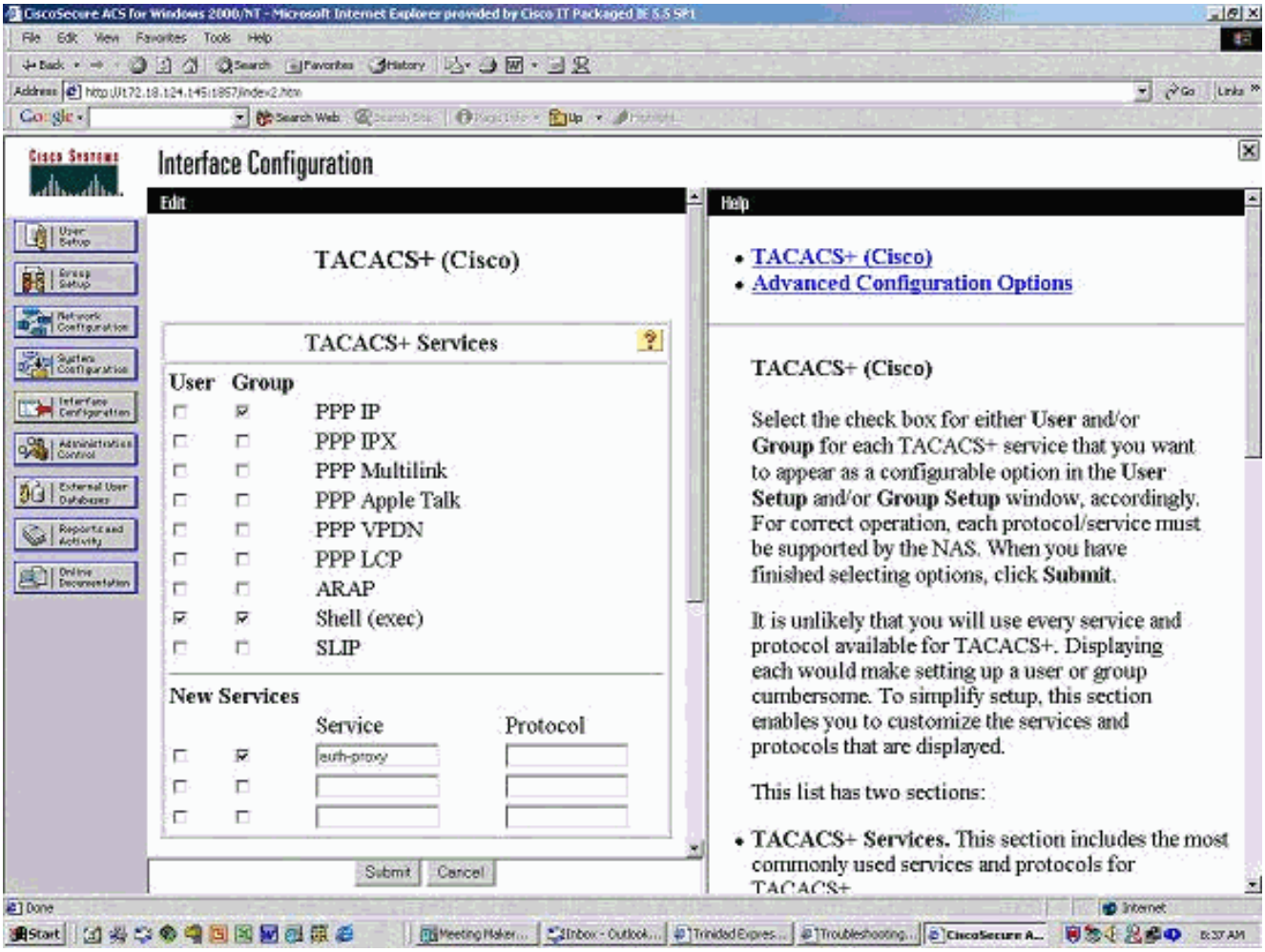
Cisco Secure UNIX(TACACS+)

```
# ./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+)

다음 절차를 수행합니다.

1. 사용자 이름 및 비밀번호(Cisco Secure 또는 Windows 데이터베이스)를 입력합니다.
2. Interface Configuration(인터페이스 컨피그레이션)에서 TACACS**+를** 선택합니다.
3. New Services(새 서비스)에서 **Group(그룹**) 옵션을 선택하고 Service(서비스) 열에 auth-proxy를 입력합니다.Protocol(프로토콜) 열을 비워 둡니다
   .



4. 고급 - 각 서비스에 대한 표시 창 - 사용자 정의 속성
5. Group Settings(그룹 설정)에서 **auth-proxy**를 선택하고 이 정보를 창에 입력합니다.

```
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)

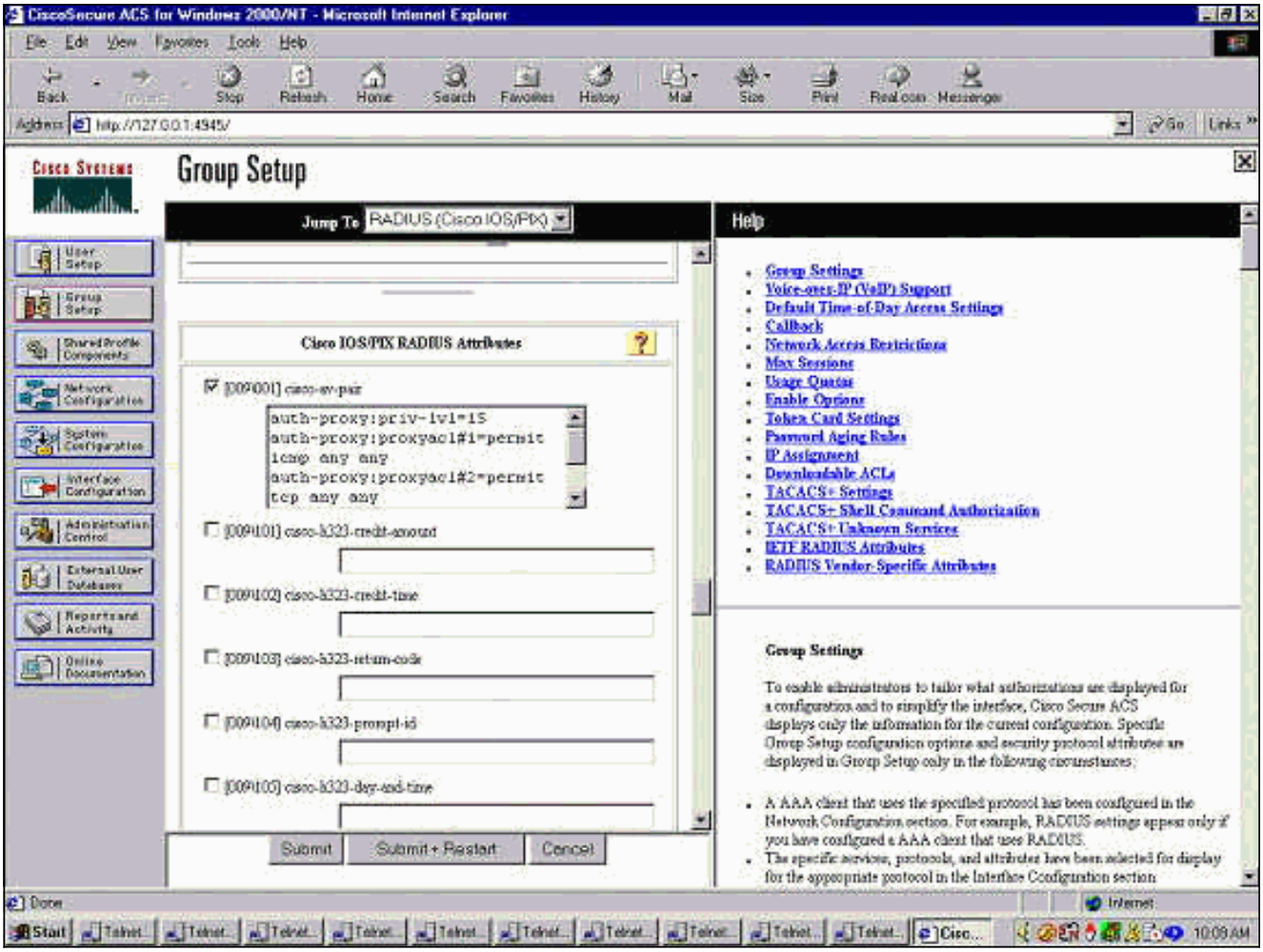
다음 절차를 수행합니다.

1. 네트워크 구성을 엽니다.NAS는 Cisco RADIUS여야 합니다.
2. Interface Configuration RADIUS를 사용할 수 있는 경우 **VSA** 상자를 선택합니다.
3. User Settings(사용자 설정)에서 사용자 이름/비밀번호를 입력합니다.
4. Group Settings(그룹 설정)에서 **[009/001] cisco-av-pair**에 대한 옵션을 선택합니다.선택 영역 아래의 텍스트 상자에 다음을 입력합니다.

```
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
```

이 창은 이 단계의 예입니다

.



사용자에게 표시되는 내용

사용자는 방화벽의 다른 쪽에서 원하는 항목을 찾으려고 합니다.

다음 메시지와 함께 창이 표시됩니다.

```
Cisco <hostname> Firewall
```

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

사용자 이름과 비밀번호가 정상이면 사용자에게 다음과 같은 메시지가 표시됩니다.

```
Cisco Systems
Authentication Successful!
```

인증이 실패하면 메시지는 다음과 같습니다.

```
Cisco Systems
Authentication Failed!
```

관련 정보

- IOS 방화벽 지원 페이지
- 기술 지원 및 문서 – Cisco Systems