实施认证代理

目录

简介

Cisco IOS® 软件防火墙版本 12.0.5.T 及更高版本中提供的认证代理用于对入站和/或出站用户进行身份验证。这些用户通常会由访问列表阻止。但使用认证代理时，用户可启动一个浏览器以通过防火墙，并在 TACACS+ 或 RADIUS 服务器上进行身份验证。服务器会将附加访问列表条目传递到路由器，以便在身份验证之后允许用户通过。

本文档为用户提供了实施认证代理的一般提示，提供了用于认证代理的一些 Cisco Secure 服务器配置文件，并描述了使用认证代理时用户看到的内容。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

如何实施认证代理

完成这些步骤：

1. 在您配置认证代理之前，请确保流量能正常通过防火墙。
2. 为最大程度地减少测试期间的网络中断，请修改现有访问列表，以拒绝对一个测试客户端的访问。
3. 确保该测试客户端不能通过防火墙，而其他主机可以通过。
4. 在您添加 **auth-proxy** 命令并进行测试时，请在控制台端口或虚拟类型终端 (VTY) 下，使用 **exec-timeout 0 0** 开启调试。

服务器配置文件

我们的测试是使用 Cisco Secure UNIX 和 Windows 完成的。如果正在使用 RADIUS，则 RADIUS 服务器必须支持供应商特定属性（属性 26）。下面是特定服务器示例：

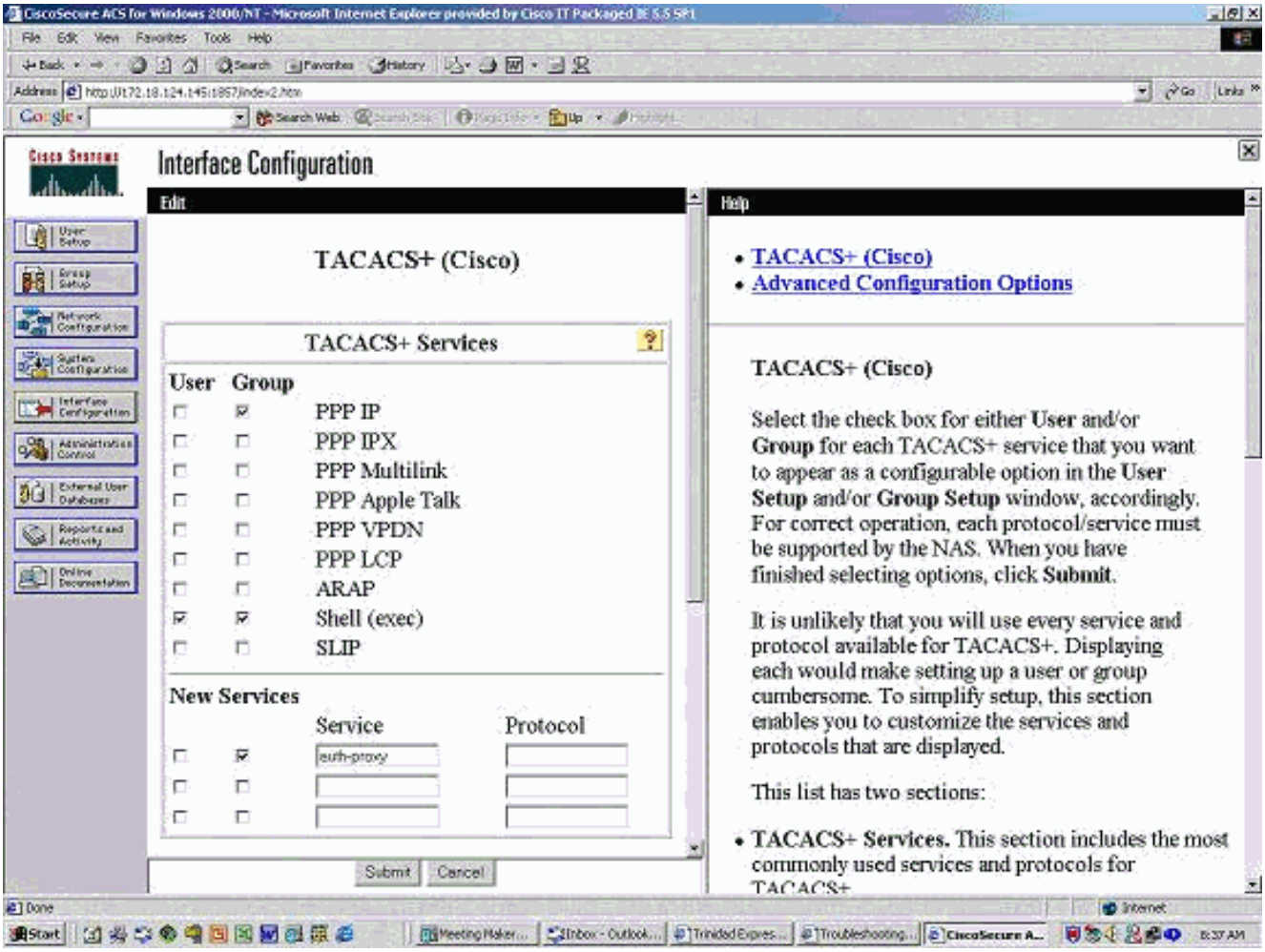
Cisco Secure UNIX (TACACS+)

```
# ./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+)

遵循该步骤。

1. 输入用户名和密码（Cisco Secure 或 Windows 数据库）。
2. 对于接口配置，请选择 **TACACS+**。
3. 在 New Services 下，选择 **Group** 选项，然后在 Service 列中键入 **auth-proxy**。将 Protocol 列保留为空白。



4. Advanced - 每个服务（自定义属性）的显示窗口。
5. 在 Group Settings 中，选中 **auth-proxy**，然后在窗口中输入以下信息：
   `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)

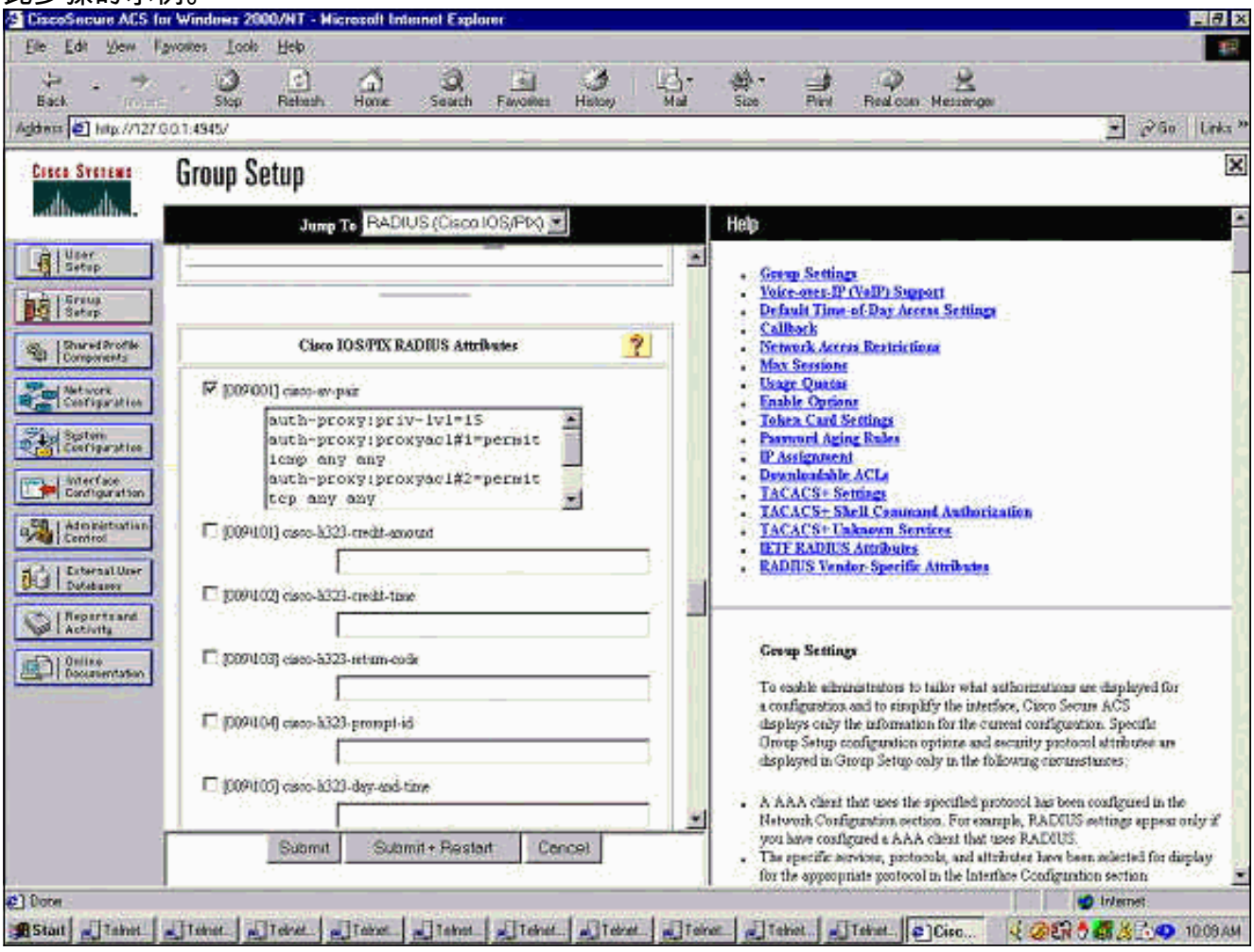
```
# ./ViewProfile -p 9900 -u proxy
User Profile Information
user = proxy{
profile_id = 58
profile_cycle = 1
radius=Cisco {
check_items= {
2="proxy"
}
reply_attributes= {
9,1="auth-proxy:priv-lvl=15"
9,1="auth-proxy:proxyacl#1=permit icmp any any"
9,1="auth-proxy:proxyacl#2=permit tcp any any"
9,1="auth-proxy:proxyacl#3=permit udp any any"
}
}

}
```

Cisco Secure Windows (RADIUS)

遵循该步骤。

1. 打开 Network Configuration。NAS 应为 Cisco RADIUS。
2. 如果 Interface Configuration RADIUS 可用，请选中 **VSA** 框。
3. 在 User Settings 中，输入用户名/密码。
4. 在 Group Settings 中，选择 **[009/001] cisco-av-pair** 的选项。在该选项下面的文本框中，键入以下内容：
   `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` 下面的窗口是此步骤的示例。



用户看到的内容

用户尝试浏览防火墙另一端的内容。

此时会显示一个含有以下消息的窗口：

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

如果用户名和密码正确，则用户会看到：

```
Cisco Systems
Authentication Successful!
```

如果身份验证失败，则消息为：

```
Cisco Systems
Authentication Failed!
```

相关信息

- IOS防火墙支持页面
- 技术支持和文档 - Cisco Systems