Implementando o proxy de autenticação

Contents

Introduction

O proxy de autenticação (auth-proxy), disponível na versão 12.0.5.T e posteriores do Cisco IOS® Software Firewall, é usado para autenticar usuários de entrada ou saída, ou ambos. Estes usuários normalmente são bloqueados por uma lista de acesso. Contudo, com o auth-proxy, os usuários usam um navegador para passar pelo firewall e fazer a autenticação em um servidor TACACS+ ou RADIUS. O servidor passa entradas de lista de acesso adicionais para o roteador, de modo a permitir que os usuários passem por ele após autenticação.

Este documento fornece dicas gerais ao usuário para a implementação do proxy de autenticação, fornece alguns perfis de servidor do Cisco Secure para proxy de autenticação e descreve o que o usuário vê quando o proxy de autenticação está em uso.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Como implementar o proxy de autenticação

Conclua estes passos:

1. Certifique-se de que o tráfego flua corretamente pelo firewall antes de configurar auth-proxy.
2. Para uma interrupção mínima da rede durante os testes, modifique a lista de acesso existente para negar acesso a um cliente de teste.
3. Certifique-se de que um cliente de teste não consiga passar pelo firewall e de que os outros hosts consigam passar.
4. Ative o debug com **exec-timeout 0 0** na porta de console ou nos terminais de tipo virtual (VTYs), enquanto adiciona os comandos **auth-proxy** e testa.

Perfis do servidor

Nosso teste foi feito com o Cisco Secure UNIX e Windows. Se RADIUS estiver em uso, o servidor RADIUS deverá suportar os atributos específicos do fornecedor (atributo 26). Veja abaixo exemplos de servidores específicos:

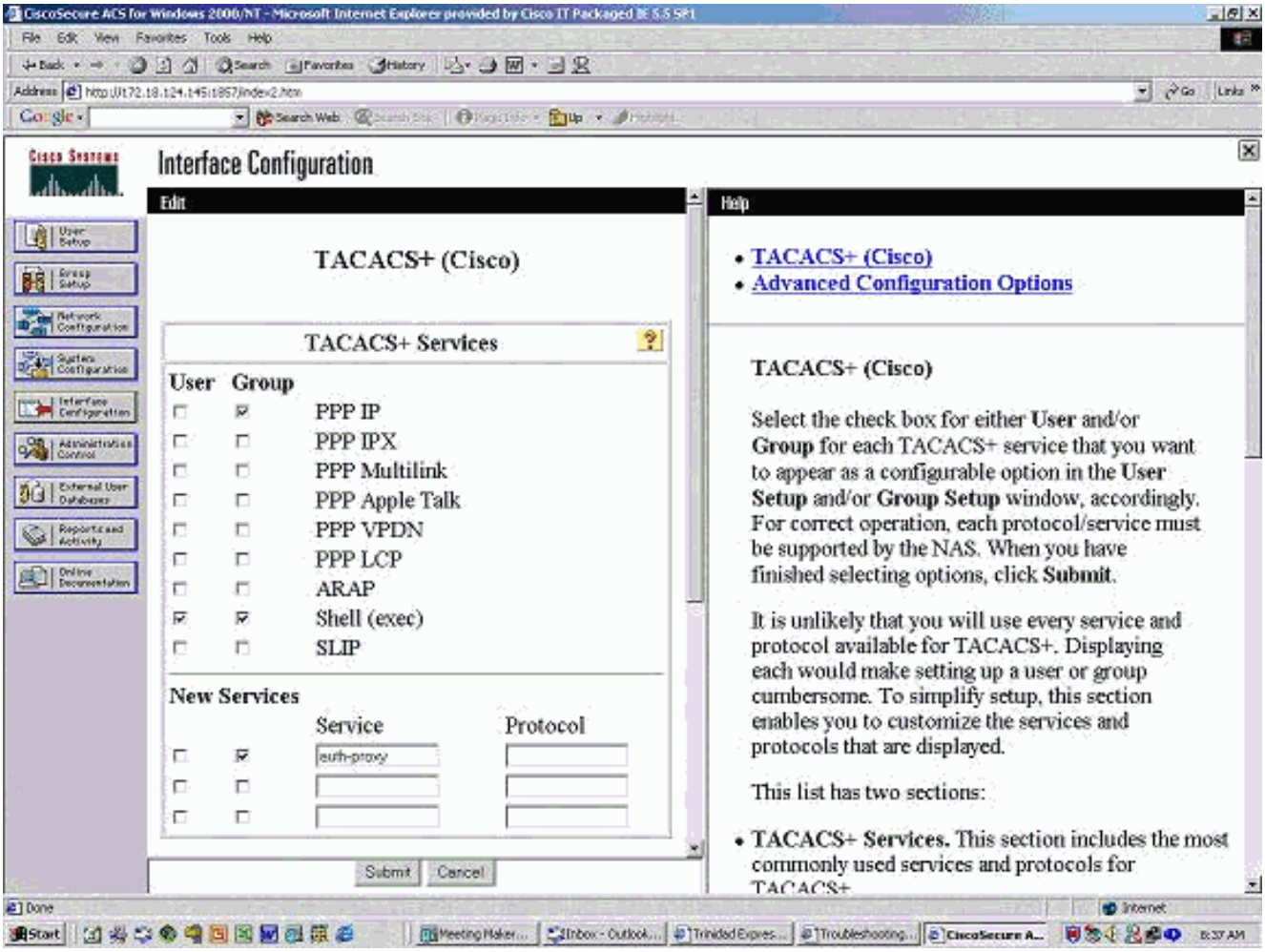
Cisco Secure UNIX (TACACS+)

```
# ./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+)

Siga este procedimento.

1. Insira o nome de usuário e a senha (banco de dados Cisco Secure ou Windows).
2. Para a configuração da interface, selecione **TACACS+**.
3. Em Novos serviços, selecione a opção **Grupo** e digite **auth-proxy** na coluna Serviço. Deixe a coluna Protocolo em
   branco.



4. Avançado janela de exibição de cada serviço atributos personalizados.
5. Em Configurações do grupo, marque **auth-proxy** e insira essas informações na janela:

```
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"
}
}

}
```

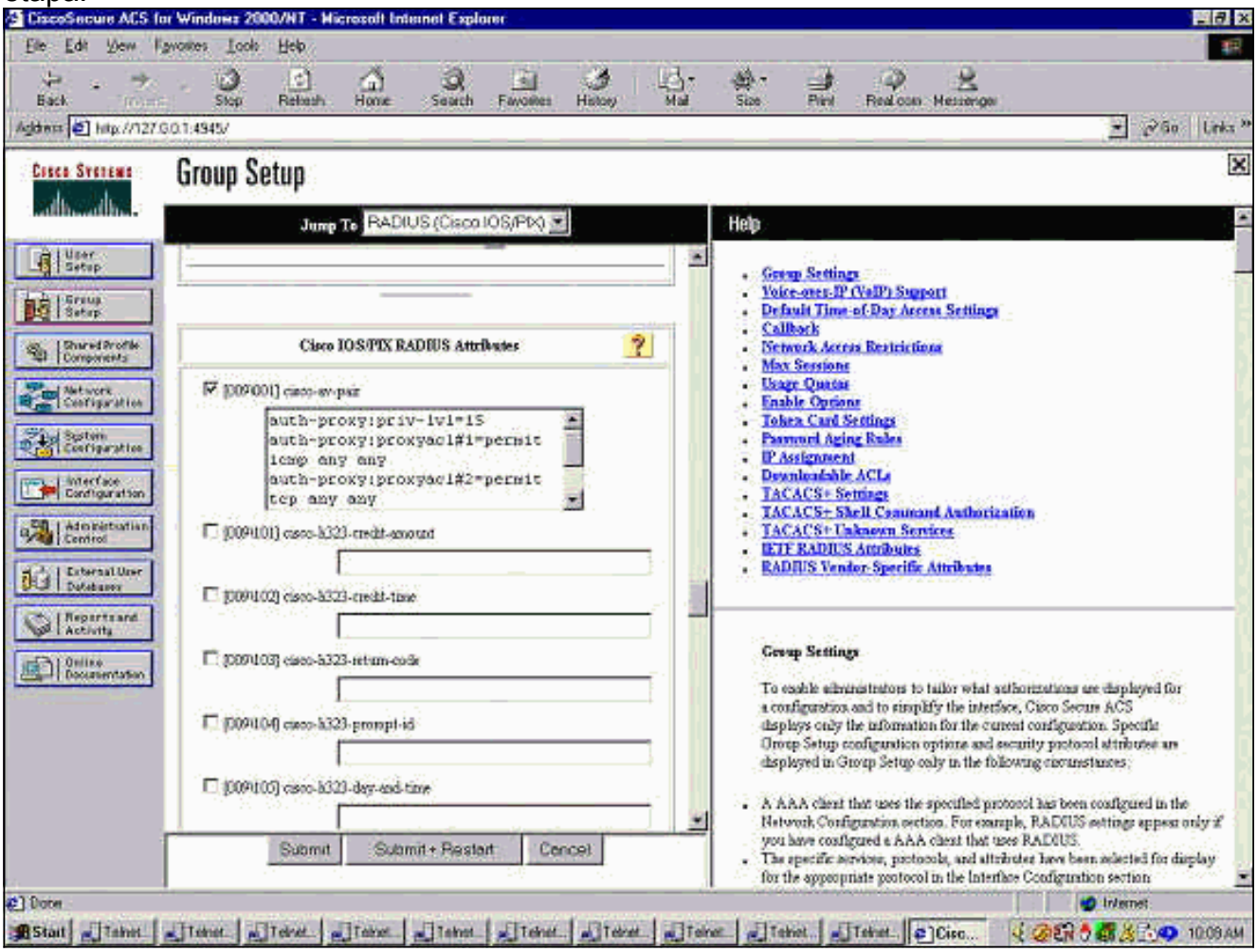
Cisco Secure Windows (RADIUS)

Siga este procedimento.

1. Abrir configuração de rede. O NAS deve ser o Cisco RADIUS.
2. Se Interface Configuration RADIUS estiver disponível, marque as caixas **VSA**.
3. Em Configurações do usuário, digite o nome de usuário/senha.
4. Em Group Settings, selecione a opção para [009/001] cisco-av-pair. Na caixa de texto abaixo da seleção, digite:

```
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
```

Esta janela é um exemplo desta etapa.



O que o usuário vê

O usuário tenta procurar algo no outro lado do firewall.

Uma janela é exibida com esta mensagem:

```
Cisco <hostname> Firewall
```

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

Se o nome de usuário e a senha forem válidos, o usuário verá:

```
Cisco Systems
Authentication Successful!
```

Se a autenticação falhar, a mensagem será:

```
Cisco Systems
Authentication Failed!
```

Informações Relacionadas

- Página de suporte de firewall do IOS
- Suporte Técnico e Documentação - Cisco Systems