Implementando o proxy de autenticação

Índice

Introdução

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 dá ao usuário dicas gerais para a aplicação do autêntico-proxy, fornece alguns perfis do servidor seguro Cisco para o proxy do AUTH, e descreve o que o usuário vê quando o autêntico-proxy está no uso.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Como implementar o proxy de autenticação

Conclua estes passos:

1. Certifique-se de que fluxos de tráfego corretamente com o Firewall antes que você configure o autêntico-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. Gire debugam sobre com EXEC-**intervalo 0 0** sob a porta de Console ou os terminais de tipo virtual (VTY), quando você adicionar os **comandos auth-proxy** e o teste.

Perfis do servidor

Nossos testes foram feitos com Cisco UNIX seguro 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 UNIX seguro (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 Windows seguro (TACACS+)

Siga este procedimento.

1. Incorpore o nome de usuário e senha (Cisco seguro ou base de dados do Windows).
2. Para a configuração da interface, selecione o **TACACS+**.
3. Sob serviços novos, selecione a opção do **grupo** e datilografe o autêntico-**proxy na** coluna do serviço. Deixe a coluna Protocolo em branco.
4. Avançado janela de exibição de cada serviço atributos personalizados.
5. Nas configurações de grupo, verifique o autêntico-**proxy** e incorpore esta informação ao indicador:
   priv-lvl=15 proxyacl#1=permit icmp any any proxyacl#2=permit tcp any any proxyacl#3=permit udp any any

Cisco UNIX seguro (RAIO)

```
# ./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 Windows seguro (RAIO)

Siga este procedimento.

1. Configuração de rede aberta. O NAS deve ser o Cisco RADIUS.
2. Se o RAIO da configuração da interface está disponível, verifique caixas **VSA**.
3. Nas configurações de usuário, incorpore o username/senha.
4. Em Group Settings, selecione a opção para [009/001] cisco-av-pair. Na caixa de texto debaixo da seleção, datilografe isto:
   `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` Este indicador é um exemplo desta etapa.

O que o usuário vê

O usuário tenta consultar algo no outro lado do Firewall.

Indicadores de um indicador 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 falha, a mensagem é:

```
Cisco Systems
Authentication Failed!
```

Informações Relacionadas

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