Implementando o proxy de autenticação

Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Como implementar o proxy de autenticação Perfis do servidor Cisco Secure UNIX (TACACS+) Cisco Secure Windows (TACACS+) O que o usuário vê Informações Relacionadas

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"
}
```

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+.
- Em Novos serviços, selecione a opção Grupo e digite auth-proxy na coluna Serviço. Deixe a coluna Protocolo em branco.

Escosecure Austion windows sould in the Worksold Internet Explorer provided by Lisco IT Packaged It 5.5 skt						
4- Dack +	101 3	Search (affevories Stistory De Of	w • • 9		
ddress 2 http:///172.18.1	24.145118	57)index2.hi			+ c≫Ga Linka '	
Congle +	0000000000	- 6:	arch Web - @charach this - @charach	de e 🎦 📭 💌 🌶 recente 👘	요즘 같은 것은 이에서 이 것을 것을 가지 못했다. 것이 같아요.	
Cinco Searems .	atorfac	o Conf	inuration		×	
dbudh.		JE 00111	iyuraavn	2		
E NUMBER	dit				-	
Eatup			TACACS+ (Cisco	a:	TACACS+ (Cisco)	
	TACACS+ Services			43 	Advanced Configuration Options	
Configuration				2	TACACS+ (Cisco)	
Configuration						
Centigeration		R	PPP IP		Calast the sheal has far sitter Then added	
OB Administration			PPP IPX		Group for each TACACS+ service that you want	
Control		Ξ.	PPP Multilink		to appear as a configurable option in the User	
Batabase			PPP Apple Talk		Setup and/or Group Setup window, accordingly.	
Reports and	E		PPP VPDN		For correct operation, each protocol/service must	
1 Activity	E .	Π	PPP LCP		be supported by the NAS. When you have	
Deceneertation			ARAP		finished selecting options, click Submit.	
	R	R	Shell (exec)	10	It is unlikely that you will use every service and	
	E.	Ē.	SLIP		protocol available for TACACS+. Displaying	
	New Seminer				each would make setting up a user or group	
Î	THEM D	service	Semire 1	Protocol	enables you to customize the services and	
	-	æ	autorine .	(100001	protocols that are displayed.	
		2	eon-proxy			
	5	-			This list has two sections:	
i.					TACACS+ Services. This section includes the most	
-			Submit Carcal	<u>.</u>	commonly used services and protocols for	
			Containe Solicer		TACACS+ 2	
			100		internet in the second s	

- 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



O que o usuário vê

O usuário tenta procurar algo no outro lado do firewall.

Uma janela é exibida com esta mensagem:

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