Implementación de Autenticación Proxy

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Cómo implementar el servidor alterno de autenticación Perfiles del servidor Cisco Secure UNIX (TACACS+) Cisco Secure Windows (TACACS+) Lo que el usuario ve Información Relacionada

Introducción

El proxy de autenticación (auth-proxy), disponible en Cisco IOS® Software Firewall versión 12.0.5.T y posteriores, se utiliza para autenticar usuarios entrantes, salientes o ambos. Estos usuarios se bloquean normalmente mediante una lista de acceso. Sin embargo, con auth-proxy, los usuarios abren un navegador para atravesar el el firewall y autenticarse en un servidor TACACS+ o RADIUS. El servidor distribuye entradas de listas de acceso adicionales para el router a través del cual se permite a los usuarios luego de la autenticación.

Este documento proporciona al usuario consejos generales para la implementación de auth-proxy, proporciona algunos perfiles de servidor Cisco Secure para auth proxy y describe lo que el usuario ve cuando auth-proxy está en uso.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

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

Cómo implementar el servidor alterno de autenticación

Complete estos pasos:

- 1. Asegúrese de que el tráfico fluye correctamente a través del firewall antes de configurar auth-proxy.
- 2. Para minimizar los trastornos ocasionados a la red durante las pruebas, modifique la lista de acceso existente para que deniegue el acceso a un cliente de prueba.
- 3. Asegúrese de que un cliente de prueba no pueda atravesar el firewall y que los otros hosts sí puedan hacerlo.
- 4. Active debug con **exec-timeout 0 0** en el puerto de la consola o en los terminales de tipo virtual (VTY), mientras agrega los comandos y la prueba **auth-proxy**.

Perfiles del servidor

Nuestras pruebas se realizaron con Cisco Secure UNIX y Windows. Si RADIUS está en uso, el servidor RADIUS debe soportar atributos específicos del proveedor (atributo 26). A continuación, ejemplos 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 procedimiento.

- 1. Introduzca el nombre de usuario y la contraseña (base de datos de Cisco Secure o Windows).
- 2. Para Configuración de la Interfaz, seleccione TACACS+.
- En New Services, seleccione la opción Group y escriba auth-proxy en la columna Service. Deje la columna Protocol (Protocolo) en blanco.

EscoSecure ACS for Windows 2000/hT - Microsoft Internet Explorer provided by Cisco IT Packaged # 5.5 SPL			541
File Edit View P	avontes Tools He		
de Back + -+) 13 G (3500	h ⊴Pavortes giftatory b∆• c) ₩ • c) ½	
interest (C) http://t.72	.18.124.145(1857)/nde	national (C)	- Crica (Lina "
ser gre s	20	Stearch web . With the second se	
Cisco Sestems	Interface Configuration		
adheadhea	Edit Help		
Mail Uper			
Lig Setup	TACACS+ (Cisco)		TACACS+ (Cisco)
Setup	Advanced Configuration Options		Advanced Configuration Options
and Network			
Surface Configuration	TACACS+ Services		TACACS+ (Cisco)
	User Group		
Enformation		ppp Ip	Sector in a stability of a stability of the State State State
OB Landstruter		PPP IPY	Select the check box for either User and/or
Control		PPP Multilink	Group for each TACACS+ service that you want
External Uper		PPP Annle Talk	Setup and/or Group Setup window, accordingly
Reports and		PPP VPDN	For correct operation, each protocol/service must
Activity		PPP LCP	be supported by the NAS. When you have
Decementation		ARAP	finished selecting options, click Submit.
	9 9	Shell (eyec)	It is unlikely that you will use every service and
		SLIP	protocol available for TACACS+. Displaying
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Sec. V	each would make setting up a user or group
	New Services		cumbersome. To simplify setup, this section
		Service Protocol	enables you to customize the services and
		euth-proxy	protocols that are displayed.
			This list has two sections:
	0 0		
			TACACS+ Services. This section includes the most
		Submit Cancel	commonly used services and protocols for
one			i i at at at a
Start 11-4 -81.5		🖬 📾 🛱 💋 🔢 🕅 Manton Halar 🔤 Stitter - Orthod 🗌	Billioidefenes Billioidefening Billionaterran B Sch 9 20 strate

- 4. Avanzada mostrar ventana para cada servicio atributos personalizados.
- 5. En Group Settings, verifique auth-proxy e ingrese esta información en la ventana:

```
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 procedimiento.

- 1. Abra Network Configuration (Configuración de red). NAS debe ser Cisco RADIUS.
- 2. Si la configuración de interfaz RADIUS está disponible, marque las casillas VSA.
- 3. En User Settings (Configuración de usuario), introduzca el nombre de usuario/la contraseña.
- 4. En Group Settings (configuración de grupos), seleccione la opción para [009/001] cisco-avpair. En el cuadro de texto debajo de la selección, escriba lo siguiente:

```
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 ventana es un ejemplo de este



Lo que el usuario ve

El usuario intenta examinar algo del otro lado del firewall.

Se muestra una ventana con este mensaje:

Authentication Proxy Username: Password: Si el nombre de usuario y la contraseña son correctos, el usuario verá:

Cisco Systems Authentication Successful! Si falla la autenticación, el mensaje es:

Cisco Systems Authentication Failed!

Información Relacionada

- Página de soporte de firewall de IOS
- Soporte Técnico y Documentación Cisco Systems