Implementación de Autenticación Proxy

Contenido

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 da a usuario las recomendaciones generales para la implementación del auténtico-proxy, proporciona algunos perfiles del Servidor seguro Cisco para el proxy del auth, y describe lo que ve el usuario cuando el auténtico-proxy es funcionando.

prerrequisitos

Requisitos

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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones

de Consejos Técnicos de Cisco.

Cómo implementar el proxy de autenticación

Complete estos pasos:

1. Aseegurese que los flujos de tráfico correctamente con el Firewall antes de que usted configure el auténtico-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. Gire el debug con el EXEC-**descanso 0 0** bajo el puerto de la consola o terminales de tipo virtual (vtys), mientras que usted agrega los **comandos auth-proxy** y la prueba.

Perfiles del servidor

Nuestra prueba fue hecha con Cisco UNIX seguro y Windows. Si RADIUS está en uso, el servidor RADIUS debe soportar atributos específicos del proveedor (atributo 26). A continuación, ejemplos de servidores específicos:

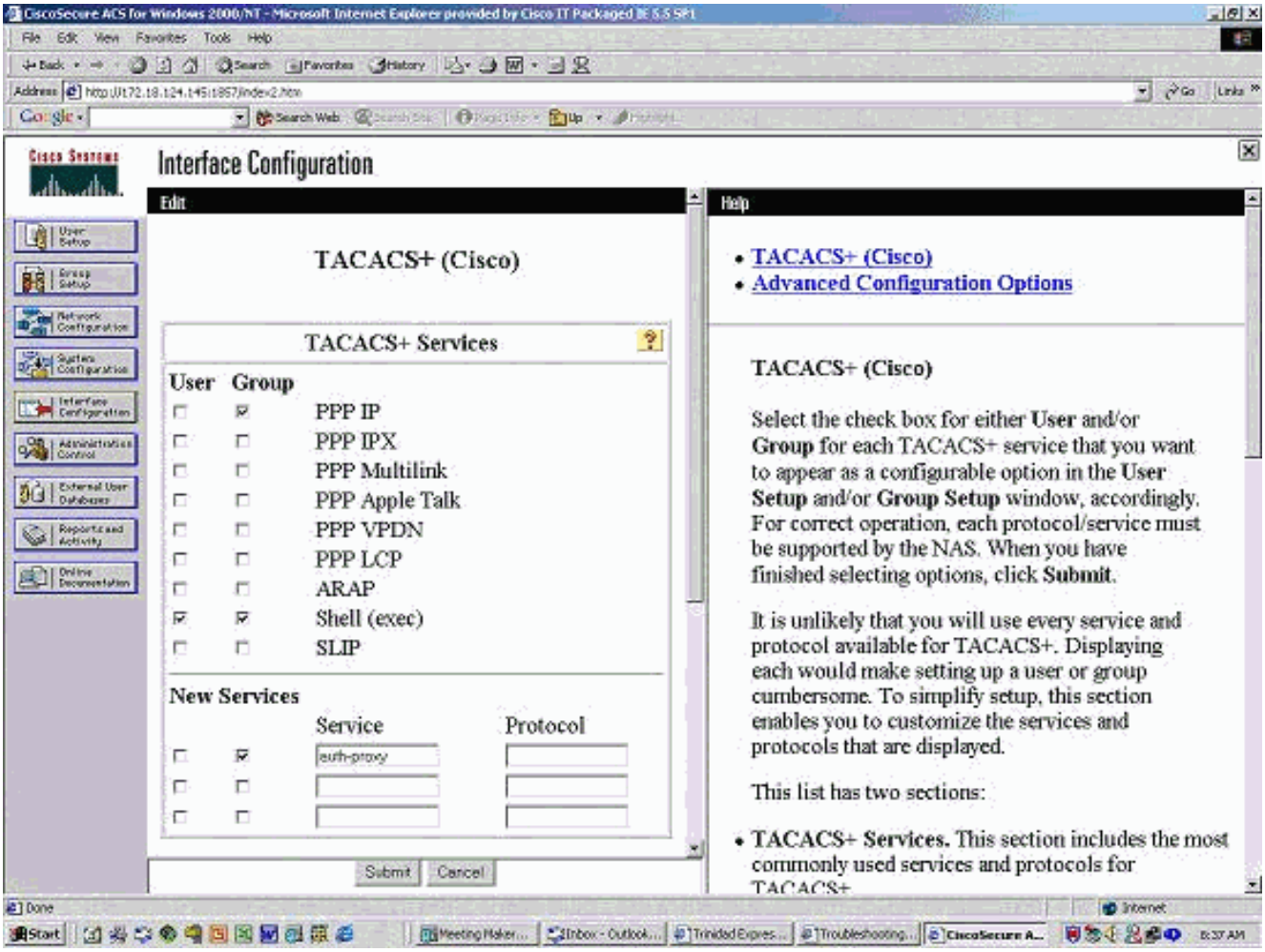
Cisco UNIX seguro (TACACS+)

```
# ./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 procedimiento.

1. Ingrese el nombre de usuario y contraseña (Cisco seguro o base de datos de Windows).
2. Para la configuración de la interfaz, seleccione el **TACACS+**.
3. Bajo nuevos servicios, seleccione la opción del **grupo** y teclee el auténtico-**proxy** en la columna del servicio. Deje la columna Protocol (Protocolo) en blanco.



4. Avanzada - mostrar ventana para cada servicio - atributos personalizados.
5. En configuraciones de grupo, el auténtico-**proxy del** control y ingresa 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 UNIX seguro (RADIUS)

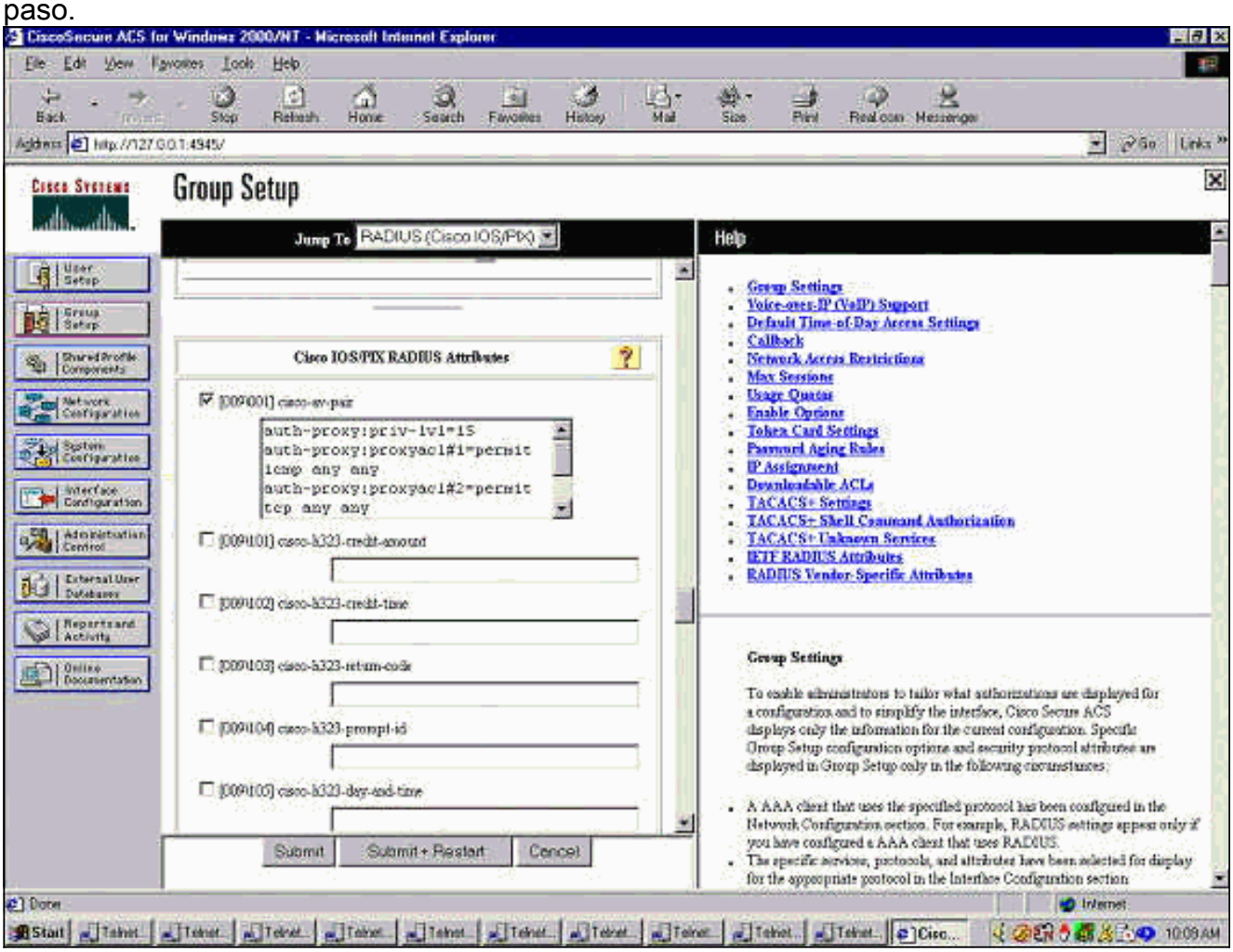
```
# ./ViewProfile -p 9900 -u proxy
User Profile Information
user = proxy{
profile_id = 58
profile_cycle = 1
radius=Cisco {
check_items= {
2="proxy"
}
reply_attributes= {
9,1="auth-proxy:priv-lvl=15"
9,1="auth-proxy:proxyacl#1=permit icmp any any"
9,1="auth-proxy:proxyacl#2=permit tcp any any"
9,1="auth-proxy:proxyacl#3=permit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

}
```

Cisco Windows seguro (RADIUS)

Siga este procedimiento.

1. Configuración de red abierta. NAS debe ser Cisco RADIUS.
2. Si la configuración de la interfaz RADIUS está disponible, marque los cuadros **VSA**.
3. En los ajustes de usuario, ingrese el nombre de usuario/la contraseña.
4. En Group Settings (configuración de grupos), seleccione la opción para [009/001] cisco-av-pair. En el cuadro de texto por debajo la selección, teclee esto:
   `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
   paso.



Lo que el usuario ve

El usuario intenta hojear algo en el otro lado del Firewall.

Visualizaciones de una ventana con este mensaje:

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

Si el nombre de usuario y la contraseña son correctos, el usuario verá:

```
Cisco Systems
Authentication Successful!
```

Si la autenticación falla, el mensaje es:

```
Cisco Systems
Authentication Failed!
```

Información Relacionada

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