Control de acceso basado en Role del Cisco IOS con el SDM: Separación del permiso de la configuración entre los grupos operativos

Contenido

Introducción

Las funciones de la encaminamiento y de la Seguridad se soportan tradicionalmente en los dispositivos diferentes, que ofrece una división clara de responsabilidad de administración entre la infraestructura de conexión en red y los Servicios de seguridad. La convergencia de la Seguridad y de la funcionalidad de ruteo en el Routers de los Servicios integrados de Cisco no ofrece esta separación clara, múltiple. Algunas organizaciones necesitan una segregación de la capacidad de la configuración restringir los clientes o a los grupos de administración del servicio a lo largo de los límites funcionales. Las opiniones CLI, una función del software de Cisco IOS®, intentan dirigir esta necesidad con el acceso basado en Role CLI. Este documento describe la configuración definida por el soporte del SDM del control de acceso basado en Role del Cisco IOS, y ofrece el fondo en las capacidades de las opiniones CLI de la interfaz de la línea de comandos del Cisco IOS.

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.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Muchas organizaciones delegan la responsabilidad del mantenimiento de la encaminamiento y de la Conectividad infraestructural a un grupo de operaciones de la red, y la responsabilidad del mantenimiento del Firewall, del VPN, y de las funciones de la prevención de intrusiones a un grupo de operaciones de la Seguridad. Las opiniones CLI pueden restringir la configuración y la capacidad de monitoreo de las funciones de la Seguridad al grupo de los secops, y restringen inversamente la conectividad de red, la encaminamiento, y otras tareas infraestructurales al grupo de los netops.

Algunos proveedores de servicio quieren ofrecer la configuración o la capacidad limitada de la supervisión a los clientes, pero no permitir que los clientes configuren o que vean las configuraciones del otro dispositivo. De nuevo, las opiniones CLI ofrecen el control granular sobre la capacidad CLI para restringir los usuarios o a los grupos de usuarios para ejecutar solamente los comandos autorizados.

El Cisco IOS Software ha ofrecido una capacidad para restringir los comandos CLI con un servidor para autorización TACACS+ a la capacidad del permit or deny de ejecutar los comandos CLI basados en la calidad de miembro del nombre de usuario o de grupo de usuarios. Las opiniones CLI ofrecen la capacidad similar, pero el control de políticas es aplicado por el dispositivo local después de que la opinión especificada el usuario se reciba del servidor de AAA. Cuando se utiliza la autorización del comando aaa, cada comando se debe autorizar individualmente por el servidor de AAA, que causa el diálogo frecuente entre el dispositivo y el servidor de AAA. Las opiniones CLI permiten el control de políticas del por-dispositivo CLI, mientras que la autorización del comando aaa aplica la misma directiva del comando authorization a todos los dispositivos los accesos del usuario.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Asocie a los usuarios a una visión

Los usuarios pueden ser asociados a una opinión local CLI por un atributo de vuelta del AAA o en configuración de la autenticación local. Para la configuración local, el nombre de usuario se configura con una opción adicional de la **visión**, que hace juego el **nombre a visualizar** configurado del **analizador de sintaxis**. Configuran a estos usuarios del ejemplo para las opiniones predeterminadas del SDM:

```
username fw-user privilege [privilege-level] view SDM_Firewall
username monitor-user privilege [privilege-level] view SDM_Monitor
username vpn-user privilege [privilege-level] view SDM_EasyVPN_Remote
username sdm-root privilege [privilege-level] view root
```

Los usuarios que se asignan a una visión dada pueden conmutar temporalmente a otra visión si tienen la contraseña para la visión que quieren ingresar. Publique este comando exec para cambiar las opiniones:

```
enable view view-name
```

Configuración de la opinión del analizador de sintaxis

Las opiniones CLI se pueden configurar del router CLI, o con el SDM. El SDM proporciona el soporte estático para cuatro opiniones, como se debate en la sección de soporte de las opiniones del SDM CLI. Para configurar la opinión CLI de la interfaz de la línea de comandos, un usuario debe ser definido como usuario de la opinión de la **raíz**, o deben pertenecer para ver con el acceso a la configuración de la **opinión del analizador de sintaxis**. Los usuarios que no se asocian a una visión y que intentan configurar las opiniones reciben este mensaje:

```
router(config#parser view test-view
No view Active! Switch to View Context
```

Las opiniones CLI permiten la inclusión o exclusión de las jerarquías del comando complete para el ejecutivo y los modos de configuración, o solamente las porciones de eso. Tres opciones están disponibles permitir o rechazar un comando o una jerarquía del comando en una visión dada:

```
router(config-view)#commands configure ?
  exclude            Exclude the command from the view
  include            Add command to the view
  include-exclusive  Include in this view but exclude from others
```

Las opiniones CLI truncan los ejecutar-config así que la configuración de la opinión del analizador de sintaxis no se visualiza. Sin embargo, la configuración de la opinión del analizador de sintaxis es visible en los lanzamiento-config.

Refiera al acceso basado en Role CLI para más información sobre la definición de la visión.

Verificar la asociación de la opinión del analizador de sintaxis

Los usuarios que se asignan a una opinión del analizador de sintaxis pueden determinar que los ven se asignan a cuando los abren una sesión a un router. Si se permite al **comando view del analizador de sintaxis de la demostración** para las opiniones de usuarios, pueden publicar el **comando view del analizador de sintaxis de la demostración** para determinar su opinión:

```
router#sh parser view
Current view is 'SDM_Firewall'
```

Soporte de las opiniones del SDM CLI

El SDM ofrece tres vistas predeterminadas, dos para la configuración y la supervisión del Firewall y de los componentes VPN, y una opinión restringida de la supervisión-solamente. Una opinión predeterminada adicional de la **raíz** está disponible en el SDM también.

El SDM no proporciona la capacidad de modificar los comandos incluidos adentro o excluidos de cada vista predeterminada, y no ofrece ninguna capacidad para definir las opiniones adicionales. Si las opiniones adicionales se definen del CLI, el SDM no ofrece las visiones adicionales en el panel de su configuración de las **cuentas de usuario/de las opiniones**.

Estas opiniones y permisos respectivos del comando se predefinen para el SDM:

Opinión de SDM_Firewall

```
parser view SDM_Firewall
 secret 5 $1$w/cD$T1ryjKM8aGCnIaKSm.Cx9/
 commands interface include all ip inspect
 commands interface include all ip verify
 commands interface include all ip access-group
 commands interface include ip
 commands interface include description
 commands interface include all no ip inspect
 commands interface include all no ip verify
 commands interface include all no ip access-group
 commands interface include no ip
 commands interface include no description
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include all ip access-list
 commands configure include all interface
 commands configure include all zone-pair
 commands configure include all zone
 commands configure include all policy-map
 commands configure include all class-map
 commands configure include all parameter-map
 commands configure include all appfw
 commands configure include all ip urlfilter
 commands configure include all ip inspect
 commands configure include all ip port-map
 commands configure include ip cef
 commands configure include ip
 commands configure include all crypto
 commands configure include no end
 commands configure include all no access-list
 commands configure include all no ip access-list
 commands configure include all no interface
 commands configure include all no zone-pair
```

```
 commands configure include all no zone
 commands configure include all no policy-map
 commands configure include all no class-map
 commands configure include all no parameter-map
 commands configure include all no appfw
 commands configure include all no ip urlfilter
 commands configure include all no ip inspect
 commands configure include all no ip port-map
 commands configure include no ip cef
 commands configure include no ip
 commands configure include all no crypto
 commands configure include no
 commands exec include all vlan
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

Opinión de SDM_EasyVPN_Remote

```
parser view SDM_EasyVPN_Remote
 secret 5 $1$UnC3$ienYd0L7Q/9xfCNkBQ4Uu.
 commands interface include all crypto
 commands interface include all no crypto
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include ip radius source-interface
 commands configure include ip radius
 commands configure include all ip nat
 commands configure include ip dns server
 commands configure include ip dns
 commands configure include all interface
 commands configure include all dot1x
 commands configure include all identity policy
 commands configure include identity profile
 commands configure include identity
 commands configure include all ip domain lookup
 commands configure include ip domain
 commands configure include ip
 commands configure include all crypto
 commands configure include all aaa
 commands configure include default end
 commands configure include all default access-list
 commands configure include default ip radius source-interface
 commands configure include default ip radius
 commands configure include all default ip nat
```

```
 commands configure include default ip dns server
 commands configure include default ip dns
 commands configure include all default interface
 commands configure include all default dot1x
 commands configure include all default identity policy
 commands configure include default identity profile
 commands configure include default identity
 commands configure include all default ip domain lookup
 commands configure include default ip domain
 commands configure include default ip
 commands configure include all default crypto
 commands configure include all default aaa
 commands configure include default
 commands configure include no end
 commands configure include all no access-list
 commands configure include no ip radius source-interface
 commands configure include no ip radius
 commands configure include all no ip nat
 commands configure include no ip dns server
 commands configure include no ip dns
 commands configure include all no interface
 commands configure include all no dot1x
 commands configure include all no identity policy
 commands configure include no identity profile
 commands configure include no identity
 commands configure include all no ip domain lookup
 commands configure include no ip domain
 commands configure include no ip
 commands configure include all no crypto
 commands configure include all no aaa
 commands configure include no
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include no
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

Opinión de SDM_Monitor

```
parser view SDM_Monitor
 secret 5 $1$RDYW$OABbxSgtx1kOozLlkBeJ9/
 commands configure include end
 commands configure include all interface
 commands configure include no end
 commands configure include all no interface
 commands exec include dir all-filesystems
 commands exec include dir
```

```
commands exec include all crypto ipsec client ezvpn
commands exec include crypto ipsec client
commands exec include crypto ipsec
commands exec include crypto
commands exec include all ping ip
commands exec include ping
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Acceso CLI Basado en Función
- Soporte Técnico y Documentación - Cisco Systems