CS 3.x: Permisos del usuario y papeles de la configuración

Contenido

Introducción

Este documento describe cómo configurar los permisos y los papeles a los usuarios en el Cisco Security Manager (CS).

prerrequisitos

Requisitos

Este documento asume que el CS está instalado y trabaja correctamente.

Componentes Utilizados

La información en este documento se basa en el CS 3.1.

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Configure los permisos del usuario

El Cisco Security Manager autentica su nombre de usuario y contraseña antes de que usted pueda iniciar sesión. Después de que se autentiquen, el administrador de seguridad establece su papel dentro de la aplicación. Este papel define sus permisos (privilegios también llamados), que son el conjunto de las tareas o las operaciones que le autorizan para realizarse. Si usted no es con certeza tareas o dispositivos autorizados, se ocultan o se inhabilitan los elementos de menú relacionados, los elementos TOC, y los botones. Además, un mensaje le dice que usted no tiene permiso para ver la información seleccionada o para realizar la operación seleccionada.

La autenticación y autorización para el administrador de seguridad es manejada por Servidor CiscoWorks o el Cisco Secure Access Control Server (ACS). Por abandono, los CiscoWorks manejan la autenticación y autorización, pero usted puede cambiar al Cisco Secure ACS usando la página de configuración del modo AAA en el CiscoWorks Common Services.

Las ventajas principales de usar el Cisco Secure ACS son la capacidad de crear los rol del usuario altamente granulares con los conjuntos especializados de los permisos (por ejemplo, permitiendo que el usuario configure cierta directiva teclea pero no otras) y la capacidad de restringir a los usuarios a ciertos dispositivos configurando los grupos de dispositivos de red (NDGs).

Los temas siguientes describen los permisos del usuario:

- Permisos del administrador de seguridad
- Comprensión de los papeles de los CiscoWorks
- Comprensión de los papeles del Cisco Secure ACS
- Asociaciones predeterminadas entre los permisos y los papeles en el administrador de seguridad

Permisos del administrador de seguridad

El administrador de seguridad clasifica los permisos en las categorías como se muestra:

1. **Visión** — Permite que usted vea las configuraciones actuales. Para más información, vea los permisos de la visión.
2. **Modifiqúese** — Permite que usted cambie las configuraciones actuales. Para más información, vea para modificar los permisos.
3. **Asigne** — Permite que usted asigne las directivas a los dispositivos y a las topologías VPN. Para más información, vea para asignar los permisos
4. **Apruebe** — Permite que usted apruebe los cambios de política y los trabajos del despliegue.

Para más información, vea para aprobar los permisos.

5. **Importación** — Permite que usted importe las configuraciones que se despliegan ya en los dispositivos en el administrador de seguridad.
6. **Despliegue** — Permite que usted despliegue los cambios de configuración a los dispositivos en su red y que realice la restauración no actualizada para volver a una configuración previamente desplegada.
7. **Control** — Permite que usted publique los comandos a los dispositivos, tales como ping.
8. **Someta** — Permite que usted someta sus cambios de configuración para la aprobación.

- Cuando usted selecciona modifique, asigne, apruebe, importe, controle o despliegue los permisos, usted debe también seleccionar los permisos correspondientes de la visión; si no, el administrador de seguridad no funcionará correctamente.
- Cuando usted selecciona modifique los permisos de la directiva, usted debe también seleccionar la correspondencia asigna y ve los permisos de la directiva.
- Cuando usted permite una directiva que utilice los objetos de la directiva como parte de su definición, usted debe también conceder los permisos de la visión a estos tipos de objeto. Por ejemplo, si usted selecciona el permiso para los políticas de ruteo de modificación, usted debe también seleccionar los permisos para ver los objetos de red e interconectar los papeles, que son los tipos de objeto requeridos por los políticas de ruteo.
- Lo mismo es verdad al permitir un objeto que utilice otros objetos como parte de su definición. Por ejemplo, si usted selecciona el permiso para los grupos de usuarios de modificación, usted debe también seleccionar los permisos para ver los objetos de red, los objetos ACL, y a los Grupos de servidores AAA.

Permisos de la visión

Los permisos (solo lecturas) de la visión en el administrador de seguridad se dividen en las categorías como se muestra:

- Permisos de las directivas de la visión
- Permisos de los objetos de visión
- Permisos adicionales de la visión

Permisos de las directivas de la visión

El administrador de seguridad incluye los permisos siguientes de la visión para las directivas:

1. **Visión > directivas > Firewall.** Permite que usted vea servicio de firewall las directivas (situadas en el selector de política bajo el Firewall) en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos servicio de firewall de las directivas incluyen las reglas de acceso, las reglas AAA, y las reglas del examen.
2. **Visión > directivas > sistema de prevención de intrusiones.** Permite que usted vea las directivas IPS (situadas en el selector de política bajo IPS), incluyendo las directivas para el IPS que se ejecuta en los routeres IOS.
3. **Visión > directivas > imagen.** Permite usted seleccione un paquete de la actualización de firma en el Asisitente de las actualizaciones IPS de la aplicación (situado bajo las herramientas > aplique la actualización IPS), pero no permite que usted asigne el paquete a los dispositivos específicos, a menos que usted también tenga el permiso de la modificación

> de las directivas > de la imagen.

4. **Visión > directivas > NAT**. Permite que usted vea las directivas de traducción de dirección de red en los dispositivos y los routeres IOS PIX/ASA/FWSM. Los ejemplos de las políticas NAT incluyen las reglas estáticas y las reglas dinámicas.
5. **Visión > directivas > VPN de sitio a sitio**. Permite que usted vea las directivas del VPN de sitio a sitio en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos de las directivas del VPN de sitio a sitio incluyen las ofertas de las propuestas IKE, del IPSec, y las claves del preshared.
6. **Visión > directivas > VPN de acceso remoto**. Permite que usted vea las directivas del VPN de acceso remoto en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos de las directivas del VPN de acceso remoto incluyen las ofertas de las propuestas IKE, del IPSec, y las directivas PKI.
7. **Visión > directivas > SSL VPN**. Permite que usted vea las políticas del VPN SSL en los dispositivos y los routeres IOS PIX/ASA/FWSM, tales como el Asistente VPN SSL.
8. **Visión > directivas > interfaces**. Permite que usted vea las directivas de la interfaz (situadas en el selector de política bajo interfaces) en los dispositivos PIX/ASA/FWSM, los routeres IOS, los sensores IPS, y los dispositivos del Catalyst 6500/7600.En los dispositivos PIX/ASA/FWSM, este permiso cubre los puertos de hardware y las configuraciones de la interfaz.En los routeres IOS, este permiso cubre las configuraciones básicas y avanzadas de la interfaz, así como otras directivas relacionadas a la interfaz, tales como DSL, PVC, PPP, y directivas del marcador.En los sensores IPS, este permiso cubre las interfaces físicas y las correspondencias del resumen.En los dispositivos del Catalyst 6500/7600, este permiso cubre las interfaces y las configuraciones de VLAN.
9. **Visión > directivas > bridging**. Permite que usted vea las directivas de la tabla ARP (situadas en el selector de política bajo la plataforma > bridging) en los dispositivos PIX/ASA/FWSM.
10. **Visión > directivas > Device Administration (Administración del dispositivo)**. Permite que usted vea Device Administration (Administración del dispositivo) las directivas (situadas en el selector de política bajo la plataforma > dispositivo Admin) en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, los ejemplos incluyen el acceso del dispositivo limpian, las directivas del acceso al servidor, y las directivas de la Conmutación por falla.En los routeres IOS, los ejemplos incluyen el acceso del dispositivo (línea incluyendo acceso) limpian, las directivas del acceso al servidor, AAA, y aseguran la disposición del dispositivo.En los sensores IPS, este permiso cubre las directivas del acceso del dispositivo y las directivas del acceso al servidor.En los dispositivos del Catalyst 6500/7600, este permiso cubre las configuraciones IDSM y las listas de acceso de VLAN.
11. **Visión > directivas > identidad**. Permite que usted vea las directivas de la identidad (situadas en el selector de política bajo la plataforma > identidad) en el Routers del Cisco IOS, incluyendo el 802.1x y las directivas del Network Admission Control (NAC).
12. **Visión > directivas > registro**. Permite que usted vea las directivas del registro (situadas en el selector de política bajo la plataforma > registro) en los dispositivos PIX/ASA/FWSM, los routeres IOS, y los sensores IPS. Los ejemplos de las directivas del registro incluyen la configuración del registro, la configuración de servidor, y las directivas del servidor de Syslog.
13. **Visión > directivas > Multicast**. Permite que usted vea las directivas del Multicast (situadas en el selector de política bajo la plataforma > Multicast) en los dispositivos PIX/ASA/FWSM. Los ejemplos de las directivas del Multicast incluyen el ruteo multicast y las directivas IGMP.

14. **Visión > directivas > QoS**. Permite que usted vea las directivas de QoS (situadas en el selector de política bajo la plataforma > calidad de servicio) en el Routers del Cisco IOS.
15. **Visión > directivas > encaminamiento**. Permite que usted vea los políticas de ruteo (situados en el selector de política bajo la plataforma > encaminamiento) en los dispositivos y los routeres IOS PIX/ASA/FWSM. Los ejemplos de los políticas de ruteo incluyen el OSPF, el RIP, y las directivas del Static Routing.
16. **> Security (Seguridad) de la visión > de las directivas**. Permite que usted vea las políticas de seguridad (situadas en el selector de política bajo el > Security (Seguridad) de la plataforma) en los dispositivos PIX/ASA/FWSM y los sensores IPS:En los dispositivos PIX/ASA/FWSM, las políticas de seguridad incluyen contra spoofing, el fragmento, y las configuraciones de tiempo de espera.En los sensores IPS, las políticas de seguridad incluyen el bloqueo de las configuraciones.
17. **Visión > directivas > reglas de la política de servicio**. Permite que usted vea las directivas de la regla de la política de servicio (situadas en el selector de política bajo reglas de la plataforma > de la política de servicio) en los dispositivos PIX 7.x/ASA. Los ejemplos incluyen las colas de administración del tráfico de prioridad e IPS, QoS, y las reglas de la conexión.
18. **Visión > directivas > preferencias del usuario**. Permite que usted vea la directiva del despliegue (situada en el selector de política bajo la plataforma > preferencias del usuario) en los dispositivos PIX/ASA/FWSM. Esta directiva contiene una opción para borrar todas las traducciones de NAT en el despliegue.
19. **Visión > directivas > dispositivo virtual**. Permite que usted vea las directivas virtuales del sensor en los dispositivos IPS. Esta directiva se utiliza para crear los sensores virtuales.
20. **Visión > directivas > FlexConfig**. Permite que usted vea FlexConfigs, que son los comandos CLI y las instrucciones adicionales que pueden ser desplegados a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600.

Permisos de los objetos de visión

El administrador de seguridad incluye los permisos siguientes de la visión para los objetos:

1. **La visión > se opone >AAA a los grupos de servidores**. Permite que usted vea los objetos del Grupo de servidores AAA. Estos objetos se utilizan en las directivas que requieren los servicios AAA (autenticación, autorización y contabilidad).
2. **La visión > se opone >AAA los servidores**. Permite que usted vea los objetos del servidor de AAA. Estos objetos representan a los servidores de AAA individuales que se definen como parte de un Grupo de servidores AAA.
3. **La visión > se opone > las listas de control de acceso - Estándar/extendió**. Permite que usted vea el estándar y el ACL ampliado se opone. Los objetos del ACL ampliado se utilizan para una variedad de directivas, tales como NAT y NAC, y para establecer el acceso VPN. Los objetos estándar ACL se utilizan para las directivas tales como el OSPF y el SNMP, así como para establecer el acceso VPN.
4. **La visión > se opone > las listas de control de acceso** - Red. Permite que usted vea los objetos de la red ACL. Los objetos de la red ACL se utilizan para realizar el filtrado de contenido en políticas del VPN SSL.
5. **La visión > se opone > los grupos de usuarios ASA**. Permite que usted vea los objetos del grupo de usuarios ASA. Estos objetos se configuran en los dispositivos de seguridad ASA en el VPN, el VPN de acceso remoto, y las configuraciones VPN fáciles SSL.

6. **La visión > se opone > las categorías**. Permite que usted vea los objetos de la categoría. Estos objetos le ayudan fácilmente a identificar las reglas y los objetos en las tablas de las reglas con el uso del color.
7. **La visión > se opone > las credenciales**. Permite que usted vea los objetos credenciales. Estos objetos se utilizan en la configuración VPN fácil durante el IKE Extended Authentication (Xauth).
8. **La visión > se opone > FlexConfigs**. Permite que usted vea los objetos de FlexConfig. Estos objetos, que contienen los comandos configuration con las instrucciones adicionales del lenguaje de la secuenciación de comandos, se pueden utilizar a los comandos configure que no son soportados por la interfaz de usuario del administrador de seguridad.
9. **> IKE Proposals de la visión > de los objetos**. Permite que usted vea los objetos de la propuesta IKE. Estos objetos contienen los parámetros requeridos para las propuestas IKE en las directivas del VPN de acceso remoto.
10. **La visión > los objetos > examinan - Correspondencias de la clase** - DNS. Permite que usted vea los objetos de la correspondencia de la clase DNS. Estos objetos hacen juego el tráfico DNS con los criterios específicos para poder realizarse las acciones en ese tráfico.
11. **La visión > los objetos > examinan - Correspondencias de la clase - FTP**. Permite que usted vea los objetos de la correspondencia de la clase FTP. Estos objetos hacen juego el tráfico FTP con los criterios específicos para poder realizarse las acciones en ese tráfico.
12. **La visión > los objetos > examinan - Correspondencias de la clase - HTTP**. Permite que usted vea los objetos de la correspondencia de la clase HTTP. Estos objetos hacen juego el tráfico HTTP con los criterios específicos para poder realizarse las acciones en ese tráfico.
13. **La visión > los objetos > examinan - Correspondencias de la clase - IM**. Permite que usted vea los objetos de la correspondencia de la clase IM. Tráfico de la coincidencia IM de estos objetos con los criterios específicos para poder realizarse las acciones en ese tráfico.
14. **La visión > los objetos > examinan - Correspondencias de la clase - SORBO**. Permite que usted vea los objetos de la correspondencia de la clase del SORBO. Estos objetos hacen juego el tráfico del SORBO con los criterios específicos para poder realizarse las acciones en ese tráfico.
15. **La visión > los objetos > examinan - Correspondencias de políticas - DNS.** Permite que usted vea los objetos de la correspondencia de políticas DNS. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico DNS.
16. **La visión > los objetos > examinan - Correspondencias de políticas - FTP.** Permite que usted vea los objetos de la correspondencia de políticas FTP. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico FTP.
17. **La visión > los objetos > examinan - Correspondencias de políticas - GTP**. Permite que usted vea los objetos de la correspondencia de políticas GTP. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico GTP.
18. **La visión > los objetos > examinan - Correspondencias de políticas - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite que usted vea los objetos de la correspondencia de la política HTTP creados para ASA/PIX los dispositivos 7.1.x y los routeres IOS. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico HTTP.
19. **La visión > los objetos > examinan - Correspondencias de políticas - HTTP (ASA7.2/PIX7.2)**. Permite que usted vea los objetos de la correspondencia de la política HTTP creados para los dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico HTTP.
20. **La visión > los objetos > examinan - Correspondencias de políticas - IM (ASA7.2/PIX7.2)**.

Permite que usted vea los objetos de la correspondencia de políticas IM creados para los dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear las correspondencias del examen para IM el tráfico.

21. **La visión > los objetos > examinan - Correspondencias de políticas - IM (IOS)**. Permite que usted vea los objetos de la correspondencia de políticas IM creados para los dispositivos IOS. Estos objetos se utilizan para crear las correspondencias del examen para IM el tráfico.
22. **La visión > los objetos > examinan - Correspondencias de políticas - SORBO**. Permite que usted vea los objetos de la correspondencia de políticas del SORBO. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico del SORBO.
23. **La visión > los objetos > examinan - Expresiones normales**. Permite que usted vea los objetos de la expresión normal. Estos objetos representan las expresiones normales individuales que se definen como parte de un grupo de la expresión normal.
24. **La visión > los objetos > examinan - Grupos de las expresiones normales**. Permite que usted vea los objetos del grupo de la expresión normal. Estos objetos son utilizados por ciertas correspondencias de la clase y examinan las correspondencias para hacer juego el texto dentro de un paquete.
25. **La visión > los objetos > examinan - El TCP asocia**. Permite que usted vea los objetos de la correspondencia TCP. Estos objetos personalizan el examen en el flujo TCP en las ambas direcciones.
26. **Visión > objetos > papeles de la interfaz**. Permite que usted vea los objetos del papel de la interfaz. Estos objetos definen los perfiles de nombre que pueden representar las interfaces múltiples en diversos tipos de dispositivos. Permiso de los papeles de la interfaz usted para aplicar las directivas a las interfaces específicas en los dispositivos múltiples sin tener que manualmente definir el nombre de cada interfaz.
27. **La visión > se opone > IPSec transforma los conjuntos**. Permite que usted vea el IPSec transforman los objetos determinados. Estos objetos comprenden una combinación de los protocolos de Seguridad, de los algoritmos y de otras configuraciones que especifican exactamente cómo los datos en el túnel IPsec serán cifrados y autenticados.
28. **La visión > se opone > las correspondencias del atributo LDAP**. Permite que usted vea los objetos de la correspondencia del atributo LDAP. Estos objetos se utilizan para asociar los nombres (definidos por el usario) de encargo del atributo a los nombres del atributo de Cisco LDAP.
29. **La visión > se opone > las redes/los host**. Permite que usted vea los objetos de la red/del host. Estos objetos son las recolecciones lógicas de los IP Addresses que representan las redes, los host, o ambos. Los objetos de la red/del host le permiten para definir las directivas sin especificar cada red o para recibirlas individualmente.
30. **La visión > se opone > las inscripciones PKI**. Permite que usted vea los objetos de la inscripción PKI. Estos objetos definen los servidores del Certification Authority (CA) que actúan dentro de un Public Key Infrastructure.
31. **Visión > objetos > listas de la expedición del puerto**. Permite que usted vea los objetos de la lista de la expedición del puerto. Estos objetos definen las asignaciones de los números del puerto en un cliente remoto a la dirección IP de la aplicación y viran hacia el lado de babor detrás de un gateway de VPN SSL.
32. **La visión > se opone > las configuraciones del Secure Desktop**. Permite que usted vea los objetos configurationes del Secure Desktop. Estos objetos son los componentes reutilizables, Nombrados que se pueden referir por las políticas del VPN SSL para proporcionar los medios confiables de eliminar todas las trazas de los datos vulnerables

que se comparten para la duración de una sesión de VPN SSL.

33. **> Services (Servicios) de la visión > de los objetos - Listas de puertos**. Permite que usted vea los objetos de la lista de puertos. Estos objetos, que contienen uno o más números de rangos de puertos, se utilizan para aerodinamizar el proceso de crear los objetos del servicio.
34. **La visión > el > Services (Servicios)/los grupos de servicios de los objetos** permite que usted vea los objetos del servicio y del grupo de servicios. Estos objetos son las asignaciones definidas del protocolo y de las definiciones del puerto que describen los servicios de red utilizados por las directivas, tales como Kerberos, SSH, y POP3.
35. **La visión > se opone > sola muestra en los servidores**. Permite que usted vea la sola muestra en los objetos del servidor. Escoja Muestra-en (SSO) deja a los usuarios de VPN SSL ingresar un nombre de usuario y contraseña una vez y poder acceder los servicios protegidos múltiplo y a los servidores Web.
36. **La visión > se opone > los monitores de SLA**. Permite que usted vea los objetos del monitor de SLA. Estos objetos son utilizados por los dispositivos de seguridad del PIX/ASA que funcionan con la versión 7.2 o posterior para realizar el seguimiento de la ruta. Esta característica proporciona un método para seguir la Disponibilidad de un ruta principal y para instalar una ruta de seguridad si el ruta principal falla.
37. **La visión > se opone > los arreglos para requisitos particulares SSL VPN**. Permite que usted vea los objetos del arreglo para requisitos particulares SSL VPN. Estos objetos definen cómo cambiar el aspecto de las páginas SSL VPN que se visualizan a los usuarios, tales como login/logout y Home Page.
38. **La visión > se opone > los gatewayes de VPN SSL**. Permite que usted vea los objetos del gateway de VPN SSL. Estos objetos definen los parámetros que habilitan el gateway que se utilizará como proxy para las conexiones a los recursos protegidos en su SSL VPN.
39. **La visión > se opone > los objetos del estilo**. Permite que usted vea los objetos del estilo. Estos objetos le dejan configurar los elementos styles, tales como características de la fuente y colores, para personalizar el aspecto de la página SSL VPN que aparece a los usuarios de VPN SSL cuando conectan con el dispositivo de seguridad.
40. **La visión > se opone > los objetos del texto**. Permite que usted vea los objetos del texto del formato libre. Estos objetos comprenden un par del nombre y del valor, donde el valor puede ser una sola cadena, una lista de cadenas, o una tabla de cadenas.
41. **La visión > se opone > los rangos de tiempo.** Permite que usted vea los objetos del rango de tiempo. Se utilizan estos objetos al crear el time basado ACL y las reglas del examen. También se utilizan al definir a los grupos de usuarios ASA para restringir el acceso VPN a los tiempos específicos durante la semana.
42. **La visión > se opone > los flujos de tráfico**. Permite que usted vea los objetos del flujo de tráfico. Estos objetos definen los flujos de tráfico específicos para uso de los dispositivos PIX 7.x/ASA 7.x.
43. **La visión > se opone > las listas url**. Permite que usted vea los objetos de la lista url. Estos objetos definen los URL que se visualizan en la página porta después de una registración satisfactoria. Esto permite a los usuarios para acceder los recursos disponibles en los sitios web SSL VPN al actuar en el modo de acceso del clientless.
44. **La visión > se opone > los grupos de usuarios**. Permite que usted vea los objetos del grupo de usuarios. Estos objetos definen a los grupos de clientes remotos que se utilicen en las topologías fáciles, los VPN de accesos remotos, y SSL VPN VPN.
45. **Visión > objetos > listas de servidores de los TRIUNFOS**. Permite que usted vea los objetos de la lista de servidores de los TRIUNFOS. Estos objetos representan los

servidores de los TRIUNFOS, que son utilizados por SSL VPN para acceder o para compartir los archivos en los sistemas remotos.

46. **La visión > se opone > las reglas del DN interno**. Permite que usted vea las reglas DN usadas por las directivas DN. Esto es un objeto interno usado por el administrador de seguridad que no aparece en el administrador del objeto de la directiva.
47. **La visión > se opone > las actualizaciones del cliente interno**. Éste es un objeto interno requerido por los objetos del grupo de usuarios que no aparece en el administrador del objeto de la directiva.
48. **La visión > se opone > interno - ACE estándar**. Esto es un objeto interno para las entradas de control de acceso estándar, que son utilizadas por los objetos ACL.
49. **La visión > se opone > interno - ACE extendidos.** Esto es un objeto interno para las entradas de control de acceso extendidas, que son utilizadas por los objetos ACL.

Permisos adicionales de la visión

El administrador de seguridad incluye los permisos adicionales siguientes de la visión:

1. **Visión > Admin**. Permite que usted vea las configuraciones administrativas del administrador de seguridad.
2. **Visión > CLI**. Permite que usted vea los comandos CLI configurados en un dispositivo y que vea los comandos de antemano que están a punto de ser desplegados.
3. **Visión > Archivo de configuración**. Permite que usted vea la lista de configuraciones contenidas en el archivo de configuración. Usted no puede ver la configuración del dispositivo o ninguna comandos CLI.
4. **Visión > dispositivos**. Permite que usted vea los dispositivos en la vista de dispositivo y toda la información relacionada, incluyendo sus configuraciones del dispositivo, las propiedades, las asignaciones, y así sucesivamente.
5. **Visión > administradores de dispositivo**. Permite que usted ponga en marcha las versiones solo lecturas de los administradores de dispositivo para los dispositivos individuales, tales como el (SDM) de Router de Cisco y Administrador de dispositivo de seguridad para el Routers del Cisco IOS.
6. **Visión > topología**. Permite que usted vea las correspondencias configuradas en la opinión del mapa.

Modifique los permisos

Modifique los permisos (de lectura/grabación) en el administrador de seguridad se dividen en las categorías como se muestra:

- Modifique los permisos de las directivas
- Modifique los permisos de los objetos
- Adicional modifique los permisos

Modifique los permisos de las directivas

Nota: Cuando usted especifica modifique los permisos de la directiva, se aseeguran que usted ha seleccionado la correspondencia asigna y ve los permisos de la directiva también.

El administrador de seguridad incluye el siguiente modifica los permisos para las directivas:

1. **Modifiqúese > las directivas > Firewall**. Permite que usted modifique servicio de firewall las directivas (situadas en el selector de política bajo el Firewall) en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos servicio de firewall de las directivas incluyen las reglas de acceso, las reglas AAA, y las reglas del examen.
2. **Modifiqúese > las directivas > sistema de prevención de intrusiones**. Permite que usted modifique las directivas IPS (situadas en el selector de política bajo IPS), incluyendo las directivas para el IPS que se ejecuta en los routeres IOS. Este permiso también permite que usted ajuste las firmas en el Asisitente de la actualización de firma (situado bajo las herramientas > aplique la actualización IPS).
3. **Modifiqúese > las directivas > imagen**. Permite que usted asigne un paquete de la actualización de firma a los dispositivos en el Asisitente de las actualizaciones IPS de la aplicación (situado bajo las herramientas > aplique la actualización IPS). Este permiso también permite que usted asigne las configuraciones autos de la actualización a los dispositivos específicos (situados bajo el control del administrador del Tools (Herramientas) > Security (Seguridad) > actualizaciones IPS).
4. **Modifiqúese > las directivas > NAT**. Permite que usted modifique las directivas de traducción de dirección de red en los dispositivos y los routeres IOS PIX/ASA/FWSM. Los ejemplos de las políticas NAT incluyen las reglas estáticas y las reglas dinámicas.
5. **Modifiqúese > las directivas > VPN de sitio a sitio**. Permite que usted modifique las directivas del VPN de sitio a sitio en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos de las directivas del VPN de sitio a sitio incluyen las ofertas de las propuestas IKE, del IPSec, y las claves del preshared.
6. **Modifiqúese > las directivas > VPN de acceso remoto**. Permite que usted modifique las directivas del VPN de acceso remoto en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos de las directivas del VPN de acceso remoto incluyen las ofertas de las propuestas IKE, del IPSec, y las directivas PKI.
7. **Modifiqúese > las directivas > SSL VPN**. Permite que usted modifique las políticas del VPN SSL en los dispositivos y los routeres IOS PIX/ASA/FWSM, tales como el Asistente VPN SSL.
8. **Modifiqúese > las directivas > las interfaces**. Permite que usted modifique las directivas de la interfaz (situadas en el selector de política bajo interfaces) en los dispositivos PIX/ASA/FWSM, los routeres IOS, los sensores IPS, y los dispositivos del Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, este permiso cubre los puertos de hardware y las configuraciones de la interfaz.En los routeres IOS, este permiso cubre las configuraciones básicas y avanzadas de la interfaz, así como otras directivas relacionadas a la interfaz, tales como DSL, PVC, PPP, y directivas del marcador.En los sensores IPS, este permiso cubre las interfaces físicas y las correspondencias del resumen.En los dispositivos del Catalyst 6500/7600, este permiso cubre las interfaces y las configuraciones de VLAN.
9. **Modifiqúese > las directivas > bridging**. Permite que usted modifique las directivas de la tabla ARP (situadas en el selector de política bajo la plataforma > bridging) en los dispositivos PIX/ASA/FWSM.
10. **Modifiqúese > las directivas > Device Administration (Administración del dispositivo)**. Permite que usted modifique Device Administration (Administración del dispositivo) las directivas (situadas en el selector de política bajo la plataforma > dispositivo Admin) en los dispositivos PIX/ASA/FWSM, los dispositivos de los routeres IOS, y del Catalyst

6500/7600:En los dispositivos PIX/ASA/FWSM, los ejemplos incluyen el acceso del dispositivo limpian, las directivas del acceso al servidor, y las directivas de la Conmutación por falla.En los routeres IOS, los ejemplos incluyen el acceso del dispositivo (línea incluyendo acceso) limpian, las directivas del acceso al servidor, AAA, y aseguran la disposición del dispositivo.En los sensores IPS, este permiso cubre las directivas del acceso del dispositivo y las directivas del acceso al servidor.En los dispositivos del Catalyst 6500/7600, este permiso cubre las configuraciones IDSM y la lista de acceso de VLAN.

11. **Modifiqúese > las directivas > identidad**. Permite que usted modifique las directivas de la identidad (situadas en el selector de política bajo la plataforma > identidad) en el Routers del Cisco IOS, incluyendo el 802.1x y las directivas del Network Admission Control (NAC).
12. **Modifiqúese > las directivas > registro**. Permite que usted modifique las directivas del registro (situadas en el selector de política bajo la plataforma > registro) en los dispositivos PIX/ASA/FWSM, los routeres IOS, y los sensores IPS. Los ejemplos de las directivas del registro incluyen la configuración del registro, la configuración de servidor, y las directivas del servidor de Syslog.
13. **Modifiqúese > las directivas > Multicast**. Permite que usted modifique las directivas del Multicast (situadas en el selector de política bajo la plataforma > Multicast) en los dispositivos PIX/ASA/FWSM. Los ejemplos de las directivas del Multicast incluyen el ruteo multicast y las directivas IGMP.
14. **Modifiqúese > las directivas > QoS**. Permite que usted modifique las directivas de QoS (situadas en el selector de política bajo la plataforma > calidad de servicio) en el Routers del Cisco IOS.
15. **Modifiqúese > las directivas > encaminamiento**. Permite que usted modifique los políticas de ruteo (situados en el selector de política bajo la plataforma > encaminamiento) en los dispositivos y los routeres IOS PIX/ASA/FWSM. Los ejemplos de los políticas de ruteo incluyen el OSPF, el RIP, y las directivas del Static Routing.
16. **Modifiqúese > > Security (Seguridad) de las directivas**. Permite que usted modifique las políticas de seguridad (situadas en el selector de política bajo el > Security (Seguridad) de la plataforma) en los dispositivos PIX/ASA/FWSM y los sensores IPS:En los dispositivos PIX/ASA/FWSM, las políticas de seguridad incluyen contra spoofing, el fragmento, y las configuraciones de tiempo de espera.En los sensores IPS, las políticas de seguridad incluyen el bloqueo de las configuraciones.
17. **Modifiqúese > las directivas > las reglas de la política de servicio**. Permite que usted modifique las directivas de la regla de la política de servicio (situadas en el selector de política bajo reglas de la plataforma > de la política de servicio) en los dispositivos PIX 7.x/ASA. Los ejemplos incluyen las colas de administración del tráfico de prioridad e IPS, QoS, y las reglas de la conexión.
18. **Modifiqúese > las directivas > las preferencias del usuario**. Permite que usted modifique la directiva del despliegue (situada en el selector de política bajo la plataforma > preferencias del usuario) en los dispositivos PIX/ASA/FWSM. Esta directiva contiene una opción para borrar todas las traducciones de NAT en el despliegue.
19. **Modifiqúese > las directivas > dispositivo virtual**. Permite que usted modifique las directivas virtuales del sensor en los dispositivos IPS. Utilice esta directiva para crear los sensores virtuales.
20. **Modifiqúese > las directivas > FlexConfig**. Permite que usted modifique FlexConfigs, que son los comandos CLI y las instrucciones adicionales que pueden ser desplegados a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600.

Modifique los permisos de los objetos

El administrador de seguridad incluye los permisos siguientes de la visión para los objetos:

1. **Modifiqúese > los grupos de servidores de los objetos >AAA**. Permite que usted vea los objetos del Grupo de servidores AAA. Estos objetos se utilizan en las directivas que requieren los servicios AAA (autenticación, autorización y contabilidad).
2. **Modifiqúese > los servidores de los objetos >AAA**. Permite que usted vea los objetos del servidor de AAA. Estos objetos representan a los servidores de AAA individuales que se definen como parte de un Grupo de servidores AAA.
3. **Modifiqúese > se opone > las listas de control de acceso - Estándar/extendió**. Permite que usted vea el estándar y el ACL ampliado se opone. Los objetos del ACL ampliado se utilizan para una variedad de directivas, tales como NAT y NAC, y para establecer el acceso VPN. Los objetos estándar ACL se utilizan para las directivas tales como el OSPF y el SNMP, así como para establecer el acceso VPN.
4. **Modifiqúese > se opone > las listas de control de acceso - Red**. Permite que usted vea los objetos de la red ACL. Los objetos de la red ACL se utilizan para realizar el filtrado de contenido en políticas del VPN SSL.
5. **Modifiqúese > se opone > los** grupos de usuarios **ASA**. Permite que usted vea los objetos del grupo de usuarios ASA. Estos objetos se configuran en los dispositivos de seguridad ASA en el VPN, el VPN de acceso remoto, y las configuraciones VPN fáciles SSL.
6. **Modifiqúese > se opone > las categorías**. Permite que usted vea los objetos de la categoría. Estos objetos le ayudan fácilmente a identificar las reglas y los objetos en las tablas de las reglas con el uso del color.
7. **Modifiqúese > se opone > las credenciales**. Permite que usted vea los objetos credenciales. Estos objetos se utilizan en la configuración VPN fácil durante el IKE Extended Authentication (Xauth).
8. **Modifiqúese > se opone > FlexConfigs**. Permite que usted vea los objetos de FlexConfig. Estos objetos, que contienen los comandos configuration con las instrucciones adicionales del lenguaje de la secuenciación de comandos, se pueden utilizar a los comandos configure que no son soportados por la interfaz de usuario del administrador de seguridad.
9. **Modifiqúese > > IKE Proposals de los objetos**. Permite que usted vea los objetos de la propuesta IKE. Estos objetos contienen los parámetros requeridos para las propuestas IKE en las directivas del VPN de acceso remoto.
10. **Modifiqúese > los objetos > examinan - Correspondencias de la clase - DNS**. Permite que usted vea los objetos de la correspondencia de la clase DNS. Estos objetos hacen juego el tráfico DNS con los criterios específicos para poder realizarse las acciones en ese tráfico.
11. **Modifiqúese > los objetos > examinan - Correspondencias de la clase - FTP**. Permite que usted vea los objetos de la correspondencia de la clase FTP. Estos objetos hacen juego el tráfico FTP con los criterios específicos para poder realizarse las acciones en ese tráfico.
12. **Modifiqúese > los objetos > examinan - Correspondencias de la clase - HTTP**. Permite que usted vea los objetos de la correspondencia de la clase HTTP. Estos objetos hacen juego el tráfico HTTP con los criterios específicos para poder realizarse las acciones en ese tráfico.
13. **Modifiqúese > los objetos > examinan - Correspondencias de la clase - IM**. Permite que usted vea los objetos de la correspondencia de la clase IM. Tráfico de la coincidencia IM de estos objetos con los criterios específicos para poder realizarse las acciones en ese tráfico.
14. **Modifiqúese > los objetos > examinan - Correspondencias de la clase - SORBO**. Permite

que usted vea los objetos de la correspondencia de la clase del SORBO. Estos objetos hacen juego el tráfico del SORBO con los criterios específicos para poder realizarse las acciones en ese tráfico.

15. **Modifiqúese > los objetos > examinan - Correspondencias de políticas - DNS**. Permite que usted vea los objetos de la correspondencia de políticas DNS. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico DNS.
16. **Modifiqúese > los objetos > examinan - Correspondencias de políticas - FTP**. Permite que usted vea los objetos de la correspondencia de políticas FTP. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico FTP.
17. **Modifiqúese > los objetos > examinan - Correspondencias de políticas - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite que usted vea los objetos de la correspondencia de la política HTTP creados para ASA/PIX los dispositivos 7.x y los routeres IOS. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico HTTP.
18. **Modifiqúese > los objetos > examinan - Correspondencias de políticas - HTTP (ASA7.2/PIX7.2)**. Permite que usted vea los objetos de la correspondencia de la política HTTP creados para los dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico HTTP.
19. **Modifiqúese > los objetos > examinan - Correspondencias de políticas - IM (ASA7.2/PIX7.2)**. Permite que usted vea los objetos de la correspondencia de políticas IM creados para los dispositivos ASA 7.2/PIX 7.2. Estos objetos se utilizan para crear las correspondencias del examen para IM el tráfico.
20. **Modifiqúese > los objetos > examinan - Correspondencias de políticas - IM (IOS)**. Permite que usted vea los objetos de la correspondencia de políticas IM creados para los dispositivos IOS. Estos objetos se utilizan para crear las correspondencias del examen para IM el tráfico.
21. **Modifiqúese > los objetos > examinan - Correspondencias de políticas - SORBO**. Permite que usted vea los objetos de la correspondencia de políticas del SORBO. Estos objetos se utilizan para crear las correspondencias del examen para el tráfico del SORBO.
22. **Modifiqúese > los objetos > examinan - Expresiones normales**. Permite que usted vea los objetos de la expresión normal. Estos objetos representan las expresiones normales individuales que se definen como parte de un grupo de la expresión normal.
23. **Modifiqúese > los objetos > examinan - Grupos de las expresiones normales**. Permite que usted vea los objetos del grupo de la expresión normal. Estos objetos son utilizados por ciertas correspondencias de la clase y examinan las correspondencias para hacer juego el texto dentro de un paquete.
24. **Modifiqúese > los objetos > examinan - El TCP asocia**. Permite que usted vea los objetos de la correspondencia TCP. Estos objetos personalizan el examen en el flujo TCP en las ambas direcciones.
25. **Modifiqúese > los objetos > los papeles de la interfaz**. Permite que usted vea los objetos del papel de la interfaz. Estos objetos definen los perfiles de nombre que pueden representar las interfaces múltiples en diversos tipos de dispositivos. Permiso de los papeles de la interfaz usted para aplicar las directivas a las interfaces específicas en los dispositivos múltiples sin tener que manualmente definir el nombre de cada interfaz.
26. **Modifiqúese > se opone > IPSec transforman los conjuntos**. Permite que usted vea el IPSec transforman los objetos determinados. Estos objetos comprenden una combinación de los protocolos de Seguridad, de los algoritmos y de otras configuraciones que especifican exactamente cómo los datos en el túnel IPsec serán cifrados y autenticados.
27. **Modifiqúese > se opone > las correspondencias del atributo LDAP**. Permite que usted vea

los objetos de la correspondencia del atributo LDAP. Estos objetos se utilizan para asociar los nombres (definidos por el usario) de encargo del atributo a los nombres del atributo de Cisco LDAP.

28. **Modifiqúese > se opone > las redes/los host**. Permite que usted vea los objetos de la red/del host. Estos objetos son las recolecciones lógicas de los IP Addresses que representan las redes, los host, o ambos. Los objetos de la red/del host le permiten para definir las directivas sin especificar cada red o para recibirlas individualmente.
29. **Modifiqúese > se opone > las inscripciones PKI**. Permite que usted vea los objetos de la inscripción PKI. Estos objetos definen los servidores del Certification Authority (CA) que actúan dentro de un Public Key Infrastructure.
30. **Modifiqúese > los objetos > las listas de la expedición del puerto**. Permite que usted vea los objetos de la lista de la expedición del puerto. Estos objetos definen las asignaciones de los números del puerto en un cliente remoto a la dirección IP de la aplicación y viran hacia el lado de babor detrás de un gateway de VPN SSL.
31. **Modifiqúese > se opone > las configuraciones del Secure Desktop**. Permite que usted vea los objetos configurationes del Secure Desktop. Estos objetos son los componentes reutilizables, Nombrados que se pueden referir por las políticas del VPN SSL para proporcionar los medios confiables de eliminar todas las trazas de los datos vulnerables que se comparten para la duración de una sesión de VPN SSL.
32. **Modifiqúese > > Services (Servicios) de los objetos - Listas de puertos**. Permite que usted vea los objetos de la lista de puertos. Estos objetos, que contienen uno o más números de rangos de puertos, se utilizan para aerodinamizar el proceso de crear los objetos del servicio.
33. **Modifiqúese > > Services (Servicios)/los grupos de servicios de los objetos.** Permite que usted vea el servicio y el grupo de servicios se opone. Estos objetos son las asignaciones definidas del protocolo y de las definiciones del puerto que describen los servicios de red utilizados por las directivas, tales como Kerberos, SSH, y POP3.
34. **Modifiqúese > se opone > sola muestra en los servidores.** Permite que usted vea la sola muestra en los objetos del servidor. Escoja Muestra-en (SSO) deja a los usuarios de VPN SSL ingresar un nombre de usuario y contraseña una vez y poder acceder los servicios protegidos múltiplo y a los servidores Web.
35. **Modifiqúese > se opone > los monitores de SLA**. Permite que usted vea los objetos del monitor de SLA. Estos objetos son utilizados por los dispositivos de seguridad del PIX/ASA que funcionan con la versión 7.2 o posterior para realizar el seguimiento de la ruta. Esta característica proporciona un método para seguir la Disponibilidad de un ruta principal y para instalar una ruta de seguridad si el ruta principal falla.
36. **Modifiqúese > se opone > los arreglos para requisitos particulares SSL VPN**. Permite que usted vea los objetos del arreglo para requisitos particulares SSL VPN. Estos objetos definen cómo cambiar el aspecto de las páginas SSL VPN que se visualizan a los usuarios, tales como login/logout y Home Page.
37. **Modifiqúese > se opone > los gatewayes de VPN SSL**. Permite que usted vea los objetos del gateway de VPN SSL. Estos objetos definen los parámetros que habilitan el gateway que se utilizará como proxy para las conexiones a los recursos protegidos en su SSL VPN.
38. **Modifiqúese > se opone > los objetos del estilo**. Permite que usted vea los objetos del estilo. Estos objetos le dejan configurar los elementos styles, tales como características de la fuente y colores, para personalizar el aspecto de la página SSL VPN que aparece a los usuarios de VPN SSL cuando conectan con el dispositivo de seguridad.
39. **Modifiqúese > se opone > los objetos del texto**. Permite que usted vea los objetos del texto

del formato libre. Estos objetos comprenden un par del nombre y del valor, donde el valor puede ser una sola cadena, una lista de cadenas, o una tabla de cadenas.

40. **Modifiqúese > se opone > los rangos de tiempo.** Permite que usted vea los objetos del rango de tiempo. Se utilizan estos objetos al crear el time basado ACL y las reglas del examen. También se utilizan al definir a los grupos de usuarios ASA para restringir el acceso VPN a los tiempos específicos durante la semana.
41. **Modifiqúese > se opone > los flujos de tráfico**. Permite que usted vea los objetos del flujo de tráfico. Estos objetos definen los flujos de tráfico específicos para uso de los dispositivos PIX 7.x/ASA 7.x.
42. **Modifiqúese > se opone > las listas url**. Permite que usted vea los objetos de la lista url. Estos objetos definen los URL que se visualizan en la página porta después de una registración satisfactoria. Esto permite a los usuarios para acceder los recursos disponibles en los sitios web SSL VPN al actuar en el modo de acceso del clientless.
43. **Modifiqúese > se opone > los grupos de usuarios**. Permite que usted vea los objetos del grupo de usuarios. Estos objetos definen a los grupos de clientes remotos que se utilicen en las topologías fáciles, los VPN de accesos remotos, y SSL VPN VPN
44. **Modifiqúese > los objetos > las listas de servidores de los TRIUNFOS**. Permite que usted vea los objetos de la lista de servidores de los TRIUNFOS. Estos objetos representan los servidores de los TRIUNFOS, que son utilizados por SSL VPN para acceder o para compartir los archivos en los sistemas remotos.
45. **Modifiqúese > se opone > las reglas del DN interno.** Permite que usted vea las reglas DN usadas por las directivas DN. Esto es un objeto interno usado por el administrador de seguridad que no aparece en el administrador del objeto de la directiva.
46. **Modifiqúese > se opone > las actualizaciones del cliente interno**. Éste es un objeto interno requerido por los objetos del grupo de usuarios que no aparece en el administrador del objeto de la directiva.
47. **Modifiqúese > se opone > interno - ACE estándar**. Esto es un objeto interno para las entradas de control de acceso estándar, que son utilizadas por los objetos ACL.
48. **Modifiqúese > se opone > interno - ACE extendido**. Esto es un objeto interno para las entradas de control de acceso extendidas, que son utilizadas por los objetos ACL.

Adicional modifique los permisos

El administrador de seguridad incluye el adicional modifica los permisos como se muestra:

1. **Modifiqúese > Admin**. Permite que usted modifique las configuraciones administrativas del administrador de seguridad.
2. **Modifiqúese > Archivo de configuración**. Permite que usted modifique la configuración del dispositivo en el archivo de configuración. Además, permite que usted agregue las configuraciones al archivo y que personalice la herramienta del archivo de configuración.
3. **Modifiqúese > los dispositivos**. Permite que usted agregue y que borre los dispositivos, así como modifica las propiedades y los atributos del dispositivo. Para descubrir las directivas en el dispositivo que es agregado, usted debe también habilitar el permiso de la importación. Además, si usted habilita el permiso de la modificación > de los dispositivos, aseegurese que usted también habilita el permiso de la asignación > de las directivas > de las interfaces.
4. **Modifiqúese > jerarquía**. Permite que usted modifique los grupos de dispositivos.
5. **Modifiqúese > topología**. Permite que usted modifique las correspondencias en la opinión del mapa.

Asigne los permisos

El administrador de seguridad incluye los permisos de la asignación de la directiva como se muestra:

1. **Asigne > las directivas > Firewall**. Permite que usted asigne servicio de firewall las directivas (situadas en el selector de política bajo el Firewall) a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos servicio de firewall de las directivas incluyen las reglas de acceso, las reglas AAA, y las reglas del examen.
2. **Asigne > las directivas > sistema de prevención de intrusiones**. Permite que usted asigne las directivas IPS (situadas en el selector de política bajo IPS), incluyendo las directivas para el IPS que se ejecuta en los routeres IOS.
3. **Asigne > las directivas > imagen**. Este permiso no es utilizado actualmente por el administrador de seguridad.
4. **Asigne > las directivas > NAT**. Permite que usted asigne las directivas de traducción de dirección de red a los dispositivos y a los routeres IOS PIX/ASA/FWSM. Los ejemplos de las políticas NAT incluyen las reglas estáticas y las reglas dinámicas.
5. **Asigne > las directivas > VPN de sitio a sitio**. Permite que usted asigne las directivas del VPN de sitio a sitio a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos de las directivas del VPN de sitio a sitio incluyen las ofertas de las propuestas IKE, del IPSec, y las claves del preshared.
6. **Asigne > las directivas > VPN de acceso remoto**. Permite que usted asigne las directivas del VPN de acceso remoto a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600. Los ejemplos de las directivas del VPN de acceso remoto incluyen las ofertas de las propuestas IKE, del IPSec, y las directivas PKI.
7. **Asigne > las directivas > SSL VPN**. Permite que usted asigne las políticas del VPN SSL a los dispositivos y a los routeres IOS PIX/ASA/FWSM, tales como el Asistente VPN SSL.
8. **Asigne > las directivas > las interfaces**. Permite que usted asigne las directivas de la interfaz (situadas en el selector de política bajo interfaces) a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, este permiso cubre los puertos de hardware y las configuraciones de la interfaz.En los routeres IOS, este permiso cubre las configuraciones básicas y avanzadas de la interfaz, así como otras directivas relacionadas a la interfaz, tales como DSL, PVC, PPP, y directivas del marcador.En los dispositivos del Catalyst 6500/7600, este permiso cubre las interfaces y las configuraciones de VLAN.
9. **Asigne > las directivas > bridging**. Permite que usted asigne las directivas de la tabla ARP (situadas en el selector de política bajo la plataforma > bridging) a los dispositivos PIX/ASA/FWSM.
10. **Asigne > las directivas > Device Administration (Administración del dispositivo)**. Permite que usted asigne Device Administration (Administración del dispositivo) las directivas (situadas en el selector de política bajo la plataforma > dispositivo Admin) a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600:En los dispositivos PIX/ASA/FWSM, los ejemplos incluyen el acceso del dispositivo limpian, las directivas del acceso al servidor, y las directivas de la Conmutación por falla.En los routeres IOS, los ejemplos incluyen el acceso del dispositivo (línea incluyendo acceso) limpian, las directivas del acceso al servidor, AAA, y aseguran la disposición del dispositivo.En los sensores IPS, este permiso cubre las directivas del acceso del dispositivo y las directivas del acceso al servidor.En los dispositivos del Catalyst 6500/7600, este

permiso cubre las configuraciones IDSM y las listas de acceso de VLAN.

11. **Asigne > las directivas > identidad**. Permite que usted asigne las directivas de la identidad (situadas en el selector de política bajo la plataforma > identidad) al Routers del Cisco IOS, incluyendo el 802.1x y las directivas del Network Admission Control (NAC).
12. **Asigne > las directivas > registro**. Permite que usted asigne las directivas del registro (situadas en el selector de política bajo la plataforma > registro) a los dispositivos y a los routeres IOS PIX/ASA/FWSM. Los ejemplos de las directivas del registro incluyen la configuración del registro, la configuración de servidor, y las directivas del servidor de Syslog.
13. **Asigne > las directivas > Multicast**. Permite que usted asigne las directivas del Multicast (situadas en el selector de política bajo la plataforma > Multicast) a los dispositivos PIX/ASA/FWSM. Los ejemplos de las directivas del Multicast incluyen el ruteo multicast y las directivas IGMP.
14. **Asigne > las directivas > QoS**. Permite que usted asigne las directivas de QoS (situadas en el selector de política bajo la plataforma > calidad de servicio) al Routers del Cisco IOS.
15. **Asigne > las directivas > encaminamiento**. Permite que usted asigne los políticas de ruteo (situados en el selector de política bajo la plataforma > encaminamiento) a los dispositivos y a los routeres IOS PIX/ASA/FWSM. Los ejemplos de los políticas de ruteo incluyen el OSPF, el RIP, y las directivas del Static Routing.
16. **Asigne > > Security (Seguridad) de las directivas**. Permite que usted asigne las políticas de seguridad (situadas en el selector de política bajo el > Security (Seguridad) de la plataforma) a los dispositivos PIX/ASA/FWSM. Las políticas de seguridad incluyen contra spoofing, el fragmento, y las configuraciones de tiempo de espera.
17. **Asigne > las directivas > las reglas de la política de servicio**. Permite que usted asigne las directivas de la regla de la política de servicio (situadas en el selector de política bajo reglas de la plataforma > de la política de servicio) a los dispositivos PIX 7.x/ASA. Los ejemplos incluyen las colas de administración del tráfico de prioridad e IPS, QoS, y las reglas de la conexión.
18. **Asigne > las directivas > las preferencias del usuario**. Permite que usted asigne la directiva del despliegue (situada en el selector de política bajo la plataforma > preferencias del usuario) a los dispositivos PIX/ASA/FWSM. Esta directiva contiene una opción para borrar todas las traducciones de NAT en el despliegue.
19. **Asigne > las directivas > dispositivo virtual**. Permite que usted asigne las directivas virtuales del sensor a los dispositivos IPS. Utilice esta directiva para crear los sensores virtuales.
20. **Asigne > las directivas > FlexConfig**. Permite que usted asigne FlexConfigs, que son los comandos CLI y las instrucciones adicionales que pueden ser desplegados a los dispositivos PIX/ASA/FWSM, a los dispositivos de los routeres IOS, y del Catalyst 6500/7600.

Nota: Cuando usted especifica asigne los permisos, se aseeguran que usted ha seleccionado los permisos correspondientes de la visión también.

Apruebe los permisos

El administrador de seguridad proporciona los permisos de la aprobación como se muestra:

1. **Apruebe > CLI**. Permite que usted apruebe los cambios del comando CLI contenidos en un trabajo del despliegue.
2. **Apruebe > directiva**. Permite que usted apruebe los cambios de configuración contenidos en

las directivas que fueron configuradas en una actividad del flujo de trabajo.

Comprensión de los papeles de los CiscoWorks

Cuando crean a los usuarios en el CiscoWorks Common Services, ellos asignan uno o más papeles. Los permisos asociados a cada papel determinan las operaciones que autorizan cada usuario a realizarse en el administrador de seguridad.

Los temas siguientes describen los papeles de los CiscoWorks:

- El CiscoWorks Common Services omite los papeles
- Asignación de los papeles a los usuarios en el CiscoWorks Common Services

El CiscoWorks Common Services omite los papeles

El CiscoWorks Common Services contiene los papeles predeterminados siguientes:

1. **Escritorio de ayuda** — Los usuarios del escritorio de ayuda pueden ver (pero no modificarse) los dispositivos, las directivas, los objetos, y las correlaciones de topología.
2. **Operador de la red** — Además de los permisos de la visión, los operadores de la red pueden ver las configuraciones administrativas de los comandos CLI y del administrador de seguridad. Los operadores de la red pueden también modificar los comandos del archivo de configuración y del problema (tales como ping) a los dispositivos.
3. **Approver** — Además de los permisos de la visión, los approvers pueden aprobar o rechazar los trabajos del despliegue. No pueden realizar el despliegue.
4. **Administrador de la red** — Los administradores de la red tienen visión completa y modifican los permisos, a excepción de modificar las configuraciones administrativas. Pueden descubrir los dispositivos y las directivas configuradas en estos dispositivos, asignar las directivas a los dispositivos, y los comandos del problema a los dispositivos. Los administradores de la red no pueden aprobar las actividades o los trabajos del despliegue; sin embargo, pueden desplegar los trabajos que fueron aprobados por otros.
5. **Administrador de sistema** — Los administradores de sistema tienen acceso completo a todos los permisos del administrador de seguridad, incluyendo la modificación, asignación de la directiva, actividad y Aprobación de trabajo, detección, despliegue, y publicación de los comandos a los dispositivos.

Nota: Los papeles adicionales, tales como datos de la exportación, se pudieron visualizar en los servicios comunes si las aplicaciones adicionales están instaladas en el servidor. El papel de los datos de la exportación está para los desarrolladores de proveedor externo y no es utilizado por el administrador de seguridad.

Consejo: Aunque usted no pueda cambiar la definición de los papeles de los CiscoWorks, usted puede definir qué papeles se asignan a cada usuario. Para más información, vea la asignación de los papeles a los usuarios en el CiscoWorks Common Services.

Asignación de los papeles a los usuarios en el CiscoWorks Common Services

El CiscoWorks Common Services le permite para definir qué papeles se asignan a cada usuario. Cambiando la definición del papel para un usuario, usted cambia los tipos de operaciones que

autorizan a este usuario se realiza en el administrador de seguridad. Por ejemplo, si usted asigna el papel del escritorio de ayuda, limitan para ver las operaciones y no puede modificar al usuario ningunos datos. Sin embargo, si usted asigna el papel del operador de la red, el usuario puede también modificar el archivo de configuración. Usted puede asignar los papeles múltiples a cada usuario.

Nota: Usted debe recomenzar al administrador de seguridad después de realizar los cambios a los permisos del usuario.

Procedimiento:

1. En los servicios comunes, la **Seguridad** selecta del **server>**, entonces selecciona la **Administración > al usuario local de confianza del servidor único puestos del** TOC.**Consejo:** Para alcanzar la página de configuración del usuario local dentro del administrador de seguridad, el control del administrador selecto del Tools (Herramientas) > Security (Seguridad) > la Seguridad del servidor, entonces hacen clic la configuración del usuario local.
2. Seleccione la casilla de verificación al lado de un usuario existente, después haga clic **editan**.
3. En la página de la información del usuario, seleccione los papeles para asignar a este usuario haciendo clic las casillas de verificación.Para más información sobre cada papel, vea que el CiscoWorks Common Services omite los papeles.
4. Haga Click en OK para salvar sus cambios.
5. Administrador de seguridad del reinicio.

Comprensión de los papeles del Cisco Secure ACS

El Cisco Secure ACS proporciona la mayor flexibilidad para manejo de los permisos del administrador de seguridad que los CiscoWorks porque soporta los papeles específicos a la aplicación que usted puede configurar. Cada papel se compone de un conjunto de los permisos que determinan el nivel de autorización a las tareas del administrador de seguridad. En el Cisco Secure ACS, usted asigna un papel a cada grupo de usuarios (y opcionalmente, a los usuarios individuales también), que permite a cada usuario en ese grupo para realizar las operaciones autorizó por los permisos definidos para ese papel.

Además, usted puede asignar estos papeles a los grupos de dispositivos del Cisco Secure ACS, permitiendo que los permisos sean distinguidos en diversos conjuntos de dispositivos.

Nota: Los grupos de dispositivos del Cisco Secure ACS son independiente de los grupos de dispositivos del administrador de seguridad.

Los temas siguientes describen los papeles del Cisco Secure ACS:

- El Cisco Secure ACS omite los papeles
- Personalizar los papeles del Cisco Secure ACS

El Cisco Secure ACS omite los papeles

El Cisco Secure ACS incluye los mismos papeles que los CiscoWorks (véase comprensión de los papeles de los CiscoWorks), más estos papeles adicionales:

1. **Seguridad Approver** — Los approvers de la Seguridad pueden ver (pero no modificarse) los dispositivos, las directivas, los objetos, las correspondencias, los comandos CLI, y las configuraciones administrativas. Además, los approvers de la Seguridad pueden aprobar o rechazar los cambios de configuración contenidos en una actividad. No pueden aprobar o rechazar el trabajo del despliegue, ni pueden realizar el despliegue.
2. **Administrador de seguridad** — Además del tener permisos de la visión, los administradores de seguridad pueden modificar los dispositivos, los grupos de dispositivos, las directivas, los objetos, y las correlaciones de topología. Pueden también asignar las directivas a los dispositivos y a las topologías VPN, y realizan la detección para importar los nuevos dispositivos en el sistema.
3. **Administrador de la red** — Además de los permisos de la visión, los administradores de la red pueden modificar el archivo de configuración, realizar el despliegue, y los comandos del problema a los dispositivos.

Nota: Los permisos contenidos en la función del administrador de red del Cisco Secure ACS son diferentes de ésos contenidos en la función del administrador de red de los CiscoWorks. Para más información, vea comprensión de los papeles de los CiscoWorks.

A diferencia de los CiscoWorks, el Cisco Secure ACS le permite para personalizar los permisos asociados a cada papel del administrador de seguridad. Para más información sobre la modificación de los papeles predeterminados, vea personalizar los papeles del Cisco Secure ACS.

Nota: El Cisco Secure ACS 3.3 o más adelante se debe instalar para la autorización del administrador de seguridad.

Personalizar los papeles del Cisco Secure ACS

El Cisco Secure ACS le permite para modificar los permisos asociados a cada papel del administrador de seguridad. Usted puede también personalizar el Cisco Secure ACS creando los rol del usuario especializados con los permisos que se apuntan a las tareas determinadas del administrador de seguridad.

Nota: Usted debe recomenzar al administrador de seguridad después de realizar los cambios a los permisos del usuario.

Procedimiento:

1. En el Cisco Secure ACS, haga clic a los **componentes del perfil compartidos** en la barra de navegación.
2. Haga clic al **Cisco Security Manager** en la página compartida de los componentes. Se visualizan los papeles que se configuran para el administrador de seguridad.
3. Siga uno de los siguientes pasos:Para crear un papel, haga click en Add Vaya al paso 4.Para modificar un papel existente, haga clic el papel. Vaya al paso 5.
4. Ingrese un nombre para el papel y, opcionalmente, una descripción.
5. Seleccione y no reelija como candidato las casillas de verificación en el árbol de los permisos para definir los permisos para este papelLa selección de la casilla de verificación para una bifurcación del árbol selecciona todos los permisos en esa bifurcación. Por ejemplo, la selección **asigna** selecciona todos los permisos de la asignación.Para una lista completa de permisos del administrador de seguridad, vea los permisos del administrador de

seguridad.**Nota:** Cuando usted selecciona modifique, apruebe, asigne, importe, controle o despliegue los permisos, usted debe también seleccionar los permisos correspondientes de la visión; si no, el administrador de seguridad no funcionará correctamente.

6. El tecleo **somete** para salvar sus cambios.
7. Administrador de seguridad del reinicio.

Asociaciones predeterminadas entre los permisos y los papeles en el administrador de seguridad

Esta tabla muestra cómo los permisos del administrador de seguridad se asocian a los papeles del CiscoWorks Common Services y a los papeles predeterminados en el Cisco Secure ACS.

Permisos	Papeles							
	Administrador del sistema	Seguridad Admin (ACS)	Seguridad Approver (ACS)	Red Admin (CW)	Red Admin (ACS)	Approver	Operador de la red	Escritorio de ayuda
Permisos de la visión								
Dispositivo de la visión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Directiva de la visión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Objetos de visión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Topología de la visión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Visión CLI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Visión Admin	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Archivo de configuración de la visión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Administradores de dispositivo de la visión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Modifique los permisos								
Modifique el dispositivo	Sí	Sí	No	Sí	No	No	No	No
Modifique la jerarquía	Sí	Sí	No	Sí	No	No	No	No

Modifique la directiva	Sí	Sí	No	Sí	No	No	No	No
Modifique la imagen	Sí	Sí	No	Sí	No	No	No	No
Modifique los objetos	Sí	Sí	No	Sí	No	No	No	No
Modifique la topología	Sí	Sí	No	Sí	No	No	No	No
Modifique el Admin	Sí	No	No	No	No	No	No	No
Modifique el Archivo de configuración	Sí	Sí	No	Sí	Sí	No	Sí	No
Permisos adicionales								
Asigne la directiva	Sí	Sí	No	Sí	No	No	No	No
Apruebe la directiva	Sí	No	Sí	No	No	No	No	No
Apruebe el CLI	Sí	No	No	No	No	Sí	No	No
Descubra (importación)	Sí	Sí	No	Sí	No	No	No	No
Despliegue	Sí	No	No	Sí	Sí	No	No	No
Control	Sí	No	No	Sí	Sí	No	Sí	No
Someta	Sí	Sí	No	Sí	No	No	No	No

Información Relacionada

- Página de soporte del Cisco Security Manager
- Soporte Técnico y Documentación - Cisco Systems