Integre varios clústeres de ISE con un dispositivo web seguro para las políticas basadas en TrustSec

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados** Limitaciones Diagrama de la red Configurar Configuración de ISE Activar SXP Configure SXP en los nodos del clúster Configure SXP en el nodo de agregación Habilitar pxGrid en el nodo de agregación aprobación automática de pxGrid Configuración TrustSec de dispositivos de red Autorización de dispositivo de red SGT Política de autorización Habilitación de ERS en el nodo de agregación de ISE (opcional) Agregar usuario al grupo de administración ESR (opcional) Configuración del dispositivo web seguro Certificado pxGrid Habilitar SXP y ERS en un dispositivo web seguro Perfil de identificación Política de descifrado basada en SGT Configuración del switch AAA **TrustSec** Verificación Información Relacionada

Introducción

Este documento describe el procedimiento para enviar información de Security Group Tag (SGT) desde varias implementaciones de ISE a un único Cisco Secure Web Appliance (oficialmente Web Security Appliance WSA) a través de pxGrid para aprovechar las políticas de acceso web basadas en SGT en una implementación de TrustSec.

Antes de la versión 14.5, Secure Web Appliance solo puede integrarse con un solo clúster de ISE para las políticas de identidad basadas en SGT. Con la introducción de esta nueva versión, Secure Web Appliance ahora puede interoperar con información de varios clústeres ISE con un nodo ISE independiente que se agrega entre ellos. Esto aporta grandes ventajas y nos permite exportar datos de usuarios de diferentes clústeres de ISE, así como la libertad de controlar el punto de salida que un usuario puede utilizar sin la necesidad de una integración 1:1.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE)
- Dispositivo web seguro
- protocolo RADIUS
- TrustSec
- pxGrid

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo web seguro 14.5
- ISE versión 3.1 P3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Limitaciones

- 1. Todos los clústeres de ISE deben mantener asignaciones uniformes para SGT.
- 2. El nodo de agregación de ISE debe tener el nombre/número de SGT del resto de los clústeres de ISE.
- 3. Secure Web Appliance sólo puede identificar la política (acceso/descifrado/enrutamiento) basada en la etiqueta SGT y no en el grupo ni el nombre de usuario .
- 4. La generación de informes y el seguimiento se basan en SGT.
- 5. Los parámetros de tamaño existentes de ISE/Secure Web Appliance siguen aplicándose a esta función.

Diagrama de la red



Proceso:

1. Cuando el usuario final se conecta a la red, recibe una SGT basada en las políticas de autorización de ISE.

2. A continuación, los diferentes clústeres de ISE envían esta información SGT en forma de asignaciones SGT-IP al nodo de agregación de ISE a través de SXP.

3. ISE Aggregation Node recibe esta información y la comparte con el único Secure Web Appliance a través de pxGrid.

4. Secure Web Appliance utiliza la información SGT que ha aprendido para proporcionar acceso a los usuarios en función de las políticas de acceso Web.

Configurar

Configuración de ISE

Activar SXP

Paso 1. Seleccione el icono de tres líneas se encuentra en la esquina superior izquierda y seleccione en Administration > System > Deployment.

Paso 2. Seleccione el nodo que desea configurar y haga clic en Editar.

| E Cisco ISE | | Administration - System | | | | | | 0 🕫 |
|----------------------|--------------|-------------------------|-------------|-----------------------------|-----------------|--------------------|--------------------|---|
| Deployment Licensing | Certificates | Logging | Maintenance | Upgrade He | alth Checks Ba | ckup & Restore | Admin Access | Settings |
| Deployment | • De | eploymer | nt Nodes | | | | Selected 1 Total 1 | 0.0 |
| > 2 Deployment | 0 | tate 🕞 Registe | r D Syncup | 🔒 Deregister | | | A | • ~ - - - - - |
| AP PART MODEL | C | Hostname | A Personal | | Role(s) | Services | No | de Status |
| | | ise01-CL1 | Administra | ition, Monitoring, Policy S | enice STANDALON | E SESSION/PROFILER | | |

Paso 3. Para activar SXP, marque la casilla Enable SXP Service (Activar servicio SXP)

| E Cisco | ISE Administration • System | | | | | | Q (0) | | | |
|------------|-----------------------------|--------------|------------|-------------------------|-----------------|---------------|------------------|--------------|----------|--|
| Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Health Checks | Backup & Restore | Admin Access | Settings | |
| | | | 2 ~ | Enable Session | Services G |) | | | | |
| | | | | Include Node in Nod | le Group None | | ~ 0 | | | |
| | | | 🛃 Enab | ie Profiling Service 🕣 | | | | | | |
| | | | Cnel | ie Threat Centric NAC S | iervice 🕞 | | | | | |
| | | | - | Enable SXP Se | rvice 🕢 | | | | | |
| | | | | Use Interface | GigabitEthernet | 0 | ~ | | | |

Paso 4. Desplácese hacia abajo y haga clic en Guardar

Nota: Repita todos los pasos para el resto de los nodos ISE en cada clúster, el nodo de agregación incluido.

Configure SXP en los nodos del clúster

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centro de trabajo > TrustSec > SXP**.

Paso 2. Haga clic en +Add para configurar el nodo de agregación ISE como un peer SXP.

| ■ Cisco ISE | | Work Centers • T | rustSec | | | | | Q | 0 | 19 | 0 |
|---------------------------------|--------------------------|------------------|---------|------------|--------------|---------|----------|-----|----------|---------|-----|
| Overview Cor | nponents TrustSec Policy | Policy Sets | SXP | ACI | Troubleshoot | Reports | Settings | | | | |
| SXP Devices All SXP Mappings | SXP Dev | vices 💿 | | | | | | | | | |
| | | | | | Rows/Page 2 | V ICC | /1>>1 | Go. | 2 % | otal Ro | NV5 |
| | Ø Refresh | Add 🛛 Trash 🗸 🖉 | Edit As | aign SXP (| Domain | | | | V Filter | ~ 1 | 0 |

Paso 3. Defina el nombre y la dirección IP del nodo de agregación ISE, seleccione la función de

peer como LISTENER. Seleccione los PSN requeridos en PSNs conectados, dominios SXP obligatorios, seleccione habilitado en estado, luego seleccione tipo de contraseña y versión requerida.

| Overview | Components | TrustSec Policy | Policy Sets | SXP | AC |
|-----------------|------------|--|----------------------|--------------|----|
| SXP Devices | | SXP Devices > SXP C | onnection | | |
| II SXP Mappings | | Upload from a CS¹ | / file | | |
| | | - Add Single Device | | | |
| | | Input fields marked v | with an asterisk (*) | are required | i. |
| | | Name ISE Aggregation n | ode | | |
| | | IP Address * 10.50.50.125 | | | |
| | | Peer Role * | | ~ | |
| | | | | | |
| | | Connected PSNs * | | | |



| Overview | Components | TrustSec Policy | Policy Sets | SXP | ACI |
|------------------|------------|---------------------------------------|-------------|--------|-----|
| SXP Devices | | SVD Domaine * | | | |
| All SXP Mappings | | default × | | | |
| | | | | | |
| | | Status * | | | |
| | | Enabled | | \sim | |
| | | | | | |
| | | Password Type * | | | |
| | | CUSTOM | | | |
| | | Password | | | |
| | | Version * | | | |
| | | V4 | | \sim | |
| | | Advanced Settings | 1 | | |
| | | | Cancel | Save | |

Paso 4. Haga clic en Save (Guardar).

Nota: Repita todos los pasos para el resto de los nodos ISE en cada clúster para generar una conexión SXP al nodo de agregación. Repita el mismo proceso en el nodo de agregación y seleccione SPEAKER como rol de peer.

Configure SXP en el nodo de agregación

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en Centro de trabajo > TrustSec > Configuración

Paso 2. Haga clic en la pestaña Configuración de SXP

Paso 3. Para propagar las asignaciones IP-SGT, marque la casilla de verificación Publicar enlaces SXP en pxGrid.



Paso 4 (opcional). Defina una contraseña predeterminada para la configuración de SXP en Contraseña global

| ≡ Cisco | ISE | W | | | | | | |
|--------------------|------------|---|----------------------------------|--------------|---------------|-------------------------|---------|----------|
| Overview | Components | TrustSec Policy | Policy Sets | SXP | ACI | Troubleshoot | Reports | Settings |
| General TrustSec S | Settings | SXP Settings | | | | | | |
| Work Process Sett | ings | Publish SXP bindir | ngs on PxGrid 🛃 Ad | d radius map | opings into S | XP IP SGT mapping table | 0 | |
| SXP Settings | | Global Passwor | ď | | | | | |
| ACI Settings | | Global Password This global passwor the device specific | rd will be overriden password | by | | | | |

Paso 5. Desplácese hacia abajo y haga clic en Guardar.

Habilitar pxGrid en el nodo de agregación

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Administración > Sistema > Implementación**.

Paso 2. Seleccione el nodo que desea configurar y haga clic en Editar.

| E Cisco ISE | | Administration - System | | | | 1 | | | | |
|--|-----------|-------------------------|------------------------------|---------------------|------------------|-------------------------------------|--|--|--|--|
| Deployment Licensing Certification | s Logging | Maintenance | Upgrade Heal | h Checks Backup & | Restore Adr | min Access Settings | | | | |
| Ceployment C T O O O O O O O O O O O O O O O O O O O | Deployr | nent Node: | S | | | Selected 1 Total 1 🕃 🔘 All V - 🏹 | | | | |
| ap rois raison | Host | name 🗠 Perso | onas | Role(s) | Services | Node Status | | | | |
| | a bere | N Admir | istration, Monitoring, Polic | y Senice STANDALONE | SESSION/PROFILER | • | | | | |

Paso 3. Para habilitar pxGrid, haga clic en el botón situado junto a pxGrid.

| Cisco ISE | Administration - System | ୍ ୦ ହା ୩ |
|---------------------|---|-----------------------|
| Deployment Uconsing | Certificates Logging Maintenance Upgrade Health Checks Backup & Restore | Admin Access Settings |
| | Enable Session Services (2) | |
| | include Node in Yorks Group Name 🗸 🕥 | |
| | 🚺 Evalue Profiling Service 🕟 | |
| | 🗌 Enable Thread Cantor Mrd Servers 💮 | |
| | Enuble SXP Service () | |
| | Us motor Ogsbittheret 0 V | |
| | 🔄 Enalte Device Admin Service 💿 | |
| | Contra Passor (Sentry Service 🔾 | |
| | | |
| | C bobse | |

Paso 4. Desplácese hacia abajo y haga clic en Guardar.

aprobación automática de pxGrid

Paso 1. Navegue hasta el icono de tres líneas situado en la esquina superior izquierda y seleccione **Administration > pxGrid Services > Settings**.

Paso 2. De forma predeterminada, ISE no aprueba automáticamente pxGrid las solicitudes de conexión de los nuevos clientes pxGrid, por lo que debe activar esa configuración seleccionando la casilla de verificación **Aprobar automáticamente nuevas cuentas basadas en certificados**.



Paso 3. Haga clic en Save (Guardar).

Configuración TrustSec de dispositivos de red

Para que Cisco ISE procese las solicitudes de los dispositivos habilitados para TrustSec, debe definir estos dispositivos habilitados para TrustSec en Cisco ISE.

Paso 1. Navegue hasta las tres líneas ubicadas en la esquina superior izquierda y seleccione en Administración > Recursos de red > Dispositivos de red.



Paso 3. Ingrese la información requerida en la sección Dispositivos de Red y en Configuración de Autenticación RADIUS.

Paso 4. Marque la casilla de verificación **Advanced TrustSec Settings** para configurar un dispositivo habilitado para TrustSec.

| Cisco ISE | Administration - Network Resources |
|--------------------------|---|
| Network Devices | Network Device Groups Network Device Profiles External RADIUS Servers |
| Network Devices | TACACS Authentication Settings |
| Default Device | SNMP Settings |
| Device Security Settings | Advanced TrustSec Settings |

Paso 5. Haga clic en la casilla de verificación Usar ID de dispositivo para la identificación TrustSec para rellenar automáticamente el nombre de dispositivo que aparece en la sección Dispositivos de red. Introduzca una contraseña en el campo Password.



Nota: El ID y la contraseña deben coincidir con el comando "cts credentials id <ID> password <PW>" que se configura posteriormente en el switch.

Paso 6. Marque la casilla de verificación **Enviar cambios de configuración al dispositivo** para que ISE pueda enviar notificaciones de CoA de TrustSec al dispositivo.

| Cisco ISE | | | | | |
|--------------------------|-----------------------|--|-------------------------|-------------------------|--------|
| Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | More ~ |
| Network Devices | | | | | |
| Default Device | ✓ Tru | stSec Notifications and U | pdates | | |
| Device Security Settings | | | 1 | | |
| | - (com | rical environment data every | Days Y | | |
| | | | | | |
| | * Dow | rioad peer authorization policy every | Days 🐱 | | |
| | | | | | |
| | * Rea | thertication every | Days 👻 🕢 | | |
| | | | | | |
| | * Dom | rioad SGACL lists every | Days ¥ | | |
| | Other 1 | frustfiel devices to trust this device | | | |
| | Send o | onfiguration changes to device | Using O CoA (|) en | |

Paso 7. Marque la casilla de verificación Incluir este dispositivo al implementar actualizaciones de asignación de etiquetas de grupo de seguridad.

Paso 8. Para permitir que ISE edite la configuración del dispositivo de red, ingrese las credenciales de usuario en los campos Nombre de usuario del modo EXEC y Contraseña del modo EXEC. Opcionalmente, proporcione enable password en el campo Enable Mode Password.

Nota: Repita los pasos para todos los demás NAD que estén destinados a formar parte del dominio TrustSec.

Autorización de dispositivo de red

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centros de trabajo > TrustSec > Política TrustSec.**

Paso 2. En el panel izquierdo, haga clic en Autorización de dispositivo de red.

| Egreen Pulicy Matrices List | - Network | k Device / | Authoriza | tion | | | | |
|--------------------------------|----------------|--------------|------------|------------------------|------------|-------------|------|--|
| Marris Texa | Laure de verse | Default Rule | If no rule | ring surs to network o | then Trust | Set_Devices | ER - | |

Paso 3. A la derecha, utilice el menú desplegable situado junto a Editar e Insertar nueva fila arriba

para crear una nueva regla NDA.

| I Cisco ISE | Work Centers - TrustSec | | | |
|---|---|------------------|--|--|
| Overview Components | TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports Settings | | | |
| Egress Policy ~ Metrices List Metric Source Tree Destination Tree | Network Device Authorization Define the Network Device Authorization Policy by assigning SGSs to network devices. Drag and drop rules to change th Default Rule II no rules defined or no match that TruetSec_Devices | e order. Este | | |
| Network Device Authorization | | | | |

Paso 4. Defina un **Nombre de regla, Condiciones** y seleccione la SGT adecuada en la lista desplegable en **Grupos de seguridad**.

Paso 5. Haga clic en Finalizado en el extremo derecho.

| E Cisco ISE | Work Centers - TrustSec | | | | | |
|------------------------------------|-----------------------------|---------------------------------|---|--|--|--|
| Overview Components | TrustSec Policy Policy Sets | SXP ACI Troubleshop | ot Reports Settings | | | |
| Egress Policy ~ ~ Matrices List | Network Device A | Authorization | devices. Drag and drop rules to change the order. | | | |
| fource Tree | Rule Name | Conditions | Security Group | | | |
| Destination Tree | 🗄 🖪 🗠 NDAD | F DEVICE Device Type equals to | v tes Tratfec,Devices v Dore | | | |
| Network Device Authorization | Default Rule | If no rules defined or no match | then Trustlee_Devices for - | | | |

Paso 6. Desplácese hacia abajo y haga clic en Guardar.

SGT

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centros de trabajo > TrustSec > Componentes.**

Paso 2. En el panel izquierdo, expanda Grupos de seguridad.

Paso 3. Haga clic en +Agregar para crear una nueva SGT.

| III Cisco ISE | Work Centers - TrustSec | 0.0 00 0 | | | | | | |
|-----------------------|---|---------------------|--|--|--|--|--|--|
| Overview Components | TrustSec Policy Policy Sets SHP ACI TrustRenhost Reports Settings | | | | | | | |
| Security Streeps | Consulta Consulta | | | | | | | |
| IP 967 Static Mapping | se Meering Security Groups | | | | | | | |
| Security Group ACLs | For Policy Expert prior Administration + Society & Restore - Policy Expert Page | | | | | | | |
| Nateork Devices | | Selected 0 Total 18 | | | | | | |
| Traities Servers | Ann → Ann → Input → Expert → E Track → O Track O Works Deploy | м | | | | | | |

Paso 4. Introduzca el nombre y seleccione un icono en los campos correspondientes.

| Work Centers • TrustSec | | | | | | |
|---|--|--|--|--|--|--|
| TrustSec Policy Policy Sets SXP ACI Troubleshoo | | | | | | |
| Security Groups List > New Security Group | | | | | | |
| Security Groups | | | | | | |
| | | | | | | |
| * Name | | | | | | |
| Cluster1_Endpoints | | | | | | |
| * Icon | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Paso 5. Opcionalmente, proporcione una descripción e introduzca un valor de etiqueta.

Nota: Para poder introducir manualmente un valor de etiqueta, navegue hasta Centros de trabajo > TrustSec > Configuración > Configuración general de TrustSec y seleccione la opción El usuario debe introducir manualmente el número SGT en Numeración de etiquetas de grupo de seguridad.

Paso 6. Desplácese hacia abajo y haga clic en Enviar

Nota: Repita estos pasos para todas las SGT necesarias.

Política de autorización

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Política > Conjuntos de políticas.**

Paso 2. Seleccione el conjunto de políticas adecuado.

Paso 3. Dentro del conjunto de políticas, expanda la Política de autorización.

| E Cisco ISE | Policy Policy Sets | | | | 9.05 | 2 0 |
|--|--------------------|---|---|-------|-------------------------------------|------|
| Policy Sets-+ Wired Access | | | | Reset | Reset Policyset Hissouris | |
| Status Policy Set Name Description | Conditio | | | | Allowed Protocols / Server Sequence | Hits |
| Q Seed | | | | | | |
| Wind Access | *** | 9 | DEVICE Oncice Puper EQUALS AT Device PuperHSwitches | | Default Network Access 🛛 😨 🔆 🕸 | |
| | | - | Radius NAS-Part Type ESSAGE Ethernet | | | |
| > Authentication Policy (2) | | | | | | |
| > Authorization Policy - Local Exceptions | | | | | | |
| > Authorization Policy - Global Exceptions | | | | | | |
| > Authorization Policy (1) | | | | | | |

Paso 4. Haga clic en el para crear una directiva de autorización.

| Authorization Policy (1) | | | | | |
|--|------------|----------|-----------------|------|---------|
| | | Results | | | |
| Status Rule Name | Conditions | Profiles | Security Groups | Hits | Actions |

Paso 5. Defina el Nombre de la Regla, las Condiciones y los Perfiles requeridos y seleccione la SGT adecuada en la lista desplegable en Grupos de Seguridad.

| | | Results | | | |
|------------------|------------|----------|-----------------|------|--------|
| Status Rule Name | Conditions | Profiles | Security Groups | Hits | Action |
| Q Search | | | | | |

Paso 6. Click Save.

Habilitación de ERS en el nodo de agregación de ISE (opcional)

El servicio de API RESTful externo (ERS) es una API que WSA puede consultar para obtener información del grupo. El servicio ERS está inhabilitado de forma predeterminada en ISE. Una vez habilitada, los clientes pueden consultar la API si se autentican como miembros del grupo **ADR** en el nodo ISE. Para habilitar el servicio en ISE y agregar una cuenta al grupo correcto, siga estos pasos:

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Administración > Sistema > Configuración.**

Paso 2. En el panel izquierdo, haga clic en Configuración de ERS.

| 🔳 Cisco IS | 3 | Administration - System | | | | | | Q | 0 90 | | |
|---|-----------|---|--|------------------------------|---------|---------------|------------------|--------------|----------|--|--|
| Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Health Checks | Backup & Restore | Admin Access | Settings | | |
| Client Provisioning FIPS Mode Security Settings | ĺ | ERS S | ettings | | | | | | | | |
| Alarm Settings | | ✓ Genera | d. | | | | | | | | |
| Posture | • | External PE The ERS se An ISE Adm | Leternal RESTML Services (ERS) is a REST API based on HTTP'S over port 9060. The ERS service is disabled by default. An ES Administrator with the "CRS-Admin" or "ERS-Operator" group assignment is required to use the API. | | | | | | | | |
| Profiling | | For more in https://10.5 | formation, please 0 50 125 9000/ers | visit the ERS SDK page 50 | at: | | | | | | |
| Protocols | | | | | | | | | | | |
| Endpoint Scripts | > | Y ERS Se | stting for Adr | ninistration Node | | | | | | | |
| Proxy | | O Enite | DIS forleastWrite | 1 | | | | | | | |
| SMTP Server | | O DeadAr | D4S | | | | | | | | |
| SMS Gateway | | | | | | | | | | | |
| System Time | | | | | | | | | | | |
| ERS Settings | | V CSRF (| Check | | | | | | | | |

Paso 3. Seleccione la opción Enable ERS for Read/Write (Habilitar ERS para lectura/escritura).

Paso 4. Haga clic en Guardar y confirme con Aceptar.

Agregar usuario al grupo de administración ESR (opcional)

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione Administration > System > Admin Access

Paso 2. En el panel izquierdo, expanda Administradores y haga clic en Usuarios administrativos.

Paso 3. Haga clic en +Add y seleccione Admin User en la lista desplegable.

| ≡ Cisco I | SE | Administration - System | | | | | Q @ 50 ¢ | | | | |
|----------------|-----------|-------------------------|-----------------|-------------------|-----------------|---------------|-------------|---------------|-------------|-----------|----|
| Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Health Checks | Backup & Re | store Admin | Access | Settings | i. |
| Authentication | | Admir | nistrator | S | | | | | | | |
| Authorization | > | | | - | | | | | Selected 0 | Fotal 1 🖉 | ٥ |
| Administrators | ~ | O ton - | - Add 🛞 C | hange Status | Delete D C | uplicate | | | | | V |
| Admin Users | | - | | | | | | | | | |
| Admin Groups | | | Create an Admir | User | Description | First Name | Last Name | Email Address | Admin Gro | adr | |
| | | | Select from Net | work Access Users | > Default Admir | User | | | Super Admin | | |
| Settings | > | | | | | | | | | | |

Paso 4. Introduzca un nombre de usuario y una contraseña en los campos correspondientes.

| I Cisco ISE | | | Ad | Iministration • S | ystem | | | 0.0536 | | |
|----------------|-----------|-----------------------|----------------|-------------------|----------|------------------------|------------------|--------------|----------|--|
| Deployment L | Licensing | Certificates Lo | opina | Maintenance | Upgrade | Health Checks | Backup & Restore | Admin Access | Settings | |
| Authentication | | Administrators List 3 | 1150 | | | | | | | |
| Authorization |) | ✓ Admin User | | | | | | | | |
| Administrators | ~ | "Name WSA | | | | | | | | |
| Admin Usors | | | | | | | | | | |
| Admin Groups | | Status 🛃 En | abled 🛩 | | | | | | | |
| | | Ernall | | | C Inches | suden alarma in emails | | | | |
| Settings | > | | | | 0 | | | | | |
| | | Design C | | | | | | | | |
| | | Inactive account of | ever disabiled | 0 | | | | | | |
| | | | | | | | | | | |
| | | ✓ Password | | | | | | | | |
| | | * Password | | | G | | | | | |
| | | * Ro-Enter Pass | erd | | | | | | | |
| | | | | | | | | | | |

Paso 5. En el campo Admin Groups, utilice el menú desplegable para seleccionar ERS Admin.

| ≡ Cisco | SE | | Administration - System | | | | | Q, | ō 9 | 8.0 |
|----------------|-----------|--------------|-------------------------|-------------|------------|---------------|------------------|--------------|---------|-----|
| Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Health Checks | Backup & Restore | Admin Access | Setting | gs |
| Authentication | | First Name | | | | | | | | |
| Authorization | > | Last Name | | | | | | | | |
| Administrators | ~ | | | | | | | | | |
| Admin Usors | | × Account | a Ontines | | | | | | | |
| Admin Groups | | Description | | | | | | | | |
| Settings | > | | | | | | | | | |
| | | Y Admin | Groups ERS Admin | | × + | | | | | |
| | | | | | | | | Save | Reset | |

Paso 6. Click Save.

Configuración del dispositivo web seguro

Certificado raíz

Si el diseño de integración utiliza una autoridad de certificados interna como raíz de la confianza para la conexión entre WSA e ISE, este certificado raíz se debe instalar en ambos dispositivos.

Paso 1. Navegue hasta Red > Administración de certificados y haga clic en Administrar certificados raíz de confianza para agregar un certificado de CA.

| 🛃 Cisco Secu | ure Web Appliance | | | Secure Web Appliance is getting a new look. Try I | | | |
|--------------------------|-----------------------------|------------------------------|---------------------------|---|-----------------------|--|--|
| S100V Reporting | Web Security Manager | Security Services | Network | System Administration | | | |
| | | | | | | | |
| Certificate Ma | inagement | | | | | | |
| Appliance Certificate | | | | | | | |
| Add Certificate | | | | | | | |
| Certificate Con | nmon Name Issued | By Domains | Status Time F | temaining Expiration | Date Delete | | |
| Export Certificate | | | | | | | |
| | | | | | | | |
| Weak Signature Usa | ge Settings | | | | | | |
| Rest | trict Weak Signature Usage: | Disabled | | | | | |
| | | | | | Edit Settings | | |
| | | | | | | | |
| Certificate FQDN Val | idation Settings | | | | | | |
| Certific | ate FQDN Validation Usage: | Disabled | | | | | |
| | | | | | Edit Settings | | |
| | | | | | | | |
| Certificate Lists | | | | | | | |
| Updates | | | | | | | |
| File Type | | Last Update | | Current Version | New Update | | |
| Cisco Trusted Root Cer | tificate Bundle | Success - Thu Jun 30 1 | 5:32:47 2022 | 2.1 | Not Available | | |
| Cisco Certificate Blocks | ed List | Success - Wed May 11 | 21:04:06 2022 | 1.3 | Not Available | | |
| No updates in progress | κ. | | | | Update Now | | |
| Certificate Hanag | | | | | | | |
| | Trust Root Certificates: | 244 certificates in Cisco tr | usted root certificate li | st Lotte for | | | |
| | | L CURRON CERTIFICATES \$000 | e to trusted root onfor | CIPSE MR | | | |
| | | | | Manage Inv | neo soot Certificates | | |

Paso 2. Haga clic en Importar.



Paso 3. Haga clic en Elegir archivo para localizar la CA raíz generada y haga clic en Enviar.

Paso 4. Haga clic en Enviar de nuevo.

Paso 5. En la esquina superior derecha, haga clic en Registrar cambios.

| Cisco Secure Web Appliance | | | Secure Web Applance is petting a new look. Try II I | | | Lagged in an admin of measure-offpla Hys Facestan - Sphere - Support and I | | | |
|----------------------------|-----------|----------------------|---|---------|-----------------------|---|--|--|-------------------|
| • | Reporting | Web Security Manager | Security Services | Network | System Administration | | | | |
| | | | | | | | | | Canoni Changes n. |

Paso 6. Haga clic en Registrar cambios de nuevo.

Certificado pxGrid

En WSA, la creación del par de claves y el certificado para su uso por pxGrid se completa como parte de la configuración de servicios ISE.

Paso 1. Vaya a Red > Identity Service Engine.

Paso 2. Haga clic en Activar y editar configuración.

Paso 3. Haga clic en Elegir archivo para localizar la CA raíz generada y haga clic en Cargar archivo.

| Identity Services Engine | |
|---|---|
| Edit Sherility Dervices Engine Settings | |
| C Exable ISE Bervice | |
| Primary 158 pedicid Node: | The Blob Applance will communicate with the 200 period node to support Blob Applance data subscription (impaing updates). A primary 200 period node (server) must be configured. |
| | (Institute or Det address) |
| | ttid packet hode Cantificate: If the IBB packet node cantificate is spead by a Cathoote Authority, conferm that the Castificate Authority is bited in the Tradeol Real Cantificates is used explored, and the Castificate Authority is bited in the Section of the |

Nota: Una configuración incorrecta común es cargar el certificado pxGrid de ISE en esta sección. El certificado de CA raíz se debe cargar en el campo Certificado de nodo de pxGrid de ISE.

Paso 4. En la sección Certificado de cliente de dispositivo web, seleccione Usar certificado y clave generados.

| Web Appliance Client Certificate: | ir secure communication between the Web Appliance and the ISE particle servers, provide a client certificate. This may need to b the ISE particle node(u) configured above. | e uph |
|-----------------------------------|--|-------|
| | Use Uploaded Certificate and Key | |
| | Certificate: Choose Film No file chooses Upload Files | |
| | Key Checke File Mar file chosen | |
| | Rev is Encrypted | |
| | No certificate has been uploaded. | |
| | Use Generated Certificate and Key Generate New Certificate and Key | |

Paso 5. Haga clic en el botón **Generar nuevo certificado y clave** y complete los campos de certificado requeridos.

| Generate Certificate an | nd Key | \times |
|-----------------------------|--|----------|
| Common Name: | | |
| Organization: | | |
| Organizational Unit: | | |
| Country: | | |
| Duration before expiration: | months | |
| Basic Constraints: | Set X509v3 Basic Constraints Extension to Critical | |
| Generate Cancel | | |

Paso 6. Haga clic en Descargar solicitud de firma de certificado.

Nota: Se recomienda seleccionar el botón **Enviar** para registrar los cambios en la configuración de ISE. Si la sesión se deja en tiempo de espera antes de que se envíen los cambios, las claves y el certificado que se generaron pueden perderse, incluso si se descargó el CSR.

Paso 7. Una vez que haya firmado la CSR con su CA, haga clic en **Elegir archivo** para localizar el certificado.

| Web Appliance Client Certificate: | For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above. | | | | | |
|-----------------------------------|--|--|--|--|--|--|
| | O Use Uploaded Certificate and Key | | | | | |
| | Certificate: Choose File No file chosen Upload Files | | | | | |
| | Key: Choose File No file chosen | | | | | |
| | Key is Encrypted | | | | | |
| | No certificate has been uploaded. | | | | | |
| | Use Generated Certificate and Key Generate New Certificate and Key | | | | | |
| | Common name: wsa.security/ab.net Organization: Osco | | | | | |
| | Organizational Unit: Security | | | | | |
| | Country: SE | | | | | |
| | Exploration Date: May 10 19:19:26 2024 GMT | | | | | |
| | Basic Constraints: Not Critical | | | | | |
| | Download Certificate Download Certificate Signing Request | | | | | |
| | Signed Certificate: | | | | | |
| | To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below. | | | | | |
| | Certificate: Choose File No file chosen Upload File | | | | | |

Paso 8. Haga clic en Cargar archivo.

Paso 9. Enviar y confirmar.

Habilitar SXP y ERS en un dispositivo web seguro

Paso 1. Haga clic en los botones Enable para SXP y ERS.



Paso 2. En el campo Credenciales de administrador ERS, introduzca la información de usuario configurada en ISE.

Paso 3. Marque la casilla para **que el nombre del servidor sea igual que el nodo pxGrid de ISE** para heredar la información configurada anteriormente. De lo contrario, introduzca la información necesaria allí.

| Enable ISE External Restful Service (ERS) | | | |
|---|-------------------------------------|-------------------------|--------------------------------|
| | ERS Administrator Credentials | | |
| | Username: | WSA | |
| | Password: | ••••• | |
| | ERS Servers | | |
| | Server name same as 15E pxGrid Node | | |
| | Primary: | ise-agg.securitylab.net | (Hostname or IPv4 address) |
| | Secondary (Optional): | | (Hostname or IPv4 address) |
| | Port: | 9060 (Enter the port re | mber specified for ERS in 15E) |

Paso 4. Enviar y confirmar.

Perfil de identificación

Para utilizar las etiquetas de grupos de seguridad o la información de grupo ISE en las políticas WSA, primero se debe crear un perfil de identificación que utilice ISE como medio para identificar a los usuarios de forma transparente.

Paso 1. Vaya a Web Security Manager > Authentication > Identification Profiles.

Paso 2. Haga clic en Agregar perfil de identificación.

Paso 3. Introduzca un nombre y, opcionalmente, una descripción.

Paso 4. En la sección Identificación y Autenticación, utilice el menú desplegable para elegir Identificar de forma transparente a los usuarios con ISE.

Identification Profiles: Add Profile

| Enable Identification Profile | |
|--|--|
| Name: 🕐 | ISE Profile (e.g. my IT Profile) |
| Description: | Identification profile for ISE Integration. |
| Internet Allowers | (neuronal answer characters 2010) |
| Enter Party. | (C) (Section 11 (1997) -) |
| Identification Hethod | |
| Identification and Authentication: 🕐 | Transparently identify users with ISE 🛛 👻 |
| Fallback to Authentication Realm or Guest Privileges: 2 | If user information is not available from the Identity Services Engine: |
| | Support Guest Privileges V |
| | Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies). |
| ership Definition | |
| ership is defined by any combination of the I | ollowing options. All criteria must be met for the policy to take effect. |
| Define Members by Subnet: | |
| | Consultation and the state of t |
| | |

Paso 5. Enviar y confirmar.

Política de descifrado basada en SGT

Paso 1. Vaya a Web Security Manager > Web Policies > Decryption Policies.

Paso 2. Haga clic en Agregar política.

Paso 3. Introduzca un nombre y, opcionalmente, una descripción.

Paso 4. En la sección Perfiles de identificación y usuarios, utilice el menú desplegable para elegir Seleccionar uno o más perfiles de identificación.

Paso 5. En la sección **Perfiles de identificación**, utilice el menú desplegable para elegir el nombre del perfil de identificación de ISE.

Paso 6. En la sección Usuarios y grupos autorizados, seleccione Grupos y usuarios

seleccionados.

| central in central by the containable of the f | contrary spectra. He cristical robust | ar one or one pointy to take error. | | | | |
|--|--|---|------------------------|--|--|--|
| Identification Profiles and Users: | Select One or More Identification Profiles 🗸 👻 | | | | | |
| | Identification Profile | Authorized Users and Groups | Add Identification Pro | | | |
| | ISE Profile | OAl Authenticated Users | | | | |
| | | Selected Groups and Users (2) ISE Secure Group Tage: No tags entered ISE Groups: No groups entered Users: No users entered | 9 | | | |
| | | Guests (users falling authentication) | | | | |
| | Authentication information may n | ot be available at WTTPS connection tim | e. For transparent | | | |

Paso 7. Haga clic en el hipervínculo situado junto a Etiquetas de grupo seguras de ISE.

Paso 8. En la sección **Búsqueda segura de etiquetas de grupo**, marque la casilla a la derecha de la SGT deseada y haga clic en **Agregar**.

| Secure Group Tag(s) currently in | cluded in this policy. | | |
|----------------------------------|------------------------|-------------------------------------|--------|
| Secure Group Tag Name | SGT Number | 8GT Description | Delete |
| Cluster1_Endpoints | 111 | Endpoints residing in ISE Cluster-1 | 0 |
| | | | |
| | | | |

| Enter any text to search for a Sec Add button to add to this policy. | ture Group Tag name, number, or o | lescription. Select one or more Secure Group Tags from th | e list and use the |
|---|-----------------------------------|---|--------------------|
| Search | ж | | |
| 0 Secure Group Tag(s) select | od for Add | | Add |
| Secure Group Tag Name | SGT Number | SGT Description | Select All |
| Production_Servers | 15 | Production Servers Security Group | 0 |
| Point of Sale Systems | 10 | Point of Sale Security Group | 0 |
| Test_Servers | 13 | Test Servers Security Group | 0 |
| Development_Servers | 12 | Development Servers Security Group | 0 |
| BYOD | 15 | 8YOO Security Group | 0 |
| PCI_Servers | 14 | PCI Servers Security Group | 0 |
| Guesta | 6 | Guest Security Group | 0 |
| ANY | 65535 | Any Security Group | 0 |
| Unknown | 0 | Unknown Security Group | 0 |
| Network_Services | 3 | Network Services Security Group | 0 |
| InustSec_Devices | 2 | TrustSec Devices Security Group | 0 |
| Cluster1_Endpoints | 191 | Endpoints residing in ISE Cluster-1 | |
| Employees | 4 | Employee Security Group | |

Paso 9. Haga clic en Finalizado para volver.

Paso 10. Enviar y confirmar.

Configuración del switch

AAA

```
aaa new-model
aaa group server radius ISE
server name ise01-cl1
server name ise02-cl1
ip radius source-interface Vlan50
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting update newinfo periodic 2440
aaa accounting dot1x default start-stop group ISE
aaa server radius dynamic-author
client 10.50.50.120 server-key Cisco123
client 10.50.50.121 server-key Cisco123
auth-type any
radius server ise01-cl1
address ipv4 10.50.50.121 auth-port 1812 acct-port 1813
pac key Ciscol23
radius server ise02-cl1
address ipv4 10.50.50.120 auth-port 1812 acct-port 1813
pac key Cisco123
```

TrustSec

cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode) cts role-based enforcement

aaa authorization network cts-list group ISE cts authorization list cts-list

Verificación

Asignación SGT de ISE a terminal.

Aquí puede ver un terminal del ISE Cluster 1 asignado a una SGT después de una autenticación y autorización exitosas:

| | v | | 100-170 | Endpoint D | Endpoint Profile | Autorisation Policy | Automization Policy | Autorisation Profiles | P Adres v | Bearly Drog | lar-ar |
|--------------------------|---|---|---------------|------------|------------------|---|---------------------|-----------------------|-------------|-----------------|----------|
| Jac 14, 2022 12 07 48 38 | | + | manufacture . | 1410100 | NP-Decise | $\operatorname{Hirst} \operatorname{Access} \to \mathbb{D}_+$ | $\max \max = 1.$ | Aug | 10.00.00.10 | Daniel Jodgerma | 1007-017 |

Aquí puede ver un terminal del ISE Cluster 2 asignado a una SGT después de una autenticación y autorización exitosas:

V
 Merry Depend D Depend Pulls
 Anti-relation Pullsy
 Anti-relation
 Anti-relation

Asignaciones SXP

Dado que la comunicación SXP está habilitada entre los nodos ISE del clúster y el nodo de agregación ISE, estos mapeos SGT-IP son aprendidos por la agregación ISE a través de SXP:

| III Cieco (56) | | Work Centers | TrustSec | | A Deservice | • • • • • • |
|--------------------------------|-----------------------|---|---|---|----------------------------------|--|
| Overview Components | Trustles Policy Polic | 54 50P AD | Southeatout Reports | Settings | | |
| 107 Januari Mi 107 Magginga | All SXP Mapp | ings o | | | | |
| | Distant Are bet base | en fitter - Marsage (197 (Suran fit | | hard and a | <u></u> _/ | View v . 0 |
| | | | | | | |
| | IP Address | HUT . | VN Learned P | rum Learned By | SNP Domain | PDNs involved |
| | P Address 1 | Nation Jacob (1991) | VN Learned P | tem Lawred By | DRP Domain | PDNs involved |
| | P Address 1 | Not Decise (2002) Not Decise (2002) | VN Loamed P | Learned By L.10.00.00.0 SHP L.10.00.00.7 SHP | BRP Domain default default | PDRs Involved 1++102 1++102 |
| | P Address 1 | Not Traction_Dension (2000) Traction_Dension (2000) Contert_Direction (2000) | VN Lawred F 10.00.00.10 10.00.00.10 | Lawred By CULMENS SHP CULMENS SHP CULMENS SHP | BR bonain ortext ortext | P5Ns toolved 10-100 10-100 10-100 |

Estas asignaciones SXP, de diferentes clústeres de ISE, se envían a WSA a través de pxGrid a través del nodo de agregación ISE:



Aplicación de políticas basada en SGT

Aquí puede ver que los diferentes terminales coinciden con sus respectivas políticas y el tráfico se bloquea en función de su SGT:

Extremo que pertenece al clúster 1 de ISE



| Results | | | | | | |
|-------------------------|--|------------------------|----------------|-----------|---|--------------------------|
| | | | | | Items Displayed 5 | 0 ¥ |
| Displaying 1 - 50 of 13 | 7 items. | | | | Previous 1 2 3 1 | Net - |
| Time (GRT +02:00) ¥ | Website (court) | Display All Details | Disposition | Bandwidth | User / Client IP | |
| 54 34 2022 54 28 57 | https://bbc.com/dd2/farioshice content mills de. Caroonin Block UKLs CL1 Destruction III - Ortanis Decryster Rolen 1958_Clar Malware Analytics File Verdict - | ber1", WBRS: No Score, | Block - URL CH | 08 | iseng_10.50.50.121_sgf111_10.50 (Identified b 10.50 | 50.12 y 198) 50.12 |

Extremo que pertenece al ISE Cluster 2



Información Relacionada

- Guía de integración de Web Security Appliance e Identity Service Engine
- <u>Configuran la integración de WSA con ISE para TrustSec Aware Services</u>
- Guía del administrador de Cisco Identity Services Engine, versión 3.1
- Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance