Configuración de la integración de Active Directory con ASDM para el inicio de sesión único y la autenticación de portal cautivo (administración integrada)

Contenido

Introducción

Este documento describe la configuración de la autenticación del portal cautivo (autenticación activa) y el inicio de sesión único (autenticación pasiva) en Firepower Module mediante ASDM (administrador adaptable de dispositivos de seguridad).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del firewall ASA (Adaptive Security Appliance) y ASDM
- Conocimiento del módulo FirePOWER
- Servicio de directorio ligero (LDAP)
- Agente de usuario Firepower

Componentes Utilizados

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

- Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecutan la versión de software 5.4.1 y superiores.
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) que ejecuta la versión de software 6.0.0 y posterior.

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. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

La autenticación de portal cautiva o la autenticación activa solicita una página de inicio de sesión y se necesitan credenciales de usuario para que un host obtenga acceso a Internet.

La autenticación de inicio de sesión único o pasiva proporciona una autenticación sin problemas a un usuario para los recursos de red y el acceso a Internet sin introducir credenciales de usuario varias veces. La autenticación de inicio de sesión único se puede lograr mediante Firepower user agent o la autenticación del navegador NTLM.

> **Nota**: Captive Portal Authentication, ASA debe estar en modo ruteado.

> **Nota:** El comando Captive Portal está disponible en ASA versión 9.5(2) y posterior.

Configurar

Paso 1. Configure el agente de usuario Firepower para el inicio de sesión único.

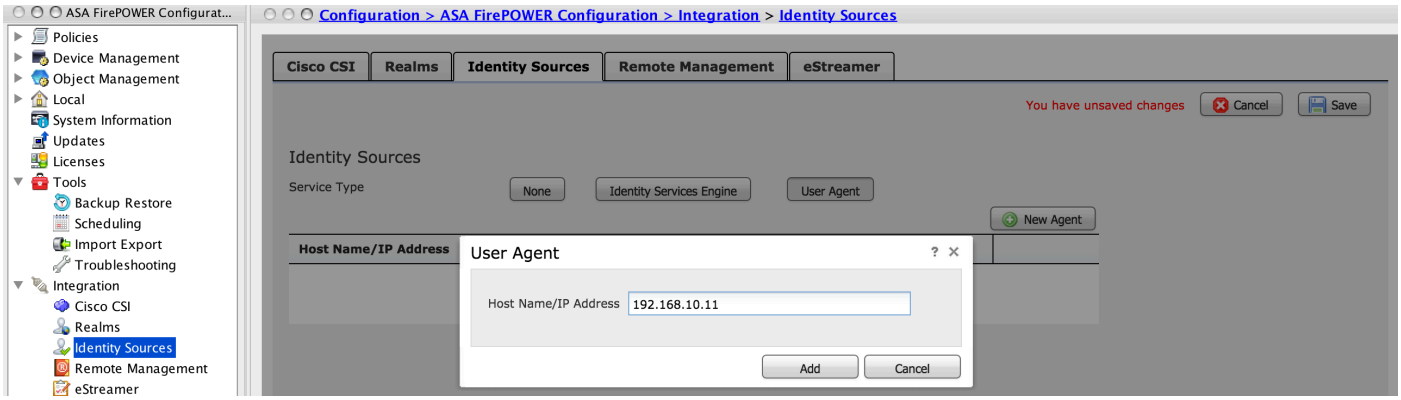
En este artículo se explica cómo configurar Firepower User Agent en la máquina con Windows:

[Instalación y desinstalación del agente de usuario de Sourcefire]

Paso 2. Integre el módulo Firepower (ASDM) con el agente de usuario.

Inicie sesión en ASDM, navegue hasta **Configuration > ASA FirePOWER Configuration > Integration > Identity Sources** y haga clic en la opción **User Agent**. Después de hacer clic en la opción **User Agent** y configurar la dirección IP del sistema User Agent. haga clic en **Agregar**,

como se muestra en la imagen:



Haga clic en el botón **Guardar** para guardar los cambios.

Paso 3. Integre Firepower con Active Directory.

Paso 3.1 Crear el rango.

Inicie sesión en ASDM, navegue hasta **Configuration > ASA FirePOWER Configuration > Integration > Realms.** Haga clic en **Agregar un nuevo rango**.

Nombre y descripción: introduzca un nombre o una descripción para identificar de forma única el rango.

Tipo: AD

Dominio primario de AD: Nombre de dominio de Active Directory (Nombre NETBIOS).

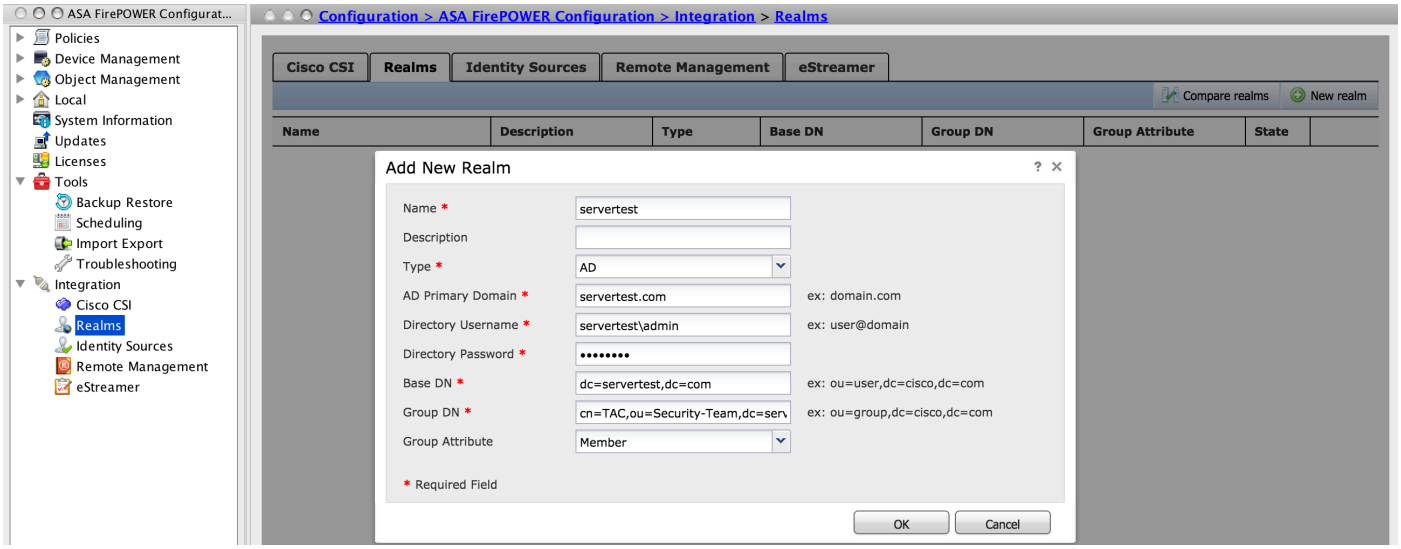
Nombre de usuario del directorio: Especifique el <*username*>.

Contraseña del directorio: Especifique la <*contraseña*>.

DN base: Dominio o DN OU específico desde donde el sistema iniciará una búsqueda en la base de datos LDAP.

DN de grupo: Especifique el DN del grupo.

Atributo de grupo: Especifique la opción Miembro de la lista desplegable.



Haga clic en **Aceptar** para guardar la configuración.

Este artículo puede ayudarle a descubrir los valores DN base y DN de grupo.

[Identificar atributos de objetos LDAP de Active Directory]

Paso 3.2 Agregue la dirección IP/nombre de host del servidor de directorio.

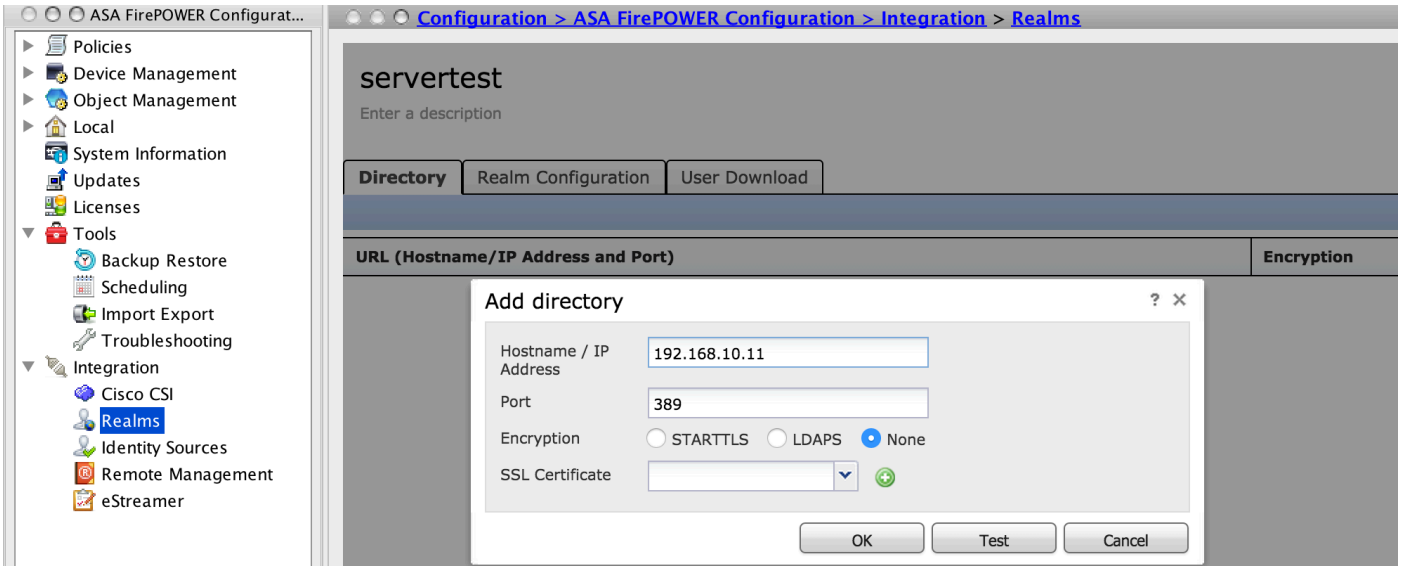
Para especificar AD Server IP/hostname, haga clic en **Add directory**.

Nombre de host/Dirección IP: configure la dirección IP/nombre de host del servidor AD.

Puerto: Especifique el número de puerto LDAP de Active Directory (Default 389).

Certificado de cifrado/SSL: (opcional) Para cifrar la conexión entre el servidor FMC y AD, consulte este artículo:

[Verificación del objeto de autenticación en el sistema FireSIGHT para la autenticación de Microsoft AD sobre SSL/T...]



Haga clic **Prueba** para verificar la conexión de FMC con el servidor AD. Ahora haga clic en **Aceptar** para guardar la configuración.

Paso 3.3 Modificación de la configuración de rango.

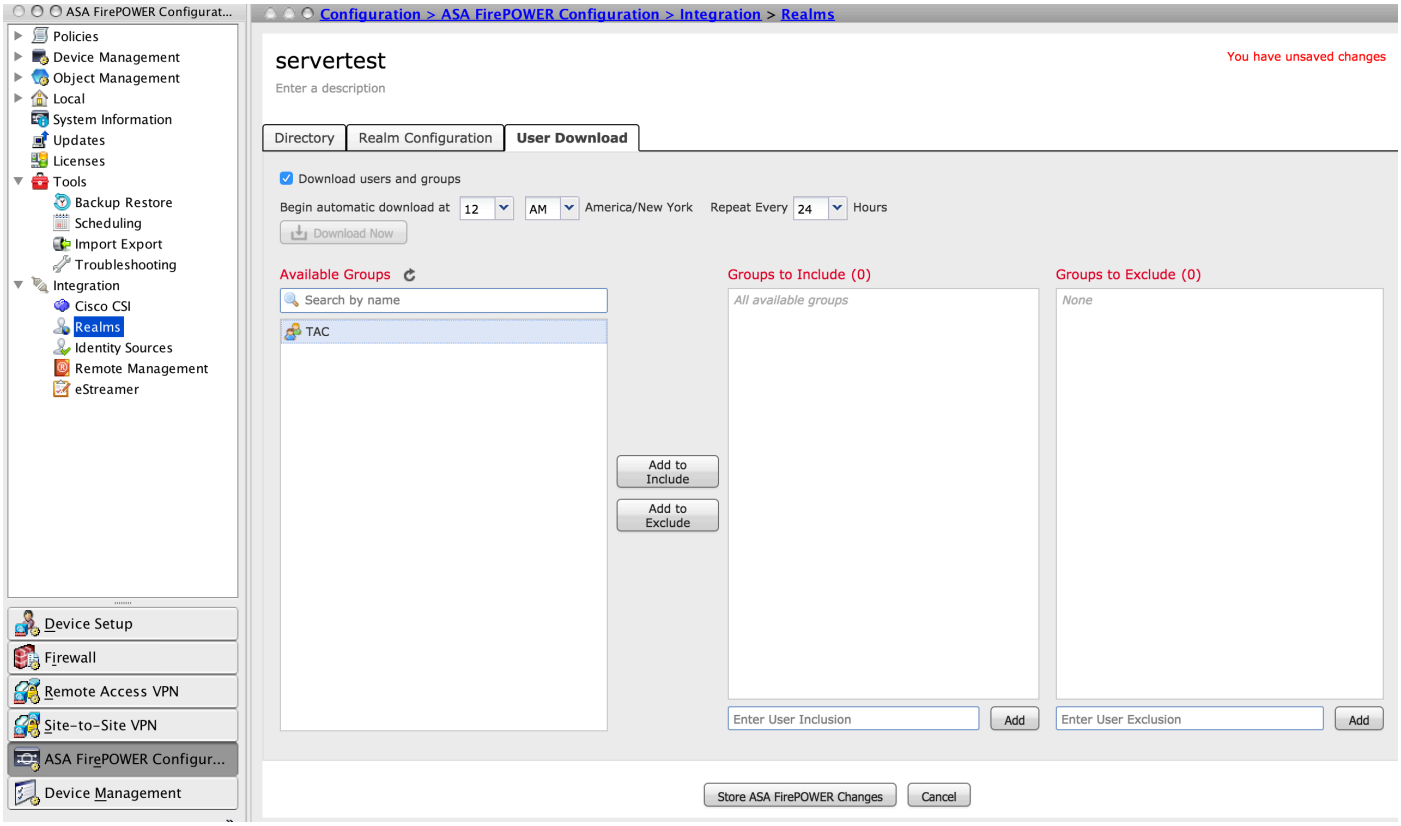
Para modificar y verificar la configuración de integración del servidor AD, navegue hasta **Configuración de rango**.

Paso 3.4 Descargar base de datos de usuarios.

Navegue hasta **Descarga de usuario** para obtener la base de datos de usuario del servidor AD.

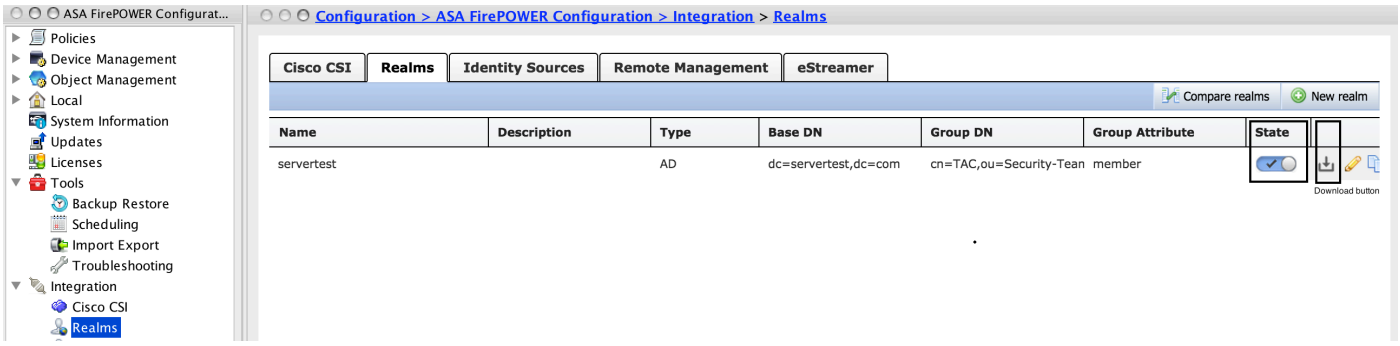
Active la casilla de verificación para descargar **Descargar usuarios y grupos** y definir el intervalo de tiempo sobre la frecuencia con la que el módulo Firepower se pone en contacto con el servidor AD para descargar la base de datos del usuario.

Seleccione el grupo y agréguelo a la opción **Include** para la que desea configurar la autenticación. De forma predeterminada, todos los grupos se seleccionan si no desea incluir los grupos.



Haga clic en **Store ASA Firepower Changes** para guardar la configuración del rango.

Active el estado del rango y haga clic en el botón de descarga para descargar los usuarios y grupos, como se muestra en la imagen.



Paso 4. Configure la política de identidad.

Una política de identidad realiza la autenticación de usuario. Si el usuario no se autentica, se deniega el acceso a los recursos de red. De este modo, se aplica el control de acceso basado en roles (RBAC) a la red y los recursos de su organización.

Paso 4.1 Portal cautivo (Autenticación activa).

Active Authentication solicita el nombre de usuario y la contraseña en el navegador para identificar una identidad de usuario que permita cualquier conexión. El explorador autentica al usuario mediante la presentación de la página de autenticación o se autentica silenciosamente con la autenticación NTLM. NTLM utiliza el navegador web para enviar y recibir información de autenticación. Active Authentication utiliza varios tipos para verificar la identidad del usuario. Los diferentes tipos de autenticación son:

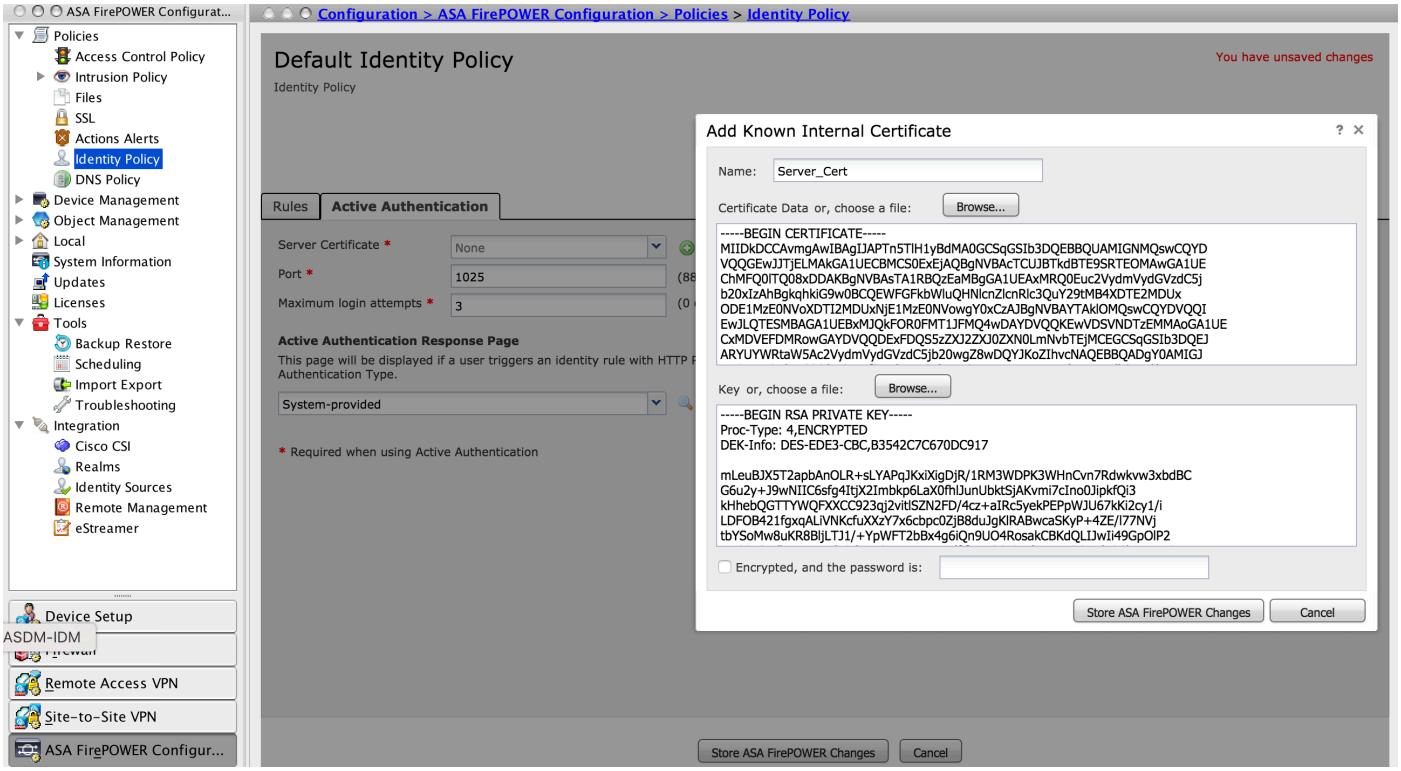
1. **HTTP Basic: En este método, el explorador solicita las credenciales del usuario.**
2. **NTLM: NTLM utiliza las credenciales de la estación de trabajo de windows y las negocia con Active Directory mediante un navegador web. Debe habilitar la autenticación NTLM en el explorador. La autenticación de usuario se realiza de forma transparente sin solicitar credenciales. Proporciona una experiencia de inicio de sesión único para los usuarios.**
3. **Negociación HTTP:** En este tipo, el sistema intenta autenticarse utilizando NTLM, si falla, el sensor utiliza el tipo de autenticación HTTP Basic como método de reserva y solicita un cuadro de diálogo para las credenciales del usuario.
4. **Página de respuesta HTTP: Esto es similar al tipo básico de HTTP; sin embargo, aquí se le solicita al usuario que rellene la autenticación en un formulario HTML que se puede personalizar.**

Cada navegador tiene una manera específica de habilitar la autenticación NTLM y, por lo tanto, puede seguir las pautas del navegador para habilitar la autenticación NTLM.

Para compartir las credenciales de forma segura con el sensor ruteado, debe instalar el certificado de servidor autofirmado o el certificado de servidor firmado públicamente en la política de identidad.

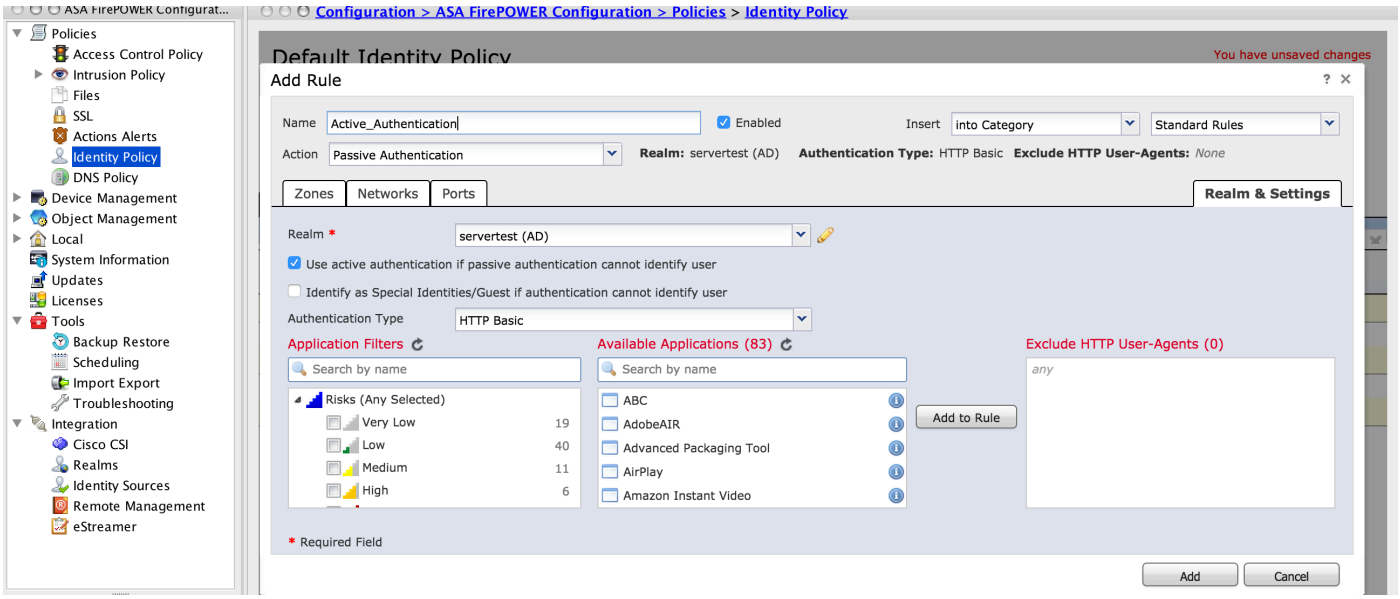
```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
               openssl genrsa -des3 -out server.key 2048

Step 2.   Generate Certificate Signing Request (CSR)
               openssl req -new -key server.key -out server.csr

Step 3.   Generate the self-signed Certificate.
openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

Vaya a **Configuración > Configuración de ASA FirePOWER > Políticas > Política de identidad**. Ahora desplácese a la ficha **Autenticación activa** y, en la opción **Certificado de servidor**, haga clic en el **icono (+)** y cargue el certificado y la clave privada que ha generado en el paso anterior utilizando openSSL, como se muestra en la imagen:



Ahora haga clic en **Agregar regla** para dar un nombre a la regla y elija la acción como **Autenticación activa**. Defina la zona de origen/destino, la red de origen/destino para la que desea habilitar la autenticación de usuario.

Vaya a la pestaña **Rango y configuración**. Seleccione el **rango** de la lista desplegable que ha configurado en el paso anterior y seleccione el **tipo de autenticación** de la lista desplegable que mejor se adapte a su entorno de red.



Paso 4.2 Configuración de ASA para el portal cautivo.

Paso 1. Defina el tráfico interesante que se redirigirá a Sourcefire para su inspección.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
```

```
ASA(config-cmap)# match access-list SFR_ACL


ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

Paso 2. Configure este comando en el ASA para habilitar el portal cautivo.

```
ASA(config)# captive-portal interface inside port 1025
```

> **Consejo:** el portal cautivo se puede habilitar globalmente o por interfaz.

> **Consejo:** Asegúrese de que el puerto del servidor, TCP 1025, esté configurado en la opción de puerto de la ficha Autenticación activa de la política de identidad.

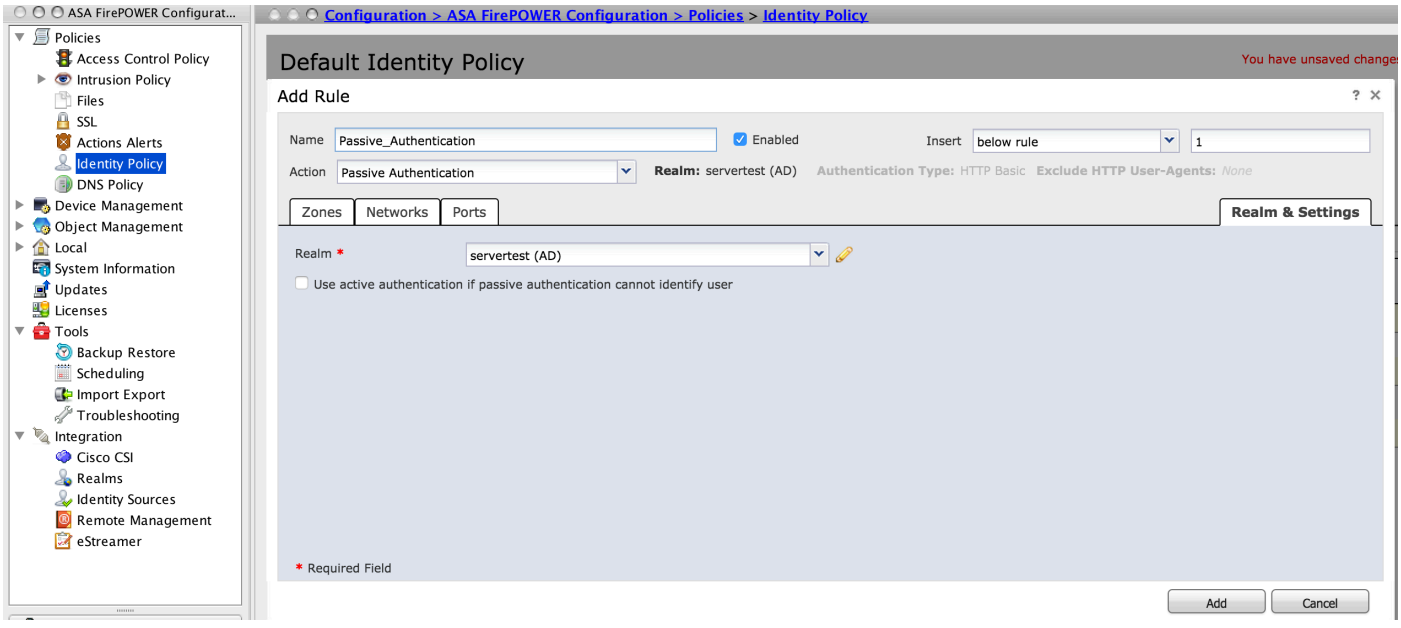
Paso 4.3 Inicio De Sesión Único (Autenticación Pasiva).

En la autenticación pasiva, cuando un usuario de dominio inicia sesión y puede autenticar el AD, Firepower User Agent sondea los detalles de la asignación de IP de usuario de los registros de seguridad de AD y comparte esta información con Firepower Module. El módulo Firepower utiliza estos detalles para aplicar el control de acceso.

Para configurar la regla de autenticación pasiva, haga clic en **Agregar regla** para dar un nombre a la regla y luego elija la **Acción** como **Autenticación pasiva**. Defina la zona de origen/destino, la red de origen/destino para la que desea habilitar la autenticación de usuario.

Vaya a la **Rango y configuración** . Seleccione el **Rango** de la lista desplegable que ha configurado en el paso anterior.

Aquí puede elegir el método de repliegue como **autenticación activa si la autenticación pasiva no puede identificar la identidad del usuario**, como se muestra en la imagen:



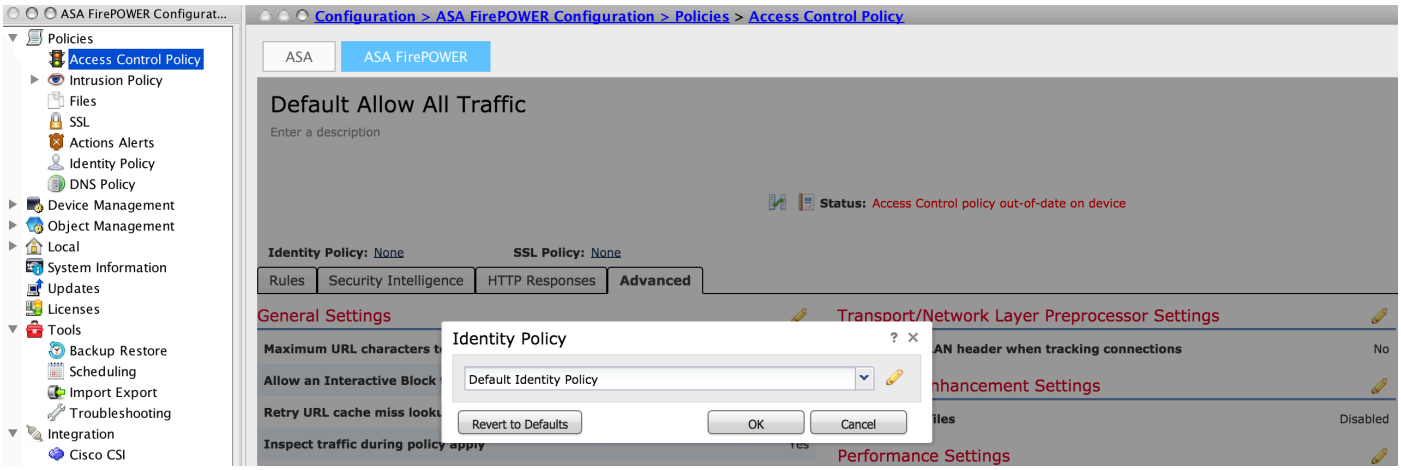
Ahora haga clic en **Store ASA Firepower Changes** para guardar la configuración de la política de

identidad.

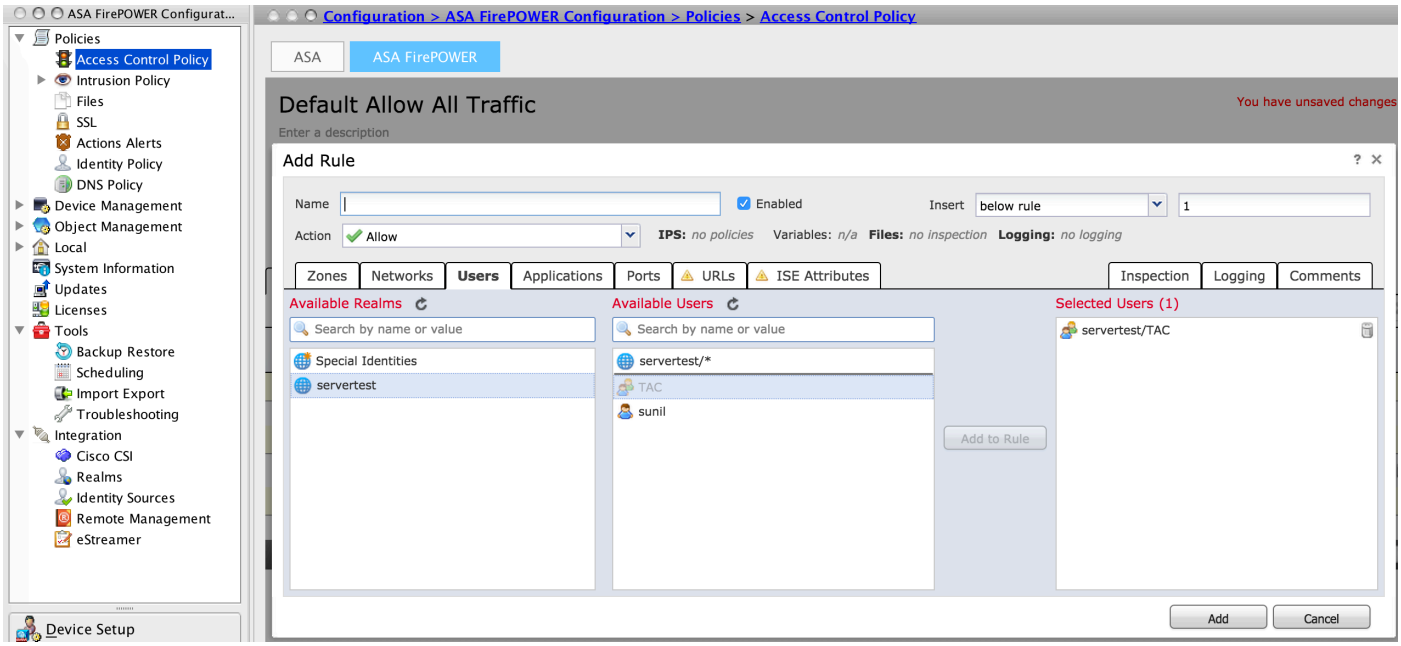
Paso 5. Configure la política de control de acceso.

Vaya a **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy .**

Haga clic en la **Política de identidad** (esquina superior izquierda), seleccione la Política de identificación que ha configurado en el paso anterior en la lista desplegable y haga clic en **Aceptar**, como se muestra en esta imagen.



Haga clic en **Agregar regla** para agregar una nueva regla, vaya a **Usuarios** y seleccione los usuarios para los que se aplicará la regla de control de acceso, como se muestra en esta imagen y haga clic en **Agregar**.



Haga clic en **Almacenar cambios en el firewall ASA** para guardar la configuración de la política de control de acceso.

Paso 6. Implemente la política de control de acceso.

Debe implementar la política de control de acceso. Antes de aplicar la política, verá una indicación de Directiva de control de acceso desactualizada en el módulo. Para implementar los cambios en el sensor, haga clic en **Implementar** y elija la **opción Implementar cambios de FirePOWER** y luego

haga clic en **Implementar** en la ventana emergente.

> **Nota:** En la versión 5.4.x, para aplicar la política de acceso al sensor, debe hacer clic en Aplicar cambios de ASA FirePOWER

> **Nota:** Vaya a Monitoring > ASA Firepower Monitoring > Task Status . Asegúrese de que la tarea debe completar la aplicación del cambio de configuración.

Paso 7. Supervisar eventos de usuario.

Vaya a **Monitoring > ASA FirePOWER Monitoring > Real-Time Event**, para supervisar el tipo de tráfico que utiliza el usuario.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Navegue hasta **Análisis > Usuarios** para verificar la regla de acceso/autenticación de usuario/asignación de IP de usuario asociada con el flujo de tráfico.

Conectividad entre Firepower Module y User Agent (autenticación pasiva)

Firepower Module utiliza el puerto TCP 3306 para recibir los datos del registro de actividad de usuario del Agente de usuario.

Para verificar el estado de servicio del módulo Firepower, utilice este comando en el FMC.

```
admin@firepower:~$ netstat -tan | grep 3306
```

Ejecute la captura de paquetes en el FMC para verificar la conectividad con el Agente de usuario.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

Conectividad entre FMC y Active Directory

El módulo Firepower utiliza el puerto TCP 389 para recuperar la base de datos de usuario del directorio activo.

Ejecute la captura de paquetes en Firepower Module para verificar la conectividad con Active Directory.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

Asegúrese de que la credencial de usuario utilizada en la configuración de rango tenga el privilegio suficiente para obtener la base de datos de usuario de AD.

Verifique la configuración de rango y asegúrese de que los usuarios/grupos se descarguen y que el tiempo de espera de la sesión del usuario esté configurado correctamente.

Navegue hasta Supervisión del estado de la tarea de supervisión de ASA Firepower y asegúrese de que la descarga de los usuarios/grupos de tareas se complete correctamente, como se muestra en esta imagen.

Conectividad entre ASA y el sistema final (autenticación activa)

autenticación activa, asegúrese de que el certificado y el puerto estén configurados correctamente en Firepower module Identity policy y ASA (comando cautive-portal). De forma predeterminada, el módulo ASA y Firepower escuchan en el puerto TCP 885 para la autenticación activa.

Para verificar las reglas activas y sus recuentos de visitas, ejecute este comando en el ASA.

```
ASA# show asp table classify domain captive-portal

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

Implementación de políticas y configuración de políticas

Asegúrese de que los campos Rango, Tipo de autenticación, Agente de usuario y Acción estén configurados correctamente en Política de identidad.

Asegúrese de que la política de identidad está correctamente asociada a la política de control de acceso.

Vaya a Monitoring > ASA Firepower Monitoring > Task Status y asegúrese de que la implementación de políticas se complete correctamente.

Troubleshoot

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems
- Configuración de la Integración de Active Directory con Firepower Appliance para el Inicio de Sesión Único y la Autenticación de Portal cautivo