Configuración de la integración de Active Directory con el dispositivo Firepower para la autenticación de portal cautivo & de inicio de sesión único

Contenido

Introducción

Este documento describe la configuración de la autenticación del portal cautivo (autenticación activa) y el inicio de sesión único (autenticación pasiva).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivos Sourcefire Firepower
- Modelos de dispositivos virtuales
- Servicio de directorio ligero (LDAP)
- AgenteUsuarioFirepower

Componentes Utilizados

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

- Firepower Management Center (FMC) versión 6.0.0 y posteriores
- Sensor Firepower versión 6.0.0 y superior

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

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

La autenticación pasiva o de inicio de sesión único proporciona a un usuario una autenticación perfecta para los recursos de red y el acceso a Internet sin que se produzcan varias credenciales de usuario. La autenticación de inicio de sesión único se puede conseguir mediante el agente de usuario de Firepower o la autenticación de explorador NTLM.

Nota: para la autenticación de portal cautivo, el dispositivo debe estar en modo enrutado.

Configurar

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

En este artículo se explica cómo configurar Firepower User Agent en un equipo con Windows:

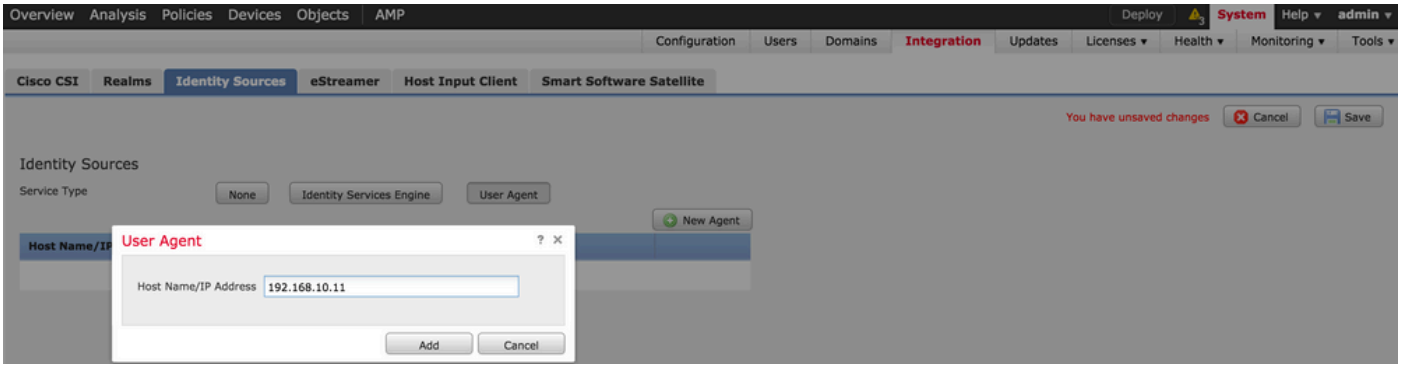
Instalación y desinstalación del agente de usuario de Sourcefire

Paso 2. Integre Firepower Management Center (FMC) con el agente de usuario

Inicie sesión en Firepower Management Center y navegue hasta System > Integration > Identity

Sources (Sistema > Integración > Orígenes de identidad). Haga clic en la opción Nuevo agente. Configure la dirección IP del sistema Agente de usuario y haga clic en el botón Agregar.

Haga clic en el botón Save para guardar los cambios.



Paso 3. Integre Firepower con Active Directory

Paso 3.1 Crear el rango

Inicie sesión en el FMC y navegue hasta System > Integration > Realm. Haga clic en la opción Add New Realm.

Nombre y descripción: proporcione un nombre o una descripción para identificar el rango de forma exclusiva.

Tipo: AD

Dominio principal de AD: nombre de dominio de Active Directory

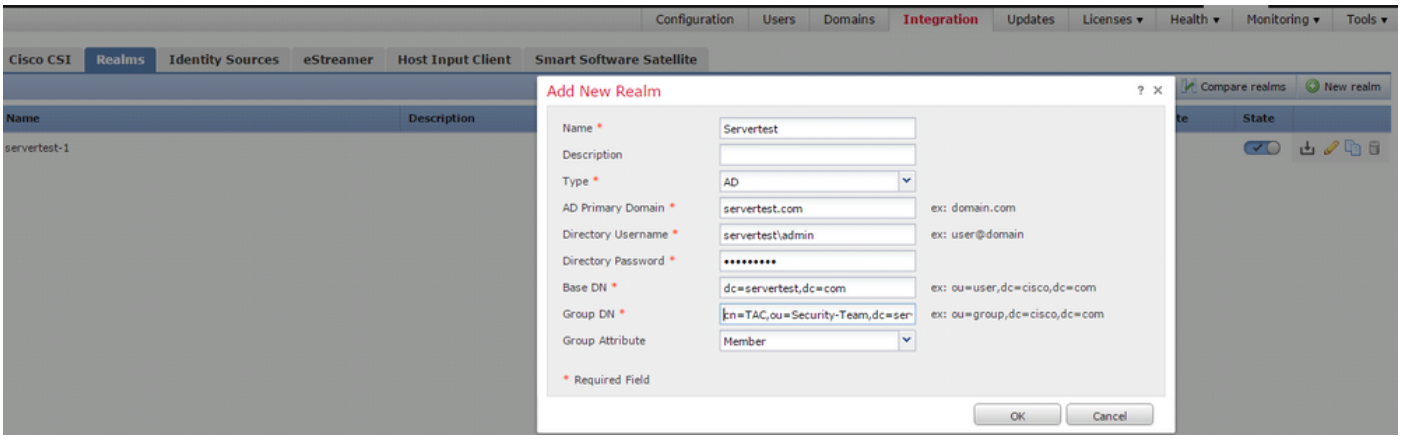
Nombre de usuario del directorio: <username>

Contraseña del directorio: <password>

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

Grupo DN: grupo DN

Atributo de grupo: Miembro



Este artículo le ayuda a calcular los valores de DN base y DN de grupo.

Identificar atributos de objeto LDAP de Active Directory

Paso 3.2 Agregar el Servidor de Directorios

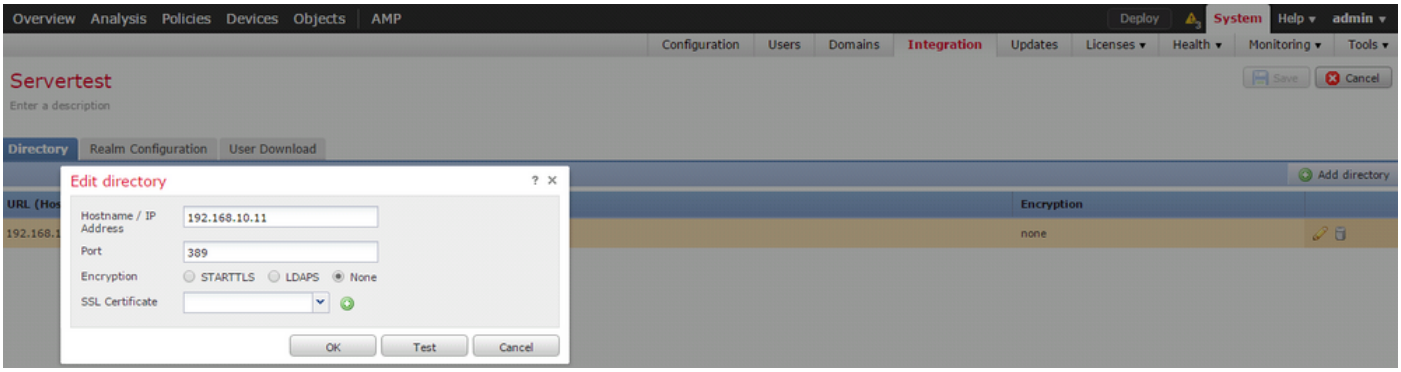
Haga clic en el botón Add para navegar al siguiente paso y luego haga clic en la opción Add directory.

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

Puerto: 389 (número de puerto LDAP de Active Directory)

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

artículo: Verificación del objeto de autenticación en el sistema FireSIGHT para la autenticación de Microsoft AD sobre SSL/TLS



Haga clic en el botón Test para verificar si FMC puede conectarse al servidor AD.

Paso 3.3 Modificar la Configuración de Rango

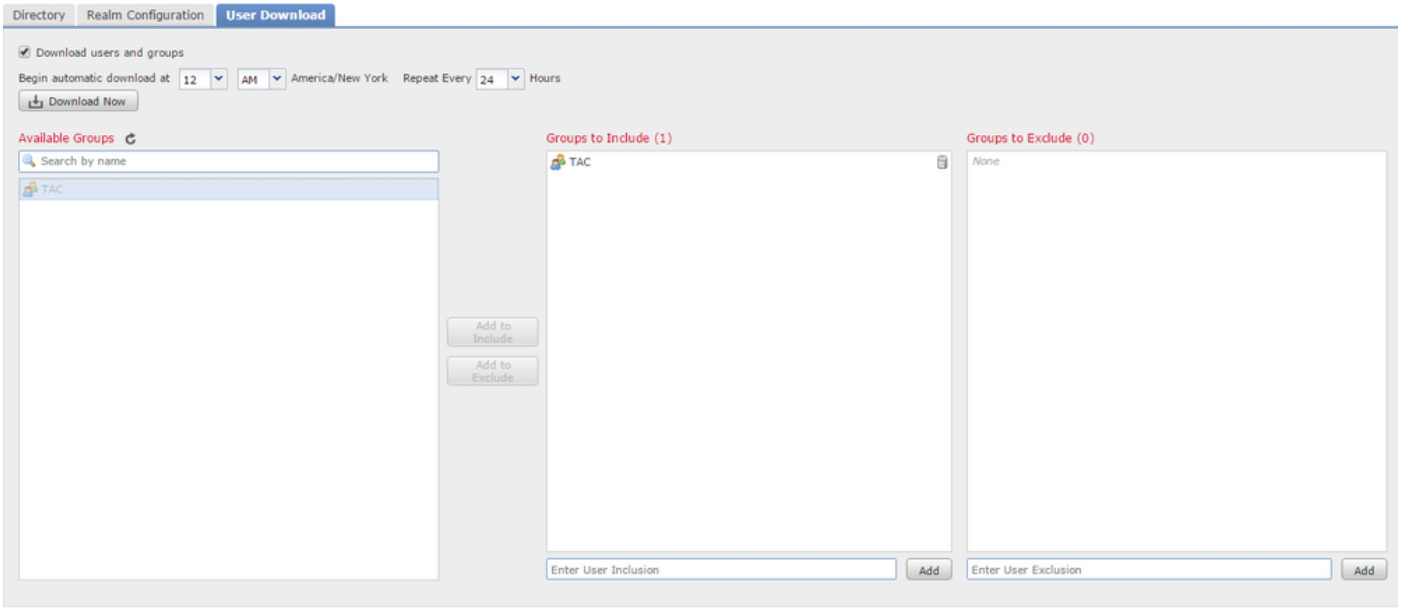
Navegue hasta Configuración de rango para verificar la configuración de integración del servidor AD y puede modificar la configuración de AD.

Paso 3.4 Descargar la base de datos de usuarios

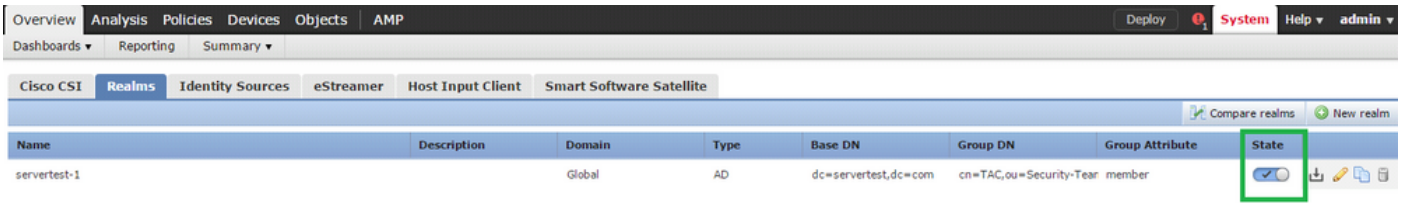
Navegue hasta la opción User Download para obtener la base de datos de usuarios del servidor AD.

Active la casilla de verificación para descargar Descargar usuarios y grupos y defina el intervalo de tiempo sobre la frecuencia con que FMC se pone en contacto con AD para descargar la base de datos de usuarios.

Seleccione el grupo y colóquelo en la opción Include para el que desea configurar la autenticación.



Como se muestra en la imagen, habilite el estado AD:



Paso 4. Configuración de 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. Esto 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)

La autenticación activa solicita un nombre de usuario/contraseña en el navegador para identificar una identidad de usuario que permita cualquier conexión. El explorador autentica al usuario con una página de autenticación o autentica de forma silenciosa con la autenticación NTLM. NTLM utiliza el explorador web para enviar y recibir información de autenticación. La autenticación activa utiliza varios tipos para verificar la identidad del usuario. Los diferentes tipos de autenticación son:

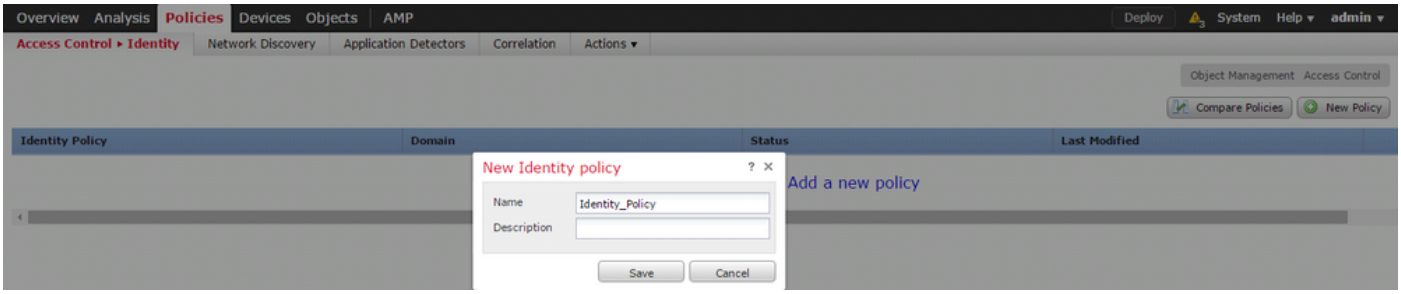
1. HTTP básico: en este método, el explorador solicita las credenciales del usuario.
2. NTLM: NTLM utiliza credenciales de estación de trabajo de Windows y las negocia con Active Directory a través de un explorador Web. Debe activar la autenticación NTLM en el explorador. La autenticación de usuario se realiza de forma transparente sin solicitudes de credenciales. Proporciona una experiencia de inicio de sesión único para los usuarios.
3. HTTP Negotiate:En este tipo, el sistema intenta autenticarse con NTLM. Si se produce un error, el sensor utiliza el tipo de autenticación básica de HTTP como método de reserva y solicita credenciales de usuario a un cuadro de diálogo.
4. Página de respuesta HTTP: es similar al tipo básico de HTTP; sin embargo, en este caso se solicita al usuario que rellene la autenticación en un formulario HTML que se puede personalizar.

Cada navegador tiene una forma específica de habilitar la autenticación NTLM y, por tanto, se adhieren a las directrices del navegador para habilitar la autenticación NTLM.

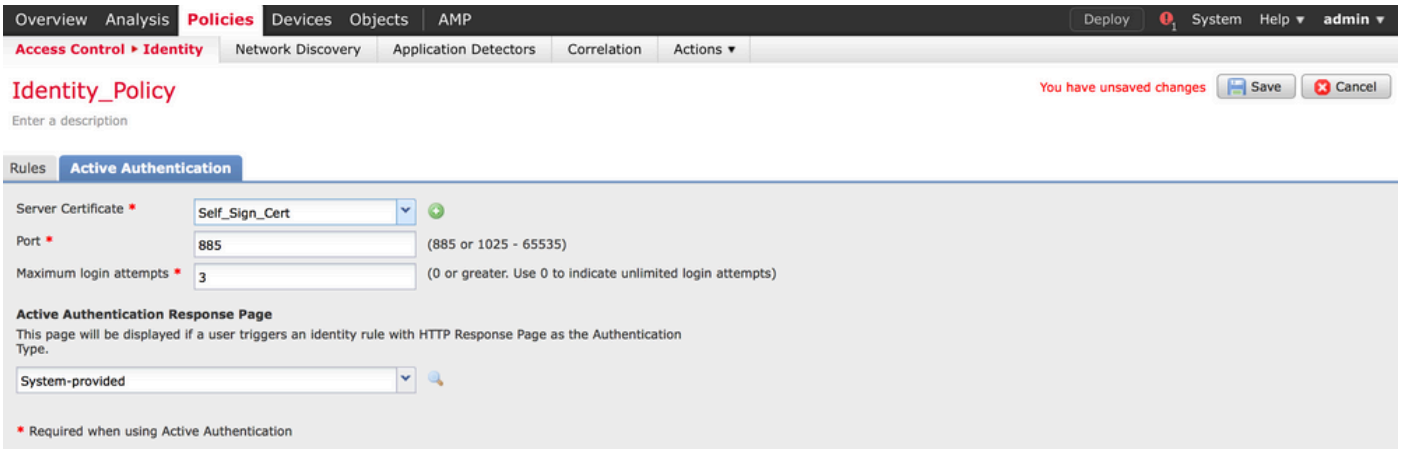
Para compartir de forma segura la credencial con el sensor enrutado, debe instalar un certificado de servidor autofirmado o un certificado de servidor firmado públicamente en la directiva de identidad.

```
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 Políticas > Control de acceso > Identidad. Haga clic en Add Policy y asigne un nombre a la política y guárdela.

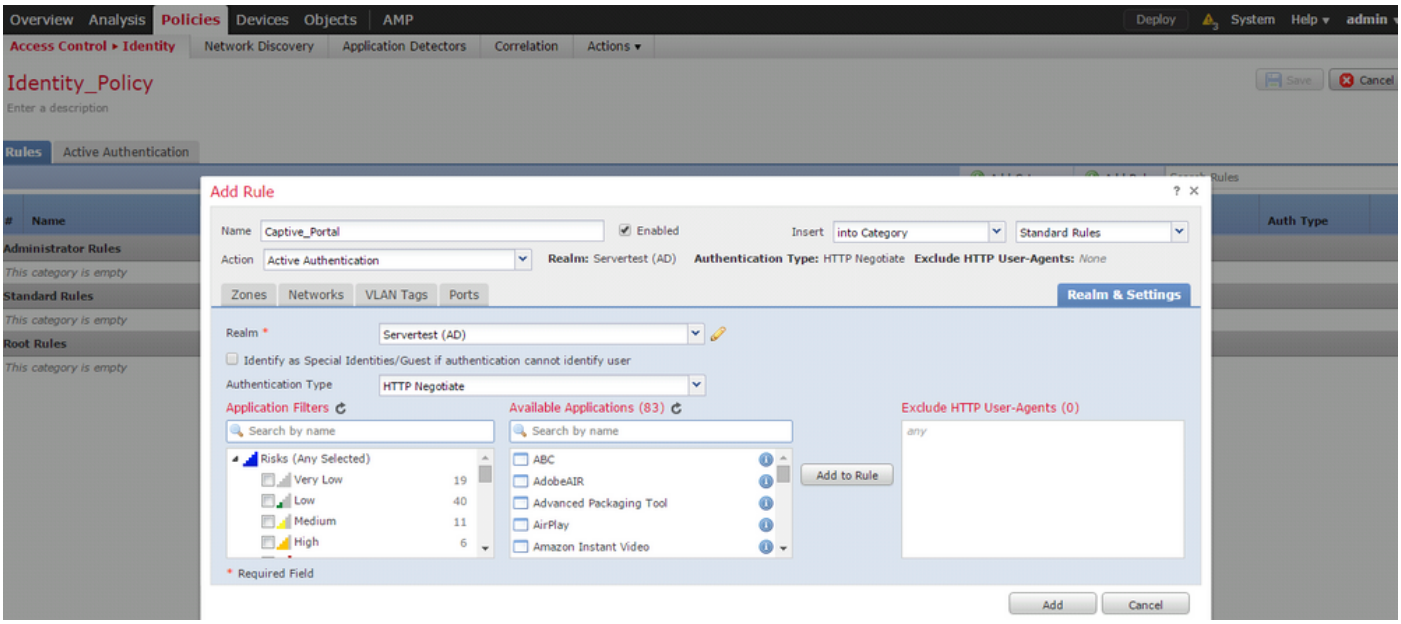


Navegue hasta la pestaña Active Authentication y en la opción Server Certificate, haga clic en el icono (+) y cargue el certificado y la clave privada que generó en el paso anterior con openSSL.



Ahora haga clic en el botón Add rule y asigne un nombre a la regla y elija la acción como Active Authentication. Defina la zona de origen/destino, la red de origen/destino para la que desea habilitar la autenticación de usuario.

Seleccione el rango que ha configurado en el paso anterior y el tipo de autenticación que mejor se adapte a su entorno.



Configuración de ASA para el portal cautivo

Para el módulo Firepower ASA, configure estos comandos en ASA para configurar el portal cautivo.

```
ASA(config)# captive-portal global port 1055
```

Asegúrese de que el puerto del servidor, TCP 1055, esté configurado en la opción port de la pestaña Identity Policy Active Authentication.

Para verificar las reglas activas y sus conteos de aciertos, ejecute el comando:

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

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

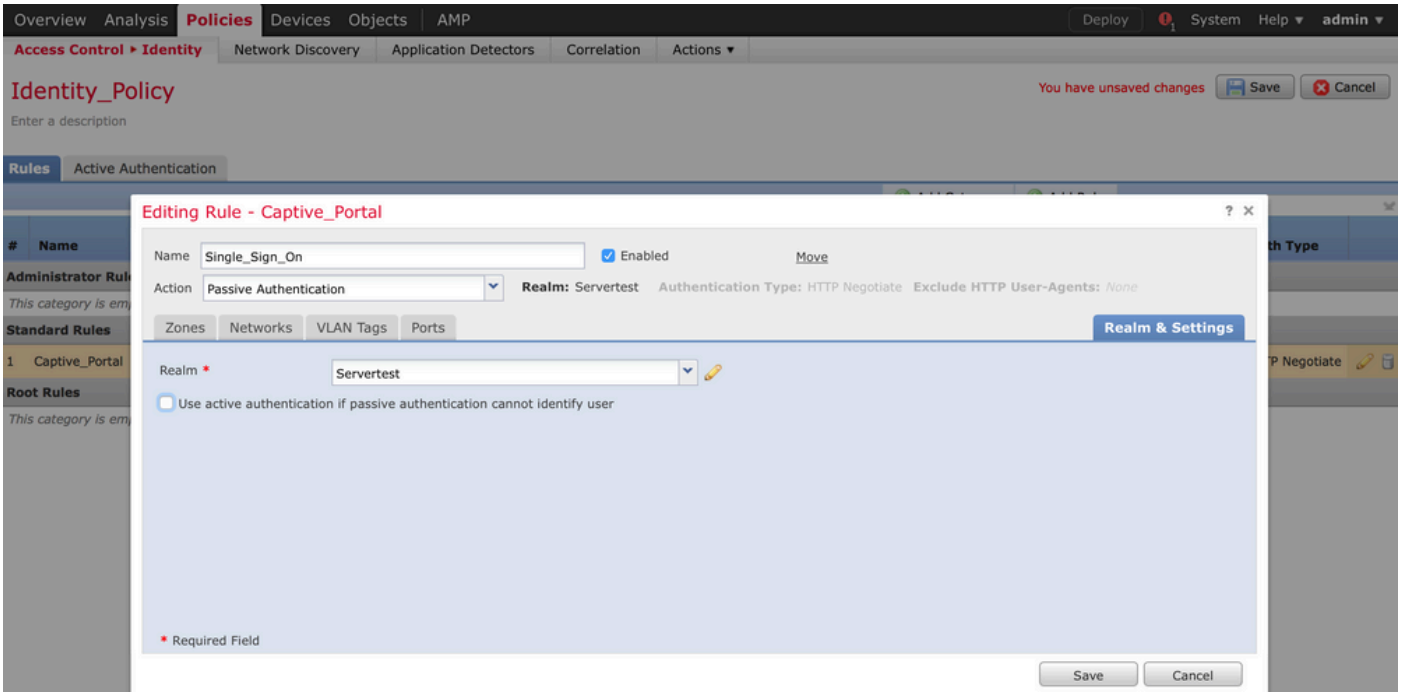
Paso 4.2 Inicio de sesión único (autenticación pasiva)

En la autenticación pasiva, cuando un usuario de dominio inicia sesión y puede autenticar el AD, el agente de usuario de Firepower sondea los detalles de asignación de IP de usuario de los registros de seguridad de AD y comparte esta información con Firepower Management Center (FMC). FMC envía estos datos al sensor para aplicar el control de acceso.

Haga clic en el botón Agregar regla y asigne un nombre a la regla y 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.

Seleccione el rango que ha configurado en el paso anterior y el tipo de autenticación que mejor se adapte a su entorno, como se muestra en esta imagen.

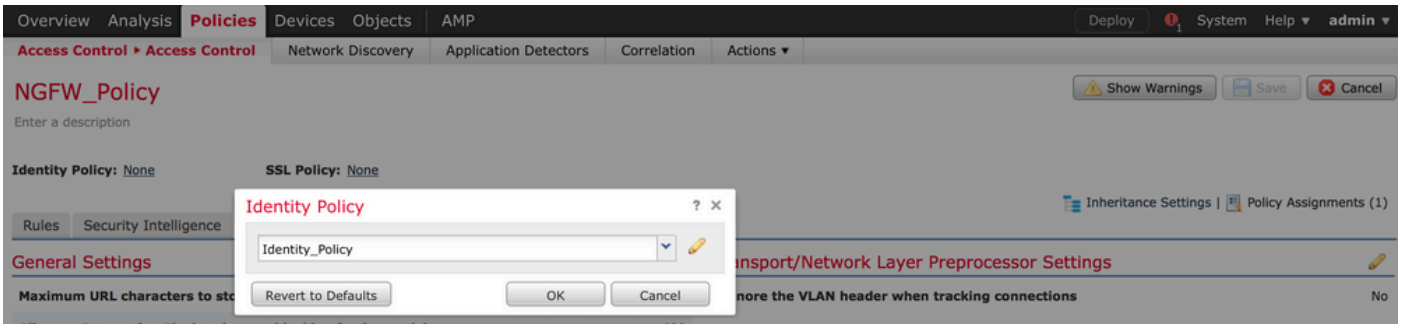
Aquí puede elegir el método de repliegue como autenticación activa si la autenticación pasiva no puede identificar la identidad del usuario.



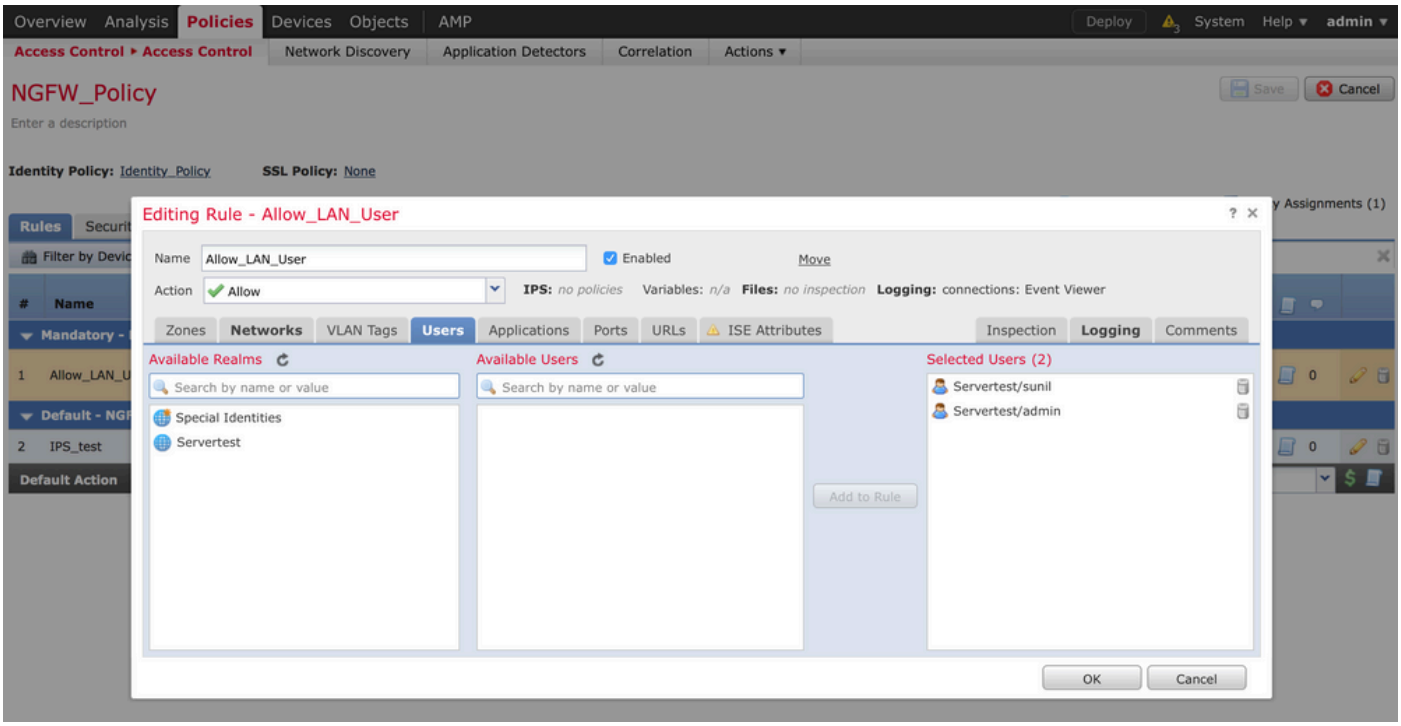
Paso 5. Configuración de la Política de Control de Acceso

Vaya a Políticas > Control de acceso > Crear/editar una política.

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

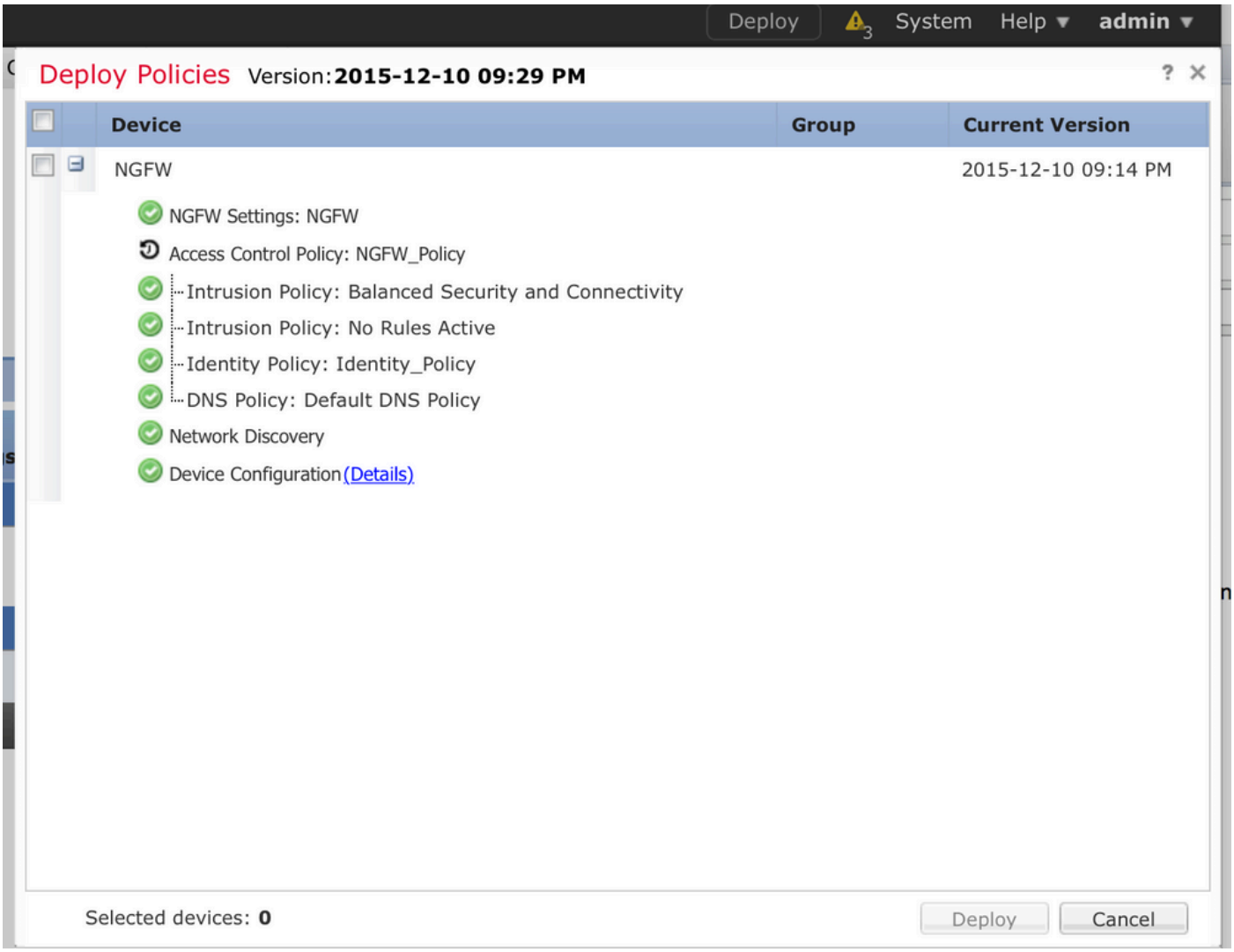


Haga clic en el botón Add rule para agregar una nueva regla. Navegue hasta Usuarios y seleccione los usuarios para los que se aplica la regla de control de acceso, como se muestra en esta imagen. Haga clic en Aceptar y haga clic en Guardar para guardar los cambios.



Paso 6. Implementar la política de control de acceso

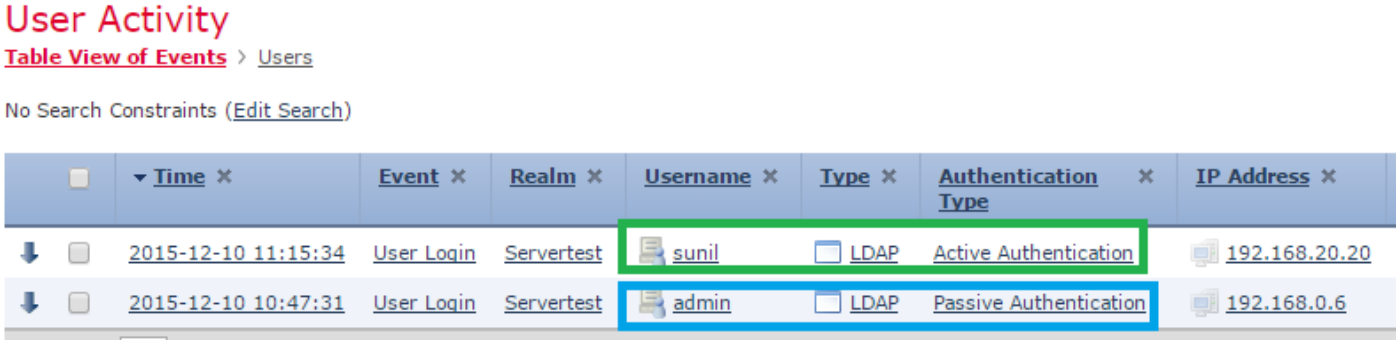
Vaya a la opción Deploy, elija el Device y haga clic en la opción Deploy para enviar el cambio de configuración al sensor. Supervise la implementación de la directiva desde la opción Message Center Icon (icono entre la opción Deploy and System) y asegúrese de que la directiva se debe aplicar correctamente, como se muestra en esta imagen.



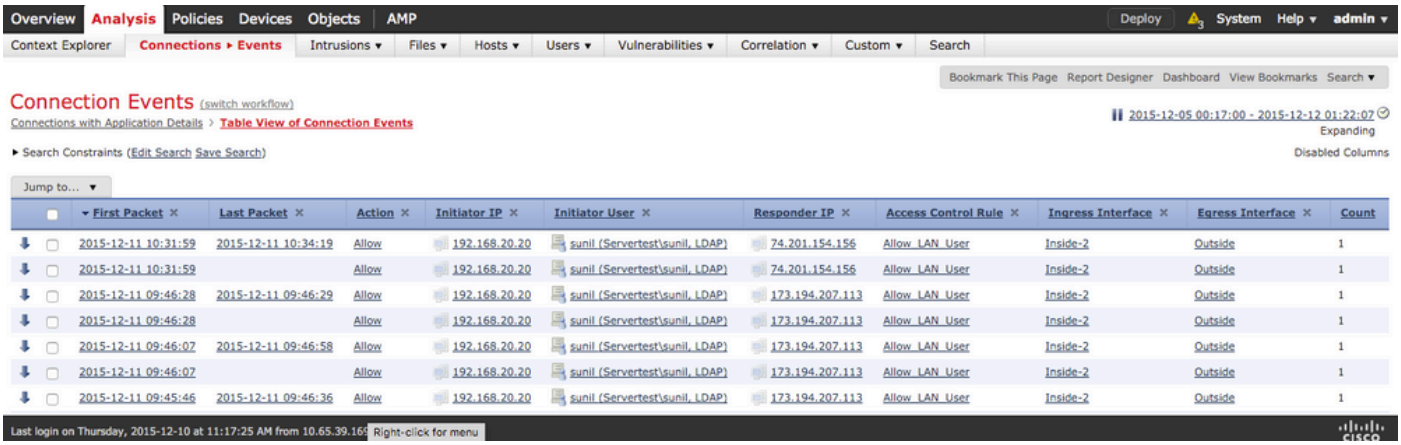
Paso 7. Supervisar eventos de usuario y eventos de conexión

Las sesiones de usuario activas actualmente están disponibles en la sección Analysis > Users > Users.

La supervisión de la actividad del usuario ayuda a averiguar qué usuario se ha asociado a qué dirección IP y cómo el sistema detecta al usuario mediante la autenticación activa o pasiva. Análisis > Usuarios > Actividad del usuario



Navegue hasta Análisis > Conexiones > Eventos, para monitorear el tipo de tráfico que utiliza el usuario.



Verificación y resolución de problemas

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

Verificar la conectividad entre FMC y el agente de usuario (autenticación pasiva)

Firepower Management Center (FMC) utiliza el puerto TCP 3306 para recibir los datos del registro de actividad del usuario desde el agente de usuario.

Para verificar el estado del servicio FMC, 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
```

Navegue hasta Análisis > Usuarios > Actividad del usuario para verificar si el FMC recibe los detalles de inicio de sesión del usuario del agente de usuario.

Verificar la conectividad entre FMC y Active Directory

FMC utiliza el puerto TCP 389 para recuperar la base de datos de usuarios del directorio activo.

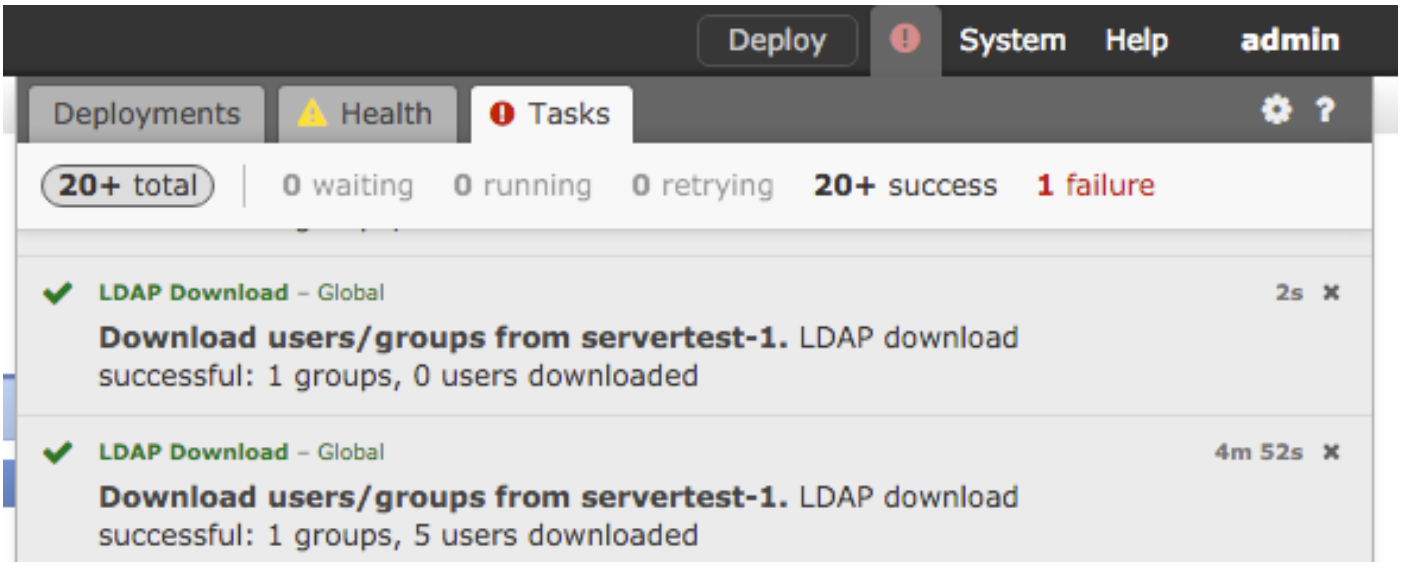
Ejecute la captura de paquetes en el FMC para verificar la conectividad con Active Directory.

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

Asegúrese de que la credencial de usuario utilizada en la configuración de rango de FMC tenga privilegios suficientes para obtener la base de datos de usuarios de AD.

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

Navegue hasta Centro de mensajes > Tareas y asegúrese de que la tarea de descarga de usuarios/grupos se complete con éxito , como se muestra en esta imagen.



Verificar la conectividad entre el sensor Firepower y el sistema final (autenticación activa)

Para la autenticación activa, asegúrese de que el certificado y el puerto estén configurados correctamente en la política de identidad de FMC.De forma predeterminada, el sensor de Firepower escucha en el puerto TCP 885 para la autenticación activa.

Verificar la configuración y la implementación de políticas

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

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

Navegue hasta Centro de mensajes > Tareas y asegúrese de que la implementación de la política se complete con éxito.

Analizar los registros de eventos

Los eventos Connection y User Activity se pueden utilizar para diagnosticar si el inicio de sesión del usuario se ha realizado correctamente o no.Estos eventos

También puede verificar qué regla de control de acceso se aplica al flujo.

Navegue hasta Análisis > Usuario para verificar los registros de eventos de usuario.

Navegue hasta Análisis > Eventos de conexión para verificar los eventos de conexión.

Información Relacionada

- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).