¿Cómo configurar la red del dispositivo de seguridad de la red de Cisco y DLP RSA para interoperar?

Contenido

Pregunta:

¿Cómo configurar la red del dispositivo de seguridad de la red de Cisco y DLP RSA para interoperar?

Descripción:

Este documento proporciona la información extra más allá del guía del usuario de Cisco WSA AsyncOS y del Guía de despliegue de la red 7.0.2 DLP RSA para ayudar a los clientes a interoperar los dos Productos.

Descripción del producto:

El dispositivo de seguridad de la red de Cisco (WSA) es un dispositivo robusto, seguro, eficiente que protege las redes corporativas contra los programas basados en web del malware y del spyware que pueden comprometer la propiedad intelectual de la seguridad corporativa y de la exposición. El dispositivo de seguridad de la red proporciona el examen profundo del contenido de la aplicación ofreciendo Web Proxy (Proxy Web) un servicio para los protocolos de comunicación estándar tales como HTTP, HTTPS, y FTP.

La habitación DLP RSA comprende una solución completa de la prevención de la pérdida de datos que permita a los clientes para descubrir y para proteger los datos vulnerables en la empresa leveraging las directivas comunes a través de la infraestructura para descubrir y para proteger los datos vulnerables en el datacenter, en la red, y en los puntos finales. La habitación DLP incluye los componentes siguientes:

- **DLP Datacenter RSA**. El DLP Datacenter le ayuda a localizar los datos vulnerables no importa dónde reside en el datacenter, en los sistemas de archivos, las bases de datos, los sistemas del correo electrónico y los entornos grandes SAN/NAS.
- **Red DLP RSA**. Los Networks Monitores DLP y aplican la transmisión de la información vulnerable en la red, tal como correo electrónico y tráfico de la Web.
- **Punto final DLP RSA**. El punto final DLP le ayuda a descubrir, a monitorear y a controlar la información vulnerable en los puntos finales tales como laptopes y escritorios.

El Cisco WSA tiene la capacidad de interoperar con la red DLP RSA.

La red DLP RSA incluye los componentes siguientes:

- **Controlador de red**. El dispositivo principal que mantiene la información sobre los datos confidenciales y las políticas de transmisión contentas. El controlador de red maneja y pone al día los dispositivos administrados con la directiva y la definición contenta sensible junto con ningunos cambia a su configuración después de la configuración inicial.
- **Dispositivos administrados**. Estos dispositivos ayudan a la transmisión y al informe de la red del Network Monitor DLP o interceptan la transmisión:
  Sensores. Instalado en los límites de red, los sensores monitorean pasivo el tráfico que sale de la red o que cruza los límites de red, analizándola para la presencia de contenido sensible. Un sensor es una solución fuera de banda; puede monitorea y señala solamente las infracciones de la directiva.**Interceptores**. También instalado en los límites de red, los interceptores permiten que usted implemente quarantining y/o el rechazo del tráfico del email (S TP) que contiene el contenido sensible. Un interceptor es un proxy en línea de la red y por lo tanto puede bloquear los datos vulnerables de dejar la empresa.**Servidores ICAP**. Dispositivos del servidor del propósito especial que permiten que usted implemente la supervisión o el bloqueo del tráfico HTTP, HTTPS, o FTP que contiene el contenido sensible. Un servidor ICAP funciona con un servidor proxy (configurado como cliente ICAP) para monitorear o para bloquear los datos vulnerables de dejar la empresa

El Cisco WSA interopera con el servidor de la red procesos de captura de imagenes DLP RSA.

Limitaciones conocidas

La integración externa DLP de Cisco WSA con la red DLP RSA soporta las acciones siguientes: Permita y bloquee. Todavía no soporta “modifica/quita la acción del contenido” (también llamado Redaction).

Requerimientos de producto para la Interoperabilidad

La interoperabilidad de Cisco WSA y de la red DLP RSA fue probada y validada con los modelos del producto y las versiones de software en la tabla siguiente. Mientras que funcionalmente el discurso de esta integración puede trabajar con las variaciones al modelo y al software, la tabla siguiente representa las únicas combinaciones probadas, validadas, y soportadas. Se recomienda fuertemente para utilizar la última versión admitida de ambos Productos.

Producto	Versión del software
Dispositivo de seguridad de la red de Cisco (WSA)	Versiones 6.3 de AsyncOS y arriba
Red DLP RSA	7.0.2

Característica externa DLP

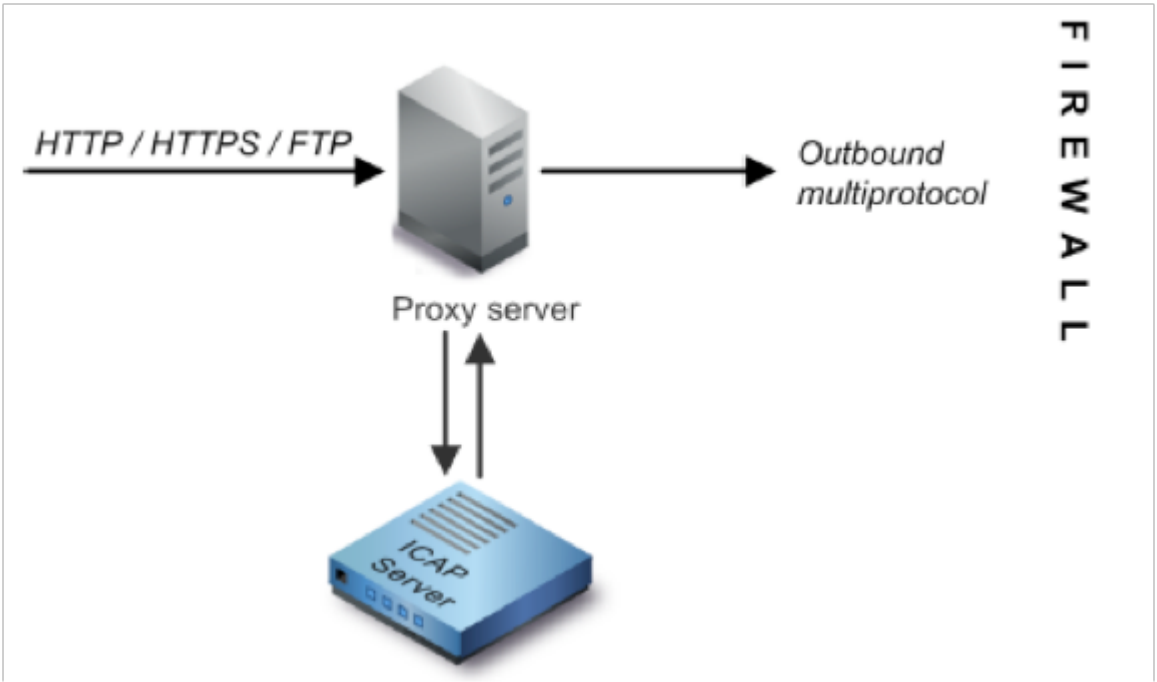
Usando la característica DLP del externo de Cisco WSA, usted puede remitir todos o el específico http saliente, tráfico HTTPS, y FTP del WSA a la red DLP. Todo el tráfico se transfiere usando el

protocolo de la adaptación de control de Internet (ICAP).

Arquitectura

La guía de la instrumentación de red DLP RSA muestra la arquitectura genérica siguiente para interoperar la red DLP RSA con un servidor proxy. Esta arquitectura no es específica al WSA, sino se aplica a cualquier proxy que interopera con la red DLP RSA.

Figura 1: Arquitectura de instrumentación para la red DLP RSA y el dispositivo de seguridad de la red de Cisco



Configurar el dispositivo de seguridad de la red de Cisco

1. Defina un sistema DLP del externo en el WSA que trabaja con el servidor ICAP de la red DLP. Para las instrucciones, vea por favor el extracto asociado del guía del usuario “instrucciones WSA del guía del usuario el definir de los sistemas externos DLP”.

2. Cree una o más directivas DLP del externo que definan que trafican el WSA envían a la red DLP para la exploración contenta usando los pasos abajo:

- Bajo **GUI > administrador de seguridad de la red > directiva externa de las directivas DLP >** Add
- Haga clic el link bajo la columna de los ***destinos*** para el grupo de políticas que usted quiere configurar
- ¿Bajo “edite sección de las configuraciones del destino”, eligen? ¿Defina los destinos que analizan las configuraciones personalizadas? del menú desplegable
- Podemos entonces configurar la directiva “para analizar todas las cargas o para analizar las cargas a ciertos dominios/a los sitios especificadas en las categorías de encargo URL

Configurar la red DLP RSA

Este documento asume que el controlador de red, el servidor ICAP y el administrador de empresa DLP RSA han estado instalados y configurados.

1. Utilice al administrador de empresa DLP RSA para configurar un servidor ICAP de la red. Para las Instrucciones detalladas en configurar su servidor ICAP de la red DLP, refiera a la guía de la instrumentación de red DLP RSA. Los parámetros principales que usted debe especificar en la página de configuración del servidor ICAP son: El nombre de host o la dirección IP del servidor ICAP.En la sección **general de las configuraciones de la** página de configuración, ingrese la siguiente información: La cantidad de tiempo en los segundos después de lo cual el servidor se juzga para haber medido el tiempo hacia fuera en el **tiempo de espera del servidor en el** campo de los **segundos**.Seleccione uno del siguiente como respuesta **sobre el tiempo de espera del servidor**:**Falle abierto**. Seleccione esta opción si usted quiere permitir la transmisión después de un tiempo de espera del servidor.**Fall cerrado**. Seleccione esta opción si usted quiere a la transmisión de bloque después de un tiempo de espera del servidor.
2. Utilice al administrador de empresa DLP RSA para crear una o más directivas Red-específicas para auditoría y para bloquear el tráfico de la red que contiene el contenido sensible. Para las Instrucciones detalladas para crear las directivas DLP, refiera a la guía de usuario de la red DLP RSA o a la ayuda de Manageronline de la empresa. Los pasos principales a realizarse son los siguientes: Del permiso de la biblioteca de la plantilla de política por lo menos una directiva que tiene sentido por su entorno y el contenido usted monitoreará.Dentro de esa directiva, las reglas Red-específicas puestas de la infracción de la directiva DLP que especifican las acciones el producto de la red se realizarán automáticamente cuando ocurren los eventos (infracciones de la directiva). Fije la regla de la detección de la directiva para detectar todos los protocolos. Fije la acción de política “para auditoría y para bloquear”.

Podemos utilizar *opcionalmente al* administrador de empresa RSA para personalizar la notificación de la red que se envía al usuario cuando ocurren las infracciones de la directiva. Esta notificación es enviada por la red DLP como reemplazo para el tráfico original.

Pruebe la configuración

1. Configure a su navegador para ordenar el tráfico saliente de su navegador para ir directamente al proxy WSA.

   Por ejemplo, si usted está utilizando al buscador FireFox del Mozilla, haga el siguiente: En el buscador FireFox, seleccione las **herramientas > las opciones**. El diálogo de opciones aparece.Haga clic la lengueta de la **red**, después haga clic las **configuraciones**. El diálogo de las configuraciones de la conexión aparece.Seleccione **Configuración manual del proxy el** checkbox, después ingrese el IP Address o el nombre de host del servidor proxy WSA en el campo y el número del puerto 3128 (el valor por defecto) del **proxy de HTTP**.El Haga Click en OK, entonces **APRUEBA** otra vez para salvar las nuevas configuraciones.

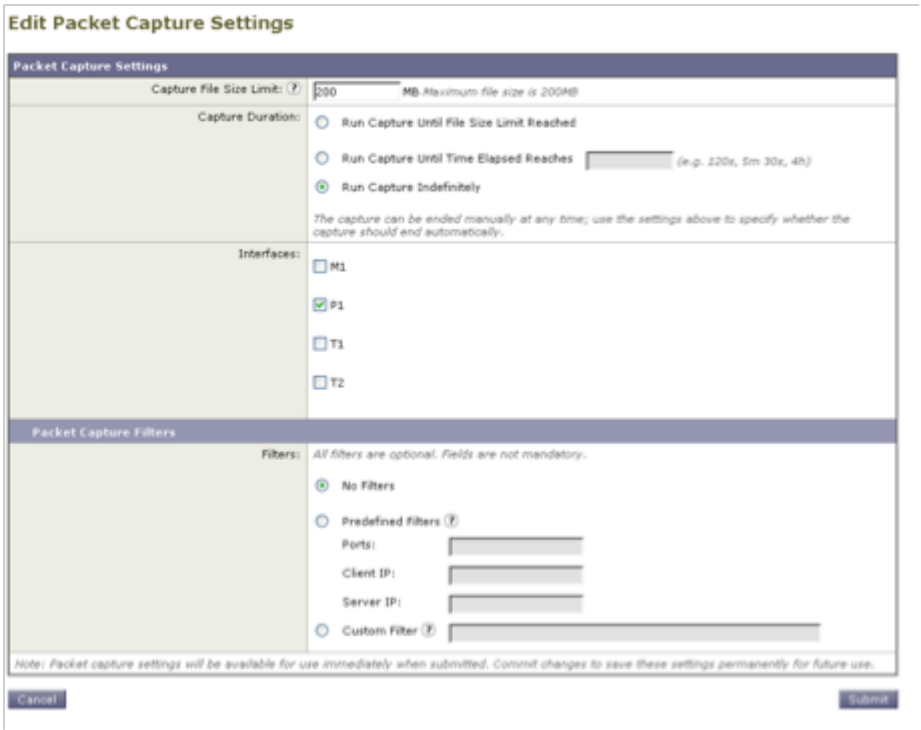
2. Intente cargar un cierto contenido que usted conozca esté con violación de la política de red DLP que usted habilitó previamente.
3. Usted debe ver un mensaje del descarte de la red ICAP en el navegador.
4. Utilice al “administrador de empresa” para ver el evento y el incidente resultantes que fueron creados como resultado de esta infracción de la directiva.

Resolución de problemas

1. Al configurar un servidor DLP del externo en el dispositivo de seguridad de la red para la red DLP RSA, utilice los valores siguientes:

   Dirección del servidor: La dirección IP o el nombre del host del servidor ICAP de la red DLP RSAPuerto: El puerto TCP usado para acceder al servidor de red DLP RSA, típicamente **1344**Mantenga el formato URL: **icap://** ***<hostname_or_ipaddress>/srv_conalarm***Ejemplo: icap://dlp.example.com/srv_conalarm
2. Habilite el tráfico que captura la característica de WSA para capturar el tráfico entre el proxy WSA y el servidor ICAP de la red. Esto es útil al diagnosticar los problemas de conectividad. Para hacer esto, haga el siguiente:

   En WSA GUI, vaya al **soporte y al menú de ayuda** en la esquina superior derecha de la interfaz de usuario. Seleccione a la **captura de paquetes del** menú, después haga clic el **botón Edit Settings Button**. La ventana de configuración de la captura del editar aparece.



   En la sección de los filtros de la **captura de paquetes de la** pantalla, ingrese el IP Address del servidor de la red procesos de captura de imagenes en **IP del servidor el** campo.El tecleo **somete** para salvar sus cambios.
3. Utilice el campo de encargo siguiente en los registros del acceso WSA (bajo ***GUI > administración del sistema > las suscripciones > los accesslogs del registro***) para conseguir más información:
   %Xp: Veredicto externo de la exploración del servidor DLP (0 = ninguna coincidencia en el

servidor ICAP; 1 = coincidencia de la directiva contra el servidor ICAP y “- (guión)” = no se inició ninguna exploración por el servidor DLP del externo)

Instrucciones del guía del usuario que definen los sistemas externos DLP.