¿Cómo configurar Cisco Web Security Appliance y la red RSA DLP para interoperar?

Contenido

Pregunta:

¿Cómo configurar Cisco Web Security Appliance y la red RSA DLP para interoperar?

Información general:

Este documento proporciona información adicional más allá de la Guía del usuario de Cisco WSA AsyncOS y la Guía de implementación de RSA DLP Network 7.0.2 para ayudar a los clientes a interoperar los dos productos.

Descripción del producto:

Cisco Web Security Appliance (WSA) es un dispositivo robusto, seguro y eficaz que protege las redes corporativas frente a programas de software espía y malware basados en Web que pueden poner en peligro la seguridad corporativa y exponer la propiedad intelectual. El dispositivo de seguridad web proporciona una inspección profunda del contenido de la aplicación al ofrecer un servicio de proxy web para protocolos de comunicación estándar como HTTP, HTTPS y FTP.

El paquete de prevención de pérdida de datos RSA incluye una completa solución de prevención de pérdida de datos que permite a los clientes descubrir y proteger los datos confidenciales de la empresa aprovechando las políticas comunes de toda la infraestructura para descubrir y proteger los datos confidenciales en el Data Center, en la red y en los terminales. La suite DLP incluye los siguientes componentes:

- Data Center RSA DLP. DLP Datacenter le ayuda a localizar los datos confidenciales independientemente de dónde se encuentren en el Data Center, en sistemas de archivos, bases de datos, sistemas de correo electrónico y entornos SAN/NAS grandes.
- Red DLP RSA. La red DLP supervisa y aplica la transmisión de información confidencial en la red, como el correo electrónico y el tráfico web.
- Extremo RSA DLP. El terminal DLP le ayuda a descubrir, supervisar y controlar información confidencial sobre terminales como portátiles y equipos de sobremesa.

Cisco WSA puede interoperar con la red RSA DLP.

RSA DLP Network incluye los siguientes componentes:

- Controlador de red. Dispositivo principal que mantiene información sobre datos confidenciales

y políticas de transmisión de contenido. El controlador de red gestiona y actualiza los dispositivos administrados con una definición de contenido sensible y de políticas junto con cualquier cambio en su configuración después de la configuración inicial.

- **Dispositivos administrados**. Estos dispositivos ayudan a la red DLP a monitorear la transmisión de la red e informar o interceptar la transmisión:
  Sensores. Instalados en los límites de la red, los sensores supervisan pasivamente el tráfico que sale de la red o que cruza los límites de la misma, analizándolo para detectar la presencia de contenido sensible. Un sensor es una solución fuera de banda; solo puede supervisar y notificar infracciones de políticas.**Interceptores**. También instalado en los límites de la red, los interceptores le permiten implementar la cuarentena y/o el rechazo del tráfico de correo electrónico (SMTP) que contiene contenido sensible. Un interceptor es un proxy de red en línea y, por lo tanto, puede bloquear la salida de datos confidenciales de la empresa.**Servidores ICAP**. Dispositivos de servidor de propósito especial que permiten implementar la supervisión o el bloqueo del tráfico HTTP, HTTPS o FTP que contiene contenido sensible. Un servidor ICAP funciona con un servidor proxy (configurado como cliente ICAP) para supervisar o bloquear la salida de datos confidenciales de la empresa

Cisco WSA interactúa con el servidor ICAP de red RSA DLP.

Limitaciones conocidas

La integración de DLP externa de Cisco WSA con la red DLP RSA admite las siguientes acciones: Permitir y bloquear. Todavía no admite la acción "Modificar/Eliminar contenido" (también denominada Redacción).

Requisitos del producto para interoperabilidad

La interoperabilidad de Cisco WSA y RSA DLP Network se ha probado y validado con los modelos de productos y las versiones de software de la siguiente tabla. Aunque funcionalmente esta integración puede funcionar con variaciones del modelo y el software, la siguiente tabla representa las únicas combinaciones probadas, validadas y admitidas. Se recomienda encarecidamente utilizar la última versión compatible de ambos productos.

Producto	Versión del software
Dispositivo de seguridad Cisco Web Security Appliance (WSA)	AsyncOS versiones 6.3 y superiores
Red RSA DLP	7.0.2

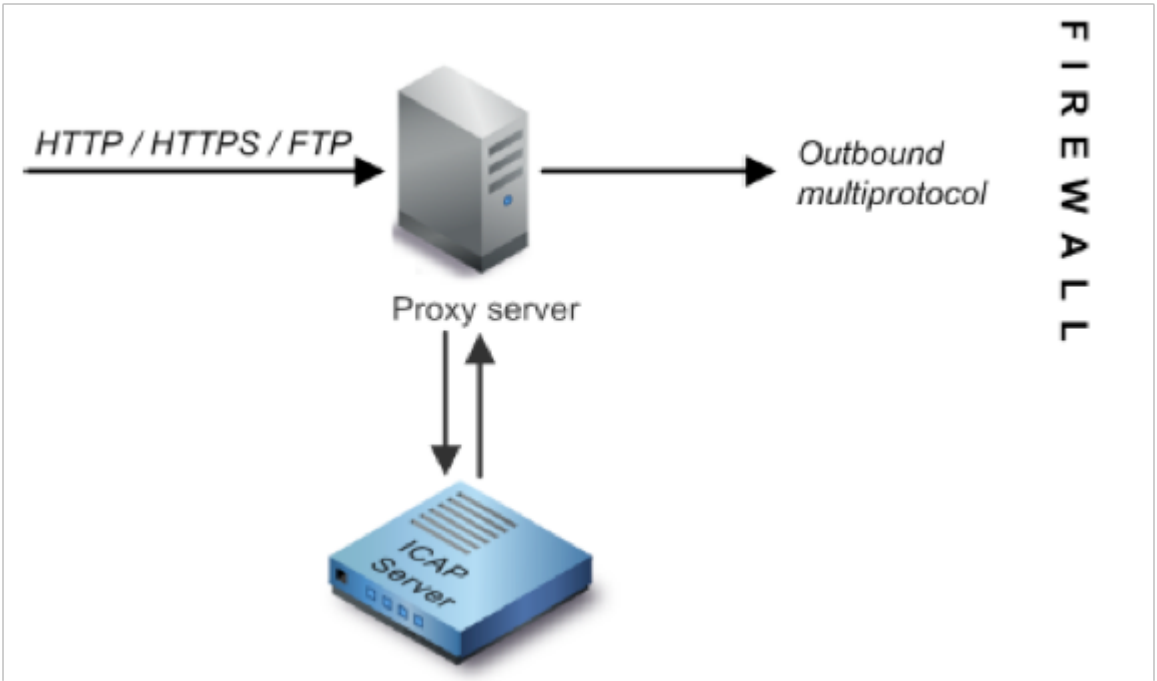
Función DLP externa

Con la función DLP externa de Cisco WSA, puede reenviar todo o parte del tráfico HTTP saliente, HTTPS y FTP desde WSA a la red DLP. Todo el tráfico se transfiere mediante el protocolo de adaptación del control de Internet (ICAP).

Arquitectura

La guía de implementación de red RSA DLP muestra la siguiente arquitectura genérica para la red RSA DLP interoperativa con un servidor proxy. Esta arquitectura no es específica de WSA, pero se aplica a cualquier proxy que interopere con la red DLP RSA.

Figura 1: Arquitectura de implementación para la red DLP RSA y el dispositivo de seguridad Cisco Web Security Appliance



Configuración de Cisco Web Security Appliance

1. Defina un sistema DLP externo en el WSA que funcione con el servidor ICAP de red DLP. Para obtener instrucciones, consulte el extracto adjunto de la guía del usuario de WSA "Instrucciones de guía del usuario para definir sistemas DLP externos".

2. Cree una o más políticas DLP externas que definan el tráfico que WSA envía a la red DLP para el análisis de contenido mediante los pasos siguientes:

- En **GUI > Web Security Manager > Políticas DLP externas > Agregar política**
- Haga clic en el enlace de la columna ***Destinos*** del grupo de políticas que desea configurar
- En la sección 'Editar configuración de destino', elija ?Definir destinos escaneando parámetros personalizados? en el menú desplegable
- A continuación, podemos configurar la política para 'Buscar todas las cargas' o para analizar las cargas en ciertos dominios/sitios especificados en categorías de URL personalizadas

Configuración de la Red DLP RSA

Este documento asume que se ha instalado y configurado RSA DLP Network Controller, ICAP Server y Enterprise Manager.

1. Utilice RSA DLP Enterprise Manager para configurar un servidor ICAP de red. Para obtener instrucciones detalladas sobre cómo configurar su servidor ICAP de red DLP, consulte la Guía de implementación de red RSA DLP. Los parámetros principales que debe especificar en la página de configuración del servidor ICAP son: Nombre de host o dirección IP del servidor ICAP.En la sección **Configuración general** de la página de configuración, introduzca la siguiente información: La cantidad de tiempo en segundos después de la cual se considera que el servidor ha agotado el tiempo de espera en el campo **Server Timeout in Segunds** .Seleccione una de las siguientes opciones como respuesta **al tiempo de espera del servidor**:**Fallo al abrir**. Seleccione esta opción si desea permitir la transmisión después de un tiempo de espera del servidor.**Fallo cerrado**. Seleccione esta opción si desea bloquear la transmisión después de un tiempo de espera del servidor.
2. Utilice RSA DLP Enterprise Manager para crear una o más políticas específicas de la red para auditar y bloquear el tráfico de red que contiene contenido sensible. Para obtener instrucciones detalladas sobre cómo crear políticas de DLP, consulte la Guía del usuario de red de RSA DLP o la ayuda en línea de Enterprise Manager. Los pasos principales a realizar son los siguientes: Desde la biblioteca de plantillas de políticas, habilite al menos una política que tenga sentido para su entorno y el contenido que supervisará.Dentro de esa política, configure reglas de violación de políticas específicas de red DLP que especifiquen las acciones que el producto de red realizará automáticamente cuando se produzcan eventos (infracciones de políticas). Establezca la regla de detección de políticas para detectar todos los protocolos. Establezca la acción de política en "auditoría y bloqueo".

Opcionalmente, podemos utilizar RSA Enterprise Manager para personalizar la notificación de red que se envía al usuario cuando se producen violaciones de políticas. Esta notificación es enviada por la red DLP como reemplazo del tráfico original.

Pruebe la configuración

1. Configure el explorador para que dirija el tráfico saliente desde el explorador directamente al proxy WSA.

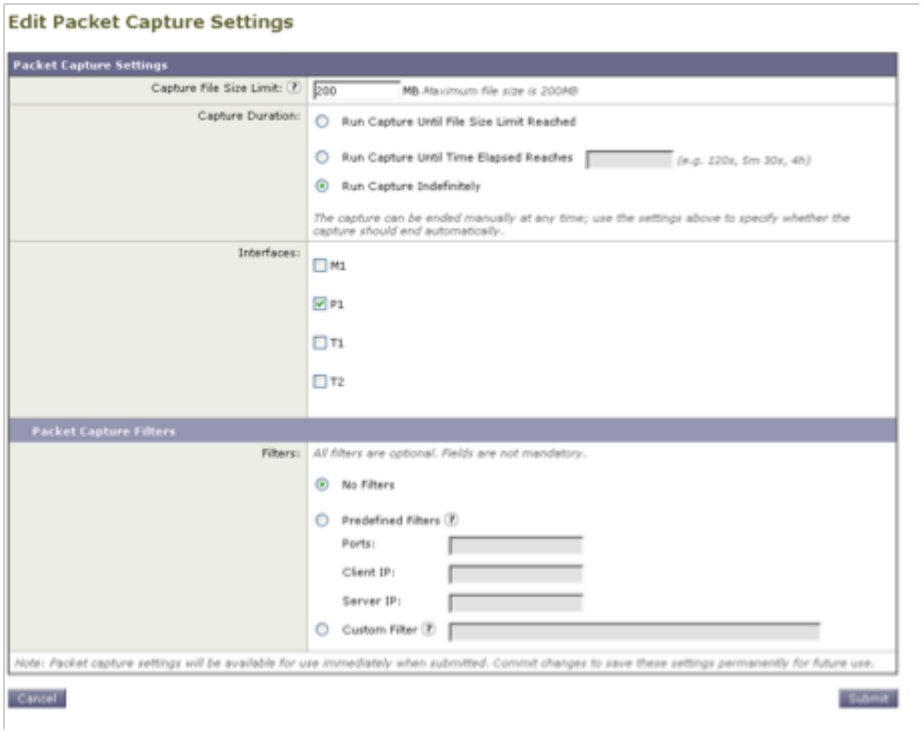
   Por ejemplo, si utiliza el explorador Mozilla FireFox, haga lo siguiente: En el explorador FireFox, seleccione **Herramientas > Opciones**. Aparecerá el cuadro de diálogo Opciones.Haga clic en la ficha **Red** y, a continuación, haga clic en **Configuración**. Aparecerá el cuadro de diálogo Configuración de la conexión.Seleccione la casilla de verificación **Manual Proxy Configuration** y, a continuación, introduzca la dirección IP o el nombre de host del servidor proxy WSA en el campo **HTTP Proxy** y el número de puerto 3128 (el valor predeterminado).Haga clic en **Aceptar** y, a continuación, **Aceptar** de nuevo para guardar los nuevos parámetros.
2. Intente cargar algún contenido que sepa que infringe la política de red DLP que ha activado anteriormente.
3. Debería ver un mensaje de descarte de ICAP de red en el navegador.
4. Utilice 'Enterprise Manager' para ver el evento y el incidente resultantes creados como resultado de esta violación de la política.

Resolución de problemas

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

   Dirección del servidor: Dirección IP o nombre de host del servidor ICAP de red RSA DLPPuerto: El puerto TCP utilizado para acceder al servidor de red RSA DLP, normalmente **1344**Formato de URL de servicio: **icap:// *<hostname_or_ipaddress>*/srv_conalarm**Ejemplo: icap://dlp.example.com/srv_conalarm
2. Habilite la función de captura de tráfico de WSA para capturar el tráfico entre el proxy WSA y el servidor ICAP de red. Esto es útil al diagnosticar problemas de conectividad. Para ello, haga lo siguiente:

   En la GUI de WSA, vaya al menú **Soporte y Ayuda** en la parte superior derecha de la interfaz de usuario. Seleccione **Captura de paquetes** en el menú y luego haga clic en el **botón Edit Settings**. Aparecerá la ventana Editar configuración de captura.



   En la sección Filtros de **captura de paquetes** de la pantalla, ingrese la dirección IP del servidor ICAP de red en el campo **IP del servidor**.Haga clic en **Enviar** para guardar los cambios.
3. Utilice el siguiente campo personalizado en los registros de acceso de WSA (bajo ***GUI > Administración del sistema >Suscripciones de registro > registros de acceso***) para obtener más información:
   %Xp: Veredicto de escaneo del servidor DLP externo (0 = no hay coincidencia en el servidor ICAP; 1 = coincidencia de políticas con el servidor ICAP y '- (guión)' = el servidor DLP externo no inició ningún escaneo)

[Instrucciones de la guía del usuario para definir sistemas DLP externos.]

_