Como configurar o Cisco Web Security Appliance e a rede RSA DLP para interoperar?

Contents

Pergunta:

Como configurar o Cisco Web Security Appliance e a rede RSA DLP para interoperar?

Overview:

Este documento fornece informações adicionais além do Cisco WSA AsyncOS User Guide e do RSA DLP Network 7.0.2 Deployment Guide para ajudar os clientes a interoperar os dois produtos.

Descrição do produto:

O Cisco Web Security Appliance (WSA) é um dispositivo robusto, seguro e eficiente que protege as redes corporativas contra programas de malware e spyware baseados na Web que podem comprometer a segurança corporativa e expor a propriedade intelectual. O Web Security Appliance fornece inspeção profunda de conteúdo de aplicativos oferecendo um serviço de proxy da Web para protocolos de comunicação padrão, como HTTP, HTTPS e FTP.

O RSA DLP Suite compreende uma solução abrangente de prevenção contra perda de dados que permite que os clientes descubram e protejam dados confidenciais na empresa, utilizando políticas comuns na infraestrutura para descobrir e proteger dados confidenciais no data center, na rede e em endpoints. O conjunto DLP inclui os seguintes componentes:

- **RSA DLP Datacenter**. O DLP Datacenter ajuda a localizar dados confidenciais, independentemente de onde eles estejam no datacenter, em sistemas de arquivos, bancos de dados, sistemas de e-mail e grandes ambientes SAN/NAS.
- **RSA DLP Network**. A Rede DLP monitora e impõe a transmissão de informações confidenciais na rede, como tráfego de e-mail e da Web.
- **Ponto de extremidade DLP RSA**. O DLP Endpoint ajuda a descobrir, monitorar e controlar informações confidenciais em endpoints, como laptops e desktops.

O Cisco WSA tem a capacidade de interoperar com a rede RSA DLP.

A rede DLP RSA inclui os seguintes componentes:

- **Controlador de rede**. O dispositivo principal que mantém informações sobre dados confidenciais e políticas de transmissão de conteúdo. O controlador de rede gerencia e atualiza dispositivos gerenciados com definição de política e conteúdo sensível, juntamente

com qualquer alteração na configuração após a configuração inicial.

- **Dispositivos gerenciados**. Esses dispositivos ajudam a Rede DLP a monitorar a transmissão da rede e a reportar ou interceptar a transmissão:
  Sensores. Instalados nos limites da rede, os sensores monitoram passivamente o tráfego que sai da rede ou atravessa os limites da rede, analisando-o quanto à presença de conteúdo sensível. Um sensor é uma solução fora de banda; ele só pode monitorar e relatar violações de política.**Interceptores**. Também instalado nos limites da rede, os Interceptores permitem que você implemente quarentena e/ou rejeição de tráfego de e-mail (SMTP) que contém conteúdo confidencial. Um Interceptor é um proxy de rede em linha e, portanto, pode bloquear a saída de dados confidenciais da empresa.**Servidores ICAP**. Dispositivos de servidor de finalidade especial que permitem implementar monitoramento ou bloqueio de tráfego HTTP, HTTPS ou FTP contendo conteúdo sensível. Um servidor ICAP trabalha com um servidor proxy (configurado como um cliente ICAP) para monitorar ou bloquear a saída de dados confidenciais da empresa

O Cisco WSA interopera com o servidor ICAP de rede RSA DLP.

Limitações conhecidas

A integração de DLP externo do Cisco WSA com a rede RSA DLP suporta as seguintes ações: Permitir e Bloquear. Ainda não suporta a ação "Modificar/Remover Conteúdo" (também chamada de Redação).

Requisitos de produto para interoperabilidade

A interoperabilidade da rede Cisco WSA e RSA DLP foi testada e validada com os modelos de produtos e as versões de software na tabela a seguir. Embora funcionalmente falando, essa integração pode funcionar com variações no modelo e no software, a tabela a seguir representa as únicas combinações testadas, validadas e suportadas. É altamente recomendável usar a versão mais recente suportada de ambos os produtos.

Produto	Versão de software
Cisco Web Security Appliance (WSA)	AsyncOS versões 6.3 e superiores
Rede DLP RSA	7.0.2

Recurso DLP externo

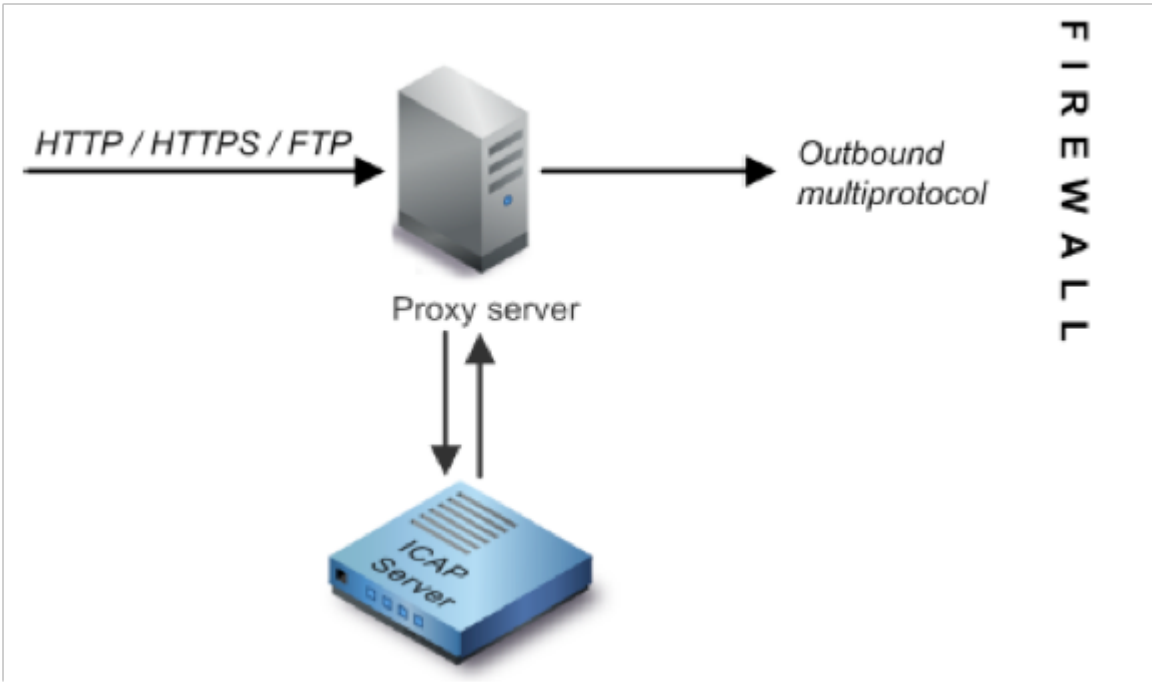
Usando o recurso DLP externo do Cisco WSA, você pode encaminhar todo o tráfego de saída HTTP, HTTPS e FTP específico da WSA para a rede DLP. Todo o tráfego é transferido usando o Internet Control Adaptation Protocol (ICAP).

Arquitetura

O Guia de implantação de rede RSA DLP mostra a seguinte arquitetura genérica para a rede RSA

DLP interoperacional com um servidor proxy. Essa arquitetura não é específica do WSA, mas se aplica a qualquer proxy que interopere com a rede DLP RSA.

Figura 1: Arquitetura de implantação para rede RSA DLP e o Cisco Web Security Appliance



Configurando o Cisco Web Security Appliance

1. Defina um sistema DLP externo no WSA que funcione com o servidor ICAP de rede DLP. Para obter instruções, consulte o trecho anexo do Guia do usuário do WSA "User Guide Instructions Definindo sistemas DLP externos".

2. Crie uma ou mais políticas de DLP externo que definam qual tráfego o WSA envia para a rede DLP para verificação de conteúdo usando as etapas abaixo:

- Em **GUI > Web Security Manager > Políticas externas DLP > Adicionar política**
- Clique no link na coluna ***Destinos*** do grupo de política que deseja configurar
- Na seção "Edit Destination Settings" (Editar configurações de destino), escolha ?Define Destinations Scanning Custom Settings? (Definir destinos verificando configurações personalizadas). no menu suspenso
- Podemos, então, configurar a política para 'Analisar todos os carregamentos' ou para pesquisar carregamentos em determinados domínios/sites especificados em categorias de URL personalizadas

Configurando a rede DLP RSA

Este documento pressupõe que o Controlador de Rede RSA DLP, o Servidor ICAP e o Enterprise Manager foram instalados e configurados.

1. Use o RSA DLP Enterprise Manager para configurar um servidor ICAP de rede. Para obter instruções detalhadas sobre como configurar seu servidor ICAP de rede DLP, consulte o Guia de implantação de rede RSA DLP. Os principais parâmetros que você deve especificar na página de configuração do Servidor ICAP são: O nome do host ou o endereço IP do servidor ICAP.Na seção **Configurações gerais** da página de configuração, insira as seguintes informações: A quantidade de tempo em segundos após o qual se considera que o servidor expirou no campo **Tempo limite do servidor em segundos**.Selecione uma das seguintes opções como resposta **Após o tempo limite do servidor**:**Falha Ao Abrir**. Selecione esta opção se quiser permitir a transmissão após o tempo limite do servidor.**Falha Ao Fechar**. Selecione esta opção se quiser bloquear a transmissão após o tempo limite de um servidor.
2. Use o RSA DLP Enterprise Manager para criar uma ou mais políticas específicas de rede para auditar e bloquear o tráfego de rede que contém conteúdo sensível. Para obter instruções detalhadas sobre como criar políticas DLP, consulte o Guia do usuário da rede RSA DLP ou a ajuda on-line do Enterprise Manager. As etapas principais a serem executadas são as seguintes: Na biblioteca de modelos de política, ative pelo menos uma política que faça sentido para o seu ambiente e o conteúdo que você monitorará.Nessa política, configure regras de violação de política específicas da rede DLP que especifiquem ações que o produto da rede executará automaticamente quando ocorrerem eventos (violações de política). Defina a regra de detecção de política para detectar todos os protocolos. Defina a ação da política como "auditar e bloquear".

Opcionalmente, podemos usar o RSA Enterprise Manager para personalizar a notificação de rede que é enviada ao usuário quando ocorrem violações de política. Essa notificação é enviada pela Rede DLP como uma substituição para o tráfego original.

Teste a configuração

1. Configure seu navegador para direcionar o tráfego de saída do navegador para ir diretamente para o proxy WSA.

   Por exemplo, se você estiver usando o navegador Mozilla FireFox, faça o seguinte: No navegador FireFox, selecione **Ferramentas > Opções**. A caixa de diálogo Opções é exibida.Clique na guia **Rede** e clique em **Configurações**. A caixa de diálogo Configurações da conexão é exibida.Marque a caixa de seleção **Manual Proxy Configuration** e insira o endereço IP ou o nome de host do servidor proxy WSA no campo **HTTP Proxy** e o número de porta 3128 (o padrão).Clique em **OK** e em **OK** novamente para salvar as novas configurações.
2. A tentativa de carregar algum conteúdo que você sabe que está violando a política de rede DLP que você ativou anteriormente.
3. Você deve ver uma mensagem de descarte ICAP de rede no navegador.
4. Use o 'Enterprise Manager' para exibir o evento e incidente resultante que foram criados como resultado dessa violação de política.

Troubleshooting

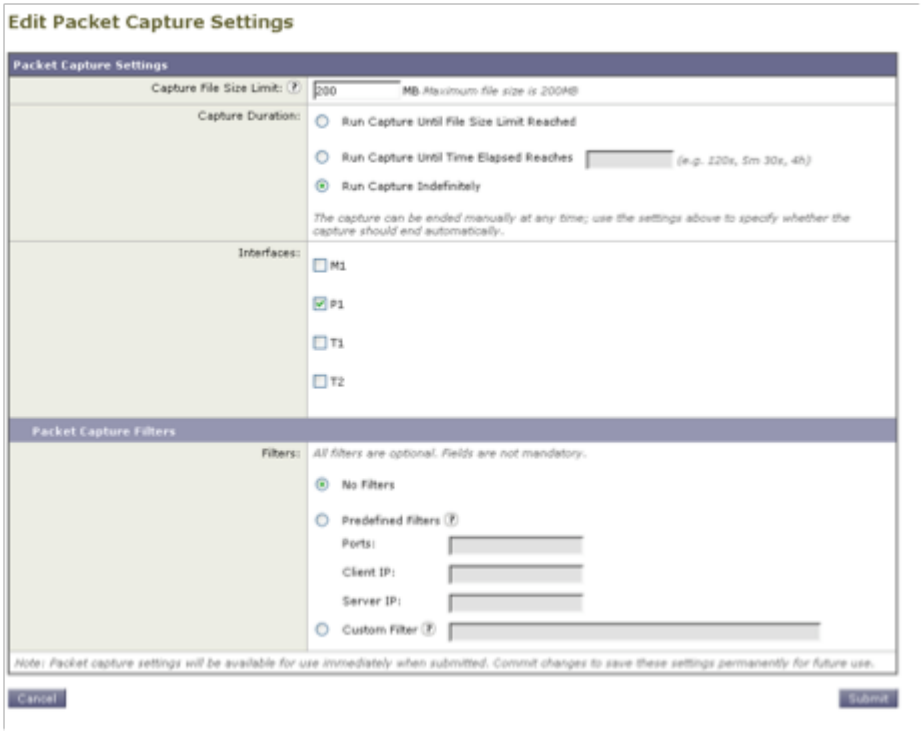
1. Ao configurar um servidor DLP externo no Web Security Appliance para rede DLP RSA, use

os seguintes valores:

Endereço do servidor: O endereço IP ou o nome do host do servidor ICAP de rede RSA DLPPorta: A porta TCP usada para acessar o servidor de rede RSA DLP, geralmente **1344**Formato de URL do serviço: **icap:// *<hostname_or_ipaddress>*/srv_conalarm**Exemplo: icap://dlp.example.com/srv_conalarm

2. Ative o recurso de captura de tráfego do WSA para capturar o tráfego entre o proxy WSA e o servidor ICAP de rede. Isso é útil ao diagnosticar problemas de conectividade. Para fazer isso, faça o seguinte:

   Na GUI do WSA, vá para o menu **Suporte e Ajuda** na parte superior direita da interface do usuário. Selecione **Captura de pacote** no menu e clique no botão **Editar configurações**. A janela Editar configurações de captura é exibida.



   Na seção Filtros de **Captura de Pacotes** da tela, insira o endereço IP do servidor ICAP de Rede no campo **IP do Servidor**.Clique em **Enviar** para salvar suas alterações.

3. Use o seguinte campo personalizado nos registros de acesso do WSA (em ***GUI > Administração do sistema > Inscrições de log > registros de acesso***) para obter mais informações:
   %Xp: Veredito de verificação do servidor DLP externo (0 = nenhuma correspondência no servidor ICAP; 1 = correspondência de política com o servidor ICAP e '- (hífen)' = Nenhuma verificação foi iniciada pelo servidor DLP externo)

[Instruções do Guia do Usuário Definindo Sistemas DLP Externos.]

_