Como configurar a rede da ferramenta de segurança da Web de Cisco e DLP RSA para interoperar?

Índice

Pergunta:

Como configurar a rede da ferramenta de segurança da Web de Cisco e DLP RSA para interoperar?

Vista geral:

Este documento fornece a informação extra além do Guia do Usuário de Cisco WSA AsyncOS e o guia de distribuição da rede 7.0.2 DLP RSA para ajudar clientes interopera os dois Produtos.

Descrição do produto:

A ferramenta de segurança da Web de Cisco (WSA) é um dispositivo robusto, seguro, eficiente que proteja redes corporativas contra os programas com base na Web do malware e do spyware que podem comprometer a segurança corporativa e expor a propriedade intelectual. A ferramenta de segurança da Web fornece a inspeção profunda do índice do aplicativo oferecendo um serviço do proxy da Web para protocolos de comunicação padrão tais como o HTTP, o HTTPS, e o FTP.

A série DLP RSA compreende uma solução detalhada da prevenção de perda de dados que permita clientes de descobrir e proteger dados sensíveis na empresa leveraging políticas comuns através da infraestrutura para descobrir e proteger dados sensíveis no datacenter, na rede, e em valores-limite. A série DLP inclui os seguintes componentes:

- **DLP Datacenter RSA**. O DLP Datacenter ajuda-o a encontrar dados sensíveis não importa onde reside no datacenter, em sistemas de arquivos, em bases de dados, em sistemas do email e em grandes ambientes SAN/NAS.
- **Rede DLP RSA**. Os monitores de rede DLP e reforçam a transmissão da informação sensível na rede, tal como o email e o tráfego de web.
- **Valor-limite DLP RSA**. O valor-limite DLP ajuda-o a descobrir, monitorar e controlar a informação sensível em valores-limite tais como portáteis e desktops.

Cisco WSA tem a capacidade para interoperar com rede DLP RSA.

A rede DLP RSA inclui os seguintes componentes:

- **Controlador de rede**. O dispositivo principal que mantém a informação sobre políticas de transmissão confidenciais dos dados e do índice. O controlador de rede controla e atualiza dispositivos gerenciado com política e a definição satisfeita sensível junto com alguns muda a sua configuração após a configuração inicial.
- **Dispositivos gerenciado**. Estes dispositivos ajudam a transmissão e o relatório da rede do monitor de rede DLP ou interceptam a transmissão:
  Sensores. Instalado em limites de rede, os sensores monitoram passivamente o tráfego que sae da rede ou que cruza os limites de rede, analisando a para a presença de índice sensível. Um sensor é uma solução fora da banda; pode somente monitora e relata violações da política.**Interceptores**. Igualmente instalado em limites de rede, os interceptores permitem que você execute quarantining e/ou rejeção do tráfego do email (S TP) que contém o índice sensível. Um interceptor é uma em-linha proxy da rede e pode consequentemente obstruir dados sensíveis de deixar a empresa.**Server ICAP**. Dispositivos do server do propósito especial que permitem que você execute a monitoração ou a obstrução do tráfego HTTP, HTTPS, ou FTP que contém o índice sensível. Um server ICAP funciona com um servidor proxy (configurado como um cliente ICAP) para monitorar ou obstruir dados sensíveis de deixar a empresa

Cisco WSA interopera com o server ICAP da rede DLP RSA.

Limitações conhecidas

A integração externo DLP de Cisco WSA com rede DLP RSA apoia as seguintes ações: Reserve e obstrua. Não apoia ainda “altera/remove a ação do índice” (igualmente chamado Redação).

Requerimentos do produto para a Interoperabilidade

A interoperabilidade de Cisco WSA e da rede DLP RSA foi testada e validada com os modelos do produto e as versões de software na tabela a seguir. Quando funcionalmente falar esta integração puder trabalhar com variações ao modelo e ao software, a tabela a seguir representa as únicas combinações testadas, validadas, e apoiadas. Recomenda-se fortemente usar a versão suportada a mais atrasada de ambo o Produtos.

Produto	Versão de software
Ferramenta de segurança da Web de Cisco (WSA)	Versões 6.3 de AsyncOS & acima
Rede DLP RSA	7.0.2

Característica externo DLP

Usando a característica externo DLP de Cisco WSA, você pode enviar tudo ou o HTTP de saída específico, o tráfego HTTPS, e FTP do WSA à rede DLP. Todo o tráfego é transferido usando o protocolo da adaptação de controle de Internet (ICAP).

Arquitetura

O guia da distribuição de rede DLP RSA mostra a seguinte arquitetura genérica para interoperar a rede DLP RSA com um servidor proxy. Esta arquitetura não é específica ao WSA, mas aplica a todo o proxy esse a interopera com rede DLP RSA.

Figura 1: Arquitetura de distribuição para a rede DLP RSA e a ferramenta de segurança da Web de Cisco

Configurando a ferramenta de segurança da Web de Cisco

1. Defina um sistema externo DLP no WSA que trabalha com o server ICAP da rede DLP. Para instruções, veja por favor o trecho anexado do Guia do Usuário do “instruções WSA Guia do Usuário definir sistemas externos DLP”.

2. Crie umas ou várias políticas externos DLP que definem que traficam o WSA enviam à rede DLP para a exploração satisfeita usando as etapas abaixo:

- Sob **GUI > gerenciador de segurança da Web > política externa do >** Add das **políticas DLP**
- Clique o link sob a coluna dos ***destinos*** para o grupo de política que você quer configurar
- Sob “edite a seção dos ajustes do destino”, escolhem? Defina os destinos que fazem a varredura de configurações personalizadas? de gota do menu para baixo
- Nós podemos então configurar a política “para fazer a varredura de todas as transferências de arquivo pela rede” ou para fazer a varredura das transferências de arquivo pela rede para determinados domínios/locais especificadas em categorias feitas sob encomenda URL

Configurando a rede DLP RSA

Este documento supõe que o controlador de rede DLP RSA, o server ICAP e a enterprise manager estiveram instalados e configurados.

1. Use a enterprise manager DLP RSA para configurar um server ICAP da rede. Para instruções detalhadas em estabelecer seu server ICAP da rede DLP, refira o guia da distribuição de rede DLP RSA. Os parâmetros principais que você deve especificar na página da configuração do servidor ICAP são: O hostname ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do server ICAP.Na seção **geral dos ajustes da** página de configuração, incorpore a informação seguinte: A quantidade de tempo nos segundos depois do qual no server é julgada para ter cronometrado para fora no **timeout de servidor no** campo dos **segundos**.Selecione um do seguinte como uma resposta **em cima do timeout de servidor**:**Falhe aberto**. Selecione esta opção se você quer permitir a transmissão após um timeout de servidor.**Falha fechada**. Selecione esta opção se você quer à transmissão de bloco após um timeout de servidor.
2. Use a enterprise manager DLP RSA para criar umas ou várias políticas Rede-específicas para examinar e obstruir o tráfego de rede que contém o índice sensível. Para instruções

detalhadas para criar políticas DLP, refira o guia de usuário de rede DLP RSA ou a ajuda de Manageronline da empresa. As etapas principais a executar são as seguintes: Da biblioteca do molde de política permita pelo menos uma política que faz o sentido para seu ambiente e o índice que você estará monitorando.Dentro dessa política, as regras Rede-específicas setup da violação da política DLP que especificam ações o produto da rede executarão automaticamente quando os eventos (violações da política) ocorrem. Ajuste a regra da detecção da política para detectar todos os protocolos. Ajuste a ação de política “examinar e obstruir”.

Opcionalmente nós podemos usar a enterprise manager RSA para personalizar a notificação da rede que está enviada ao usuário quando as violações da política ocorrem. Esta notificação é enviada pela rede DLP como uma substituição para o tráfego original.

Teste a instalação

1. Configurar seu navegador para dirigir o tráfego de saída de seu navegador para ir diretamente ao proxy WSA.

   Por exemplo, se você está usando o navegador FireFox de Mozilla, faça o seguinte: No navegador FireFox, selecione **ferramentas > opções**. O diálogo de opções aparece.Clique a aba da **rede**, a seguir clique **ajustes**. O diálogo das configurações de conexão aparece.Selecione a caixa de seleção da **configuração manual de proxy**, a seguir inscreva o endereço IP ou nome do host do servidor proxy WSA no campo do **proxy HTTP** e no número de porta 3128 (o padrão).Clique a **APROVAÇÃO**, a seguir **APROVADO** outra vez salvar os ajustes novos.
2. Tente transferir arquivos pela rede algum índice que você conhece é em violação da política de rede que DLP você permitiu previamente.
3. Você deve ver uma mensagem do descarte ICAP da rede no navegador.
4. Use a “enterprise manager” para ver o evento e o incidente resultantes que foram criados em consequência desta violação da política.

Troubleshooting

1. Ao configurar um server externo DLP na ferramenta de segurança da Web para a rede DLP RSA, use os seguintes valores:

   Endereço do servidor: O endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome de host do server ICAP da rede DLP RSAPorta: A porta TCP usada para alcançar o servidor de rede DLP RSA, tipicamente **1344**Preste serviços de manutenção ao formato URL: **icap://** ***<hostname_or_ipaddress>/srv_conalarm***Exemplo: icap://dlp.example.com/srv_conalarm
2. Permita o tráfego que captura a característica de WSA para capturar o tráfego entre o proxy WSA e o server ICAP da rede. Isto é útil ao diagnosticar problemas de conectividade. Para fazer isto, faça o seguinte:

   Em WSA GUI, vá ao **apoio e ao menu de ajuda no** direita superior da interface do utilizador. Selecione a **captura de pacote de informação do** menu, a seguir clique o **botão Edit Settings Button**. A janela de configuração da captação da edição aparece.

Na seção dos filtros da **captura de pacote de informação da** tela, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do server ICAP da rede ao campo do **IP de servidor**.O clique **submete-se** para salvar suas mudanças.

3. Use o seguinte campo feito sob encomenda nos logs do acesso WSA (sob ***GUI > administração do sistema > assinaturas > accesslogs do log***) para obter mais informação: %Xp: Sentença externo da exploração do server DLP (0 = nenhum fósforo no server ICAP; 1 = fósforo da política contra o server ICAP e “- (hífen)” = nenhuma exploração foi iniciada pelo server externo DLP)

Instruções do Guia do Usuário que definem sistemas externos DLP.