ASDM 6.3 e mais atrasado: Exemplo de configuração da inspeção das opções IP

Índice

Introdução

Este documento fornece uma configuração de exemplo de como configurar a ferramenta de segurança adaptável de Cisco (ASA) a fim passar os pacotes IP com determinadas opções IP permitidas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Release Version running 8.3 de Cisco ASA e mais atrasado
- Software Release Version running 6.3 do gerenciador de segurança adaptável de Cisco e mais atrasado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Cada pacote IP contém um cabeçalho IP com um campo de opções. O campo de opções, referido geralmente como opções IP, fornece as funções de controle que são exigidas em algumas situações, mas desnecessário para a maioria de comunicações comuns. Em particular, as opções IP incluem disposições para selos de tempo, Segurança, e o roteamento especial. O uso das opções IP é opcional, e o campo pode conter zero, umas, ou mais opções.

As opções IP são um risco de segurança e se um pacote IP com o campo de opções IP permitido é passado com o ASA, escapará a informação sobre a instalação interna de uma rede à parte externa. Em consequência, um atacante pode traçar a topologia de sua rede. Enquanto Cisco ASA é um dispositivo que reforce a Segurança na empresa, à revelia, ele deixa cair os pacotes que têm o campo de opções IP permitido. Um mensagem do syslog da amostra é mostrado aqui, para sua referência:

```
IP 106012|10.110.1.34||XX.YY.ZZ.ZZ||Deny de 10.110.1.34 a XX.YY.ZZ.ZZ, opções IP: “Alerta de roteador”
```

Contudo, nos cenários de distribuição específicos onde o tráfego de vídeo tem que passar através de Cisco ASA, os pacotes IP com determinadas opções IP têm que ser passados com de outra maneira o atendimento de videoconferência podem falhar. Do Software Release Version 8.2.2 de Cisco ASA avante, uns novos recursos chamados “inspeção para opções IP” foram introduzidos. Com esta característica, você pode controlar que pacotes com opções IP específicas são permitidos através de Cisco ASA.

Àrevelia, esta característica é permitida e a inspeção para as opções IP abaixo é permitida na política global. Configurar esta inspeção instrui o ASA para permitir um pacote passe, ou cancele as opções IP especificadas e permita então que o pacote passe.

- **Fim da lista de opções (EOOL)** ou da **opção IP 0** - esta opção aparece no fim de todas as opções a fim marcar a extremidade de uma lista de opções.
- **Nenhuma operação (NOP)** ou **opção IP 1** - este campo de opções faz o comprimento total da variável do campo.
- **Alerta de roteador (RTRALT)** ou **opção IP 20** - esta opção notifica roteadores de trânsito para inspecionar os índices do pacote mesmo quando o pacote não é destinado para esse roteador.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Configuração ASDM

Usando o ASDM, você pode ver como permitir a inspeção para os pacotes IP que têm o campo de opções IP, NOP.

O campo de opções no cabeçalho IP pode conter zero, umas, ou mais opções, que faz o comprimento total da variável do campo. Contudo, o cabeçalho IP deve ser um múltiplo de 32 bit. Se o número de bit de todas as opções não é um múltiplo de 32 bit, a opção NOP está usada como “o estofamento interno” a fim alinhar as opções em um limite de 32 bits.

1. Vá à **configuração** > ao **Firewall** > aos **objetos** > **inspecionam mapas** > **opções IP**, e o clique **adiciona**.
2. As opções IP adicionar inspecionam o indicador do mapa aparecem. Especifique o nome do mapa da inspeção, seleto **permita pacotes com nenhuma opção da operação (NOP)**, e clique a **APROVAÇÃO**.**Nota:** Você pode igualmente selecionar o **claro o valor de opção da** opção dos **pacotes**, de modo que este campo no pacote IP seja desabilitado, e os pacotes passam através de Cisco ASA.
3. Um novo inspeciona o **testmap** chamado mapa é criado. Clique em Apply.
4. Vá às **regras da configuração** > do **Firewall** > da **política de serviços**, selecione a política global existente, e o clique **edita**. O indicador da regra da política de serviços da edição aparece. Selecione as **ações** aba da **regra**, marca de verificação o artigo das **opções IP**, e escolha-as **configuram** a fim atribuir o mapa recém-criado da inspeção.
5. Escolha **seleto opções IP inspecionam o mapa para o controle fino sobre a inspeção** > o **testmap**, e clicam a **APROVAÇÃO**.
6. Selecionados inspecionam o mapa podem ser vistos no campo de **opções IP**. Clique a **APROVAÇÃO** a fim reverter de volta à aba das regras da política de serviços.
7. Com seu rato, paire sobre a aba das **ações da regra** de modo que você possa encontrar todos os mapas disponíveis da inspeção do protocolo associados com este mapa global.

Está aqui um snippet da amostra da configuração de CLI equivalente, para sua referência:

Cisco ASA

```
ciscoasa(config)#policy-map type inspect ip-options
testmap

ciscoasa(config-pmap)#parameters

ciscoasa(config-pmap-p)#nop action allow

ciscoasa(config-pmap-p)#exit

ciscoasa(config)#policy-map global_policy

ciscoasa(config-pmap)#class inspection_default

ciscoasa(config-pmap-c)#inspect ip-options testmap

ciscoasa(config-pmap-p)#exit

ciscoasa(config)#write memory
```

Comportamento padrão de Cisco ASA a fim permitir pacotes RSVP

A inspeção das opções IP é permitida à revelia. Vá às **regras da configuração** > do **Firewall** > da

política de serviços. Selecione a política global, o clique **edita**, e seleciona a aba das **inspeçãos do padrão**. Aqui, você encontrará o protocolo RSVP no campo de **opções IP**. Isto assegura-se de que o protocolo RSVP esteja inspecionado e permitido através de Cisco ASA. Em consequência, um atendimento video fim-a-fim é estabelecido sem nenhum problema.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **a serviço-política da mostra inspeciona IP-opções** - Indica o número de pacotes deixados cair e/ou permitidos conforme a regra configurada da serviço-política.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte técnico do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Suporte Técnico e Documentação - Cisco Systems