Configurar a inspeção de opções IP no ASDM 6.3 e posterior

Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Informações de Apoio Configurar Configuração do ASDM Comportamento padrão do Cisco ASA para permitir pacotes RSVP Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento fornece uma configuração de exemplo de como configurar o Cisco Adaptive Security Appliance (ASA) para passar os pacotes IP com determinadas opções de IP ativadas.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco ASA executando o software versão 8.3 e posterior
- Cisco Adaptive Security Manager executando o software versão 6.3 e posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

Cada pacote IP contém um cabeçalho IP com um campo Opções. O campo Opções, geralmente conhecido como Opções IP, fornece funções de controle necessárias em algumas situações, mas desnecessárias para a maioria das comunicações comuns. Em particular, as Opções IP incluem provisões para carimbos de data/hora, segurança e roteamento especial. O uso de opções IP é opcional e o campo pode conter zero, uma ou mais opções.

As Opções IP são um risco à segurança e se um pacote IP com o campo Opções IP ativado for passado pelo ASA, ele vazará informações sobre a configuração interna de uma rede para o exterior. Como resultado, um invasor pode mapear a topologia da sua rede. Como o Cisco ASA é um dispositivo que reforça a segurança na empresa, por padrão, ele descarta os pacotes que têm o campo Opções IP ativado. Um exemplo de mensagem de syslog é mostrado aqui, para sua referência:

106012|10.110.1.34||XX.YY.ZZ.ZZ||Negar IP de 10.110.1.34 para XX.YY.ZZ.ZZ, opções IP: "Alerta do roteador"

No entanto, em cenários de implantação específicos em que o tráfego de vídeo tem que passar pelo Cisco ASA, os pacotes IP com determinadas opções de IP têm que ser passados, caso contrário, a chamada de videoconferência pode falhar. A partir da versão 8.2.2 do software Cisco ASA, um novo recurso chamado "Inspection for IP options" foi introduzido. Com esse recurso, você pode controlar quais pacotes com opções IP específicas são permitidos pelo Cisco ASA.

Por padrão, esse recurso está ativado e a inspeção das Opções IP abaixo está habilitada na política global. A configuração dessa inspeção instrui o ASA a permitir que um pacote passe ou a limpar as opções IP especificadas e permitir a passagem do pacote.

- End of Options List (EOOL) ou IP Option 0 Essa opção aparece no final de todas as opções para marcar o fim de uma lista de opções.
- Nenhuma operação (NOP) ou opção de IP 1 Este campo de opções faz com que o comprimento total da variável de campo seja total.
- Router Alert (RTRALT) ou IP Option 20 Essa opção notifica os roteadores de trânsito para inspecionar o conteúdo do pacote mesmo quando o pacote não está destinado a 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 do ASDM

Usando o ASDM, você pode ver como habilitar a inspeção para os pacotes IP que têm o campo

Opções IP, NOP.

O campo Opções no cabeçalho IP pode conter zero, uma ou mais opções, o que torna o comprimento total da variável de campo. No entanto, o cabeçalho IP deve ser um múltiplo de 32 bits. Se o número de bits de todas as opções não for um múltiplo de 32 bits, a opção NOP será usada como "preenchimento interno" para alinhar as opções em um limite de 32 bits.

1. Vá para Configuration > Firewall > Objects > Inspect Maps > IP-Options e clique em Add.

IP-Options	
Description	Add
	Edit
	Delete
	IP-Options Description

2. A janela Add IP-Options Inspect Map é exibida. Especifique o nome do Mapa de Inspeção, selecione **Permitir pacotes com a opção Sem Operação (NOP)** e clique em

a Aud P-Options inspect map	
Name: (testmap)	
Description:	
Parameters	
Allow packets with the End of Options List (EOOL) option	
Clear the option value from the packets	
Allow packets with the No Operation (NOP) option	
Clear the option value from the packets	
Allow packets with the Router Alert (RTRALT) option	
Clear the option value from the packets	

também pode selecionar a **opção Limpar o valor da opção na** opção **de pacotes**, para que esse campo no pacote IP seja desativado e os pacotes passem pelo Cisco ASA.

3. Um novo mapa de inspeção chamado **testmap** é criado. Clique em Apply.

onfiguration > Firewall > Objects > Inspe	act Maps > IP-Options
Configure IP-Options maps.	
P-Options Inspect Maps	
Name	Description

4. Vá para Configuration > Firewall > Service Policy Rules, selecione a política global existente e clique em Edit. A janela Editar regra de política de serviço é exibida. Selecione a guia Ações da regra, marque o item Opções de IP e escolha Configurar para atribuir o mapa de inspeção recém-

💰 Edit S	ervice Policy Rule)	
Traffic C	lassification Default	Inspections Rule Act	ions
Protor		ution Sattings Oas	Mattleur
	Conne	ection settings Qos	Nethow
² []	Select all inspection rul	es	
E	CTIQBE		
] DCERPC	Configure	
] DNS	Configure	DNS Inspect Map: migrated_dns_i
	ESMTP	Configure	
] FTP	Configure	
] GTP	Configure	
] H.323 H.225	Configure	
] H.323 RAS	Configure	
] HTTP	Configure	
] ICMP		
] ICMP Error		
]ıls		
] IM	Configure	
] IP-Options	Configure	
] IPSec-Pass-Thru	Configure	
	Тммр	Configure	

5. Escolha Select an IP-Options inspect map for fine control over inspection > testmap e clique

0	Use the default IP-Op Select an IP-Options i	tions inspection r	nap ne control over	inspecti
	Name testmap			Add

 O mapa de inspeção selecionado pode ser visualizado no campo IP-Options. Clique em OK para voltar à guia Service Policy Rules (Regras da política de serviço).

Edit Service Policy Rule		
raffic Classification Default I	nspections Rule Ac	tions
Protocol Inspection Coppe	tion Settings 005	NetElow
Conne	con seconds 205	
Select all inspection rule	is	
CTIQBE		
DCERPC	Configure	
DNS DNS	Configure	DNS Inspect Map: migrated_dns_
ESMTP	Configure	
FTP	Configure	
GTP	Configure	
M.323 H.225	Configure	
H.323 RAS	Configure	
HTTP	Configure	
ICMP		
ICMP Error		
IL 5		
IM 🗌	Configure	
IP-Options	Configure	IP-Options Inspect Map: testmap
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	

 Com o mouse, passe o mouse sobre a guia Ações da regra para encontrar todos os mapas de inspeção de protocolo disponíveis associados a esse mapa global.

🗣 Add 🔹 🕑 E	dit 🔲 D	elete 🕈	+ * 10	Q n	nd 🔛 Diagram 🖃 Pad	ket Trace			A 444 - 107 - 10 - 10 -
Traffic Classification						Dula Arthura	A W00 + M FOC M C		
Name		Enabled	Match	Source	Destination	Service	Time	Rule Actions Filter:	Filter:
Global; Policy:	q_ledolg	olicy							Name
inspection_de			Metch	st any	🥌 any	default-inspec		Inspect DNS Map migrate.	- IPv4 Network Objects
								Inspect ESMTP Inspect FTP Inspect H323 H225 Inspect H323 RA5 Inspect M323 RA5 Inspect M2TBIOS Inspect RSH Inspect RSH Inspect RSH Inspect SUMPT Inspect SUMPT Inspect SUMPT Inspect SUMPT Inspect SUMPT Inspect SUMPT	Ð

Aqui está um exemplo da configuração de CLI equivalente, para sua referência:



Comportamento padrão do Cisco ASA para permitir pacotes RSVP

Por padrão, a inspeção de opções de IP está ativada. Vá para **Configuration > Firewall > Service Policy Rules**. Selecione a Política global, clique em **Editar** e selecione a guia **Inspeções padrão**. Aqui, você encontrará o protocolo RSVP no campo **IP-Options**. Isso garante que o protocolo RSVP seja inspecionado e permitido através do Cisco ASA. Como resultado, uma chamada de vídeo de ponta a ponta é estabelecida sem nenhum problema.

🖆 Edit Service Policy Rule

Traffic Classification Default Inspections Rule Actions

Following services will match the default inspection traffic:

Service	Protocol	Port
ctiqbe	tcp	2748
dns	udp	53
ftp	tcp	21
gtp	udp	2123, 3386
h323 - h225	tcp	1720
h323 - ras	udp	1718 - 1719
http	tcp	80
icmp	icmp	
ils	tcp	389
ip-options	rsvp	
mgcp	udp	2427, 2727
netbios	udp	137 - 138
radius-acct	udp	1646
rpc	udp	111
rsh	tcp	514
rtsp	tcp	554
sin	ten	5060

Verificar

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

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

• show service-policy inspect ip-options - Exibe o número de pacotes descartados e/ou permitidos de acordo com a regra de política de serviço configurada.

Troubleshoot

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

Informações Relacionadas

- Suporte técnico para dispositivos de segurança adaptável Cisco ASA 5500 Series
- <u>Suporte Técnico e Documentação Cisco Systems</u>