ASDM 6.3以降でのIPオプションインスペクショ ンの設定

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 表記法

 背景説明

 設定

 ASDM の設定

 RSVP パケットを許可するための Cisco ASA のデフォルト動作

 確認

 トラブルシュート

 関連情報

<u>概要</u>

このドキュメントでは、特定の IP オプションがイネーブルの IP パケットを送信するために Cisco 適応型セキュリティ アプライアンス(ASA)を設定する方法について設定例を紹介します

<u>前提条件</u>

<u>要件</u>

0

このドキュメントに特有の要件はありません。

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• Cisco ASA ソフトウェア リリース バージョン 8.3 以降

• Cisco Adaptive Security Manager ソフトウェア リリース バージョン 6.3 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

<u>背景説明</u>

各 IP パケットには、Options フィールドのある IP ヘッダーが含まれています。Options フィール ドは、通常は IP オプションと呼ばれ、制御機能を提供します。特定の状況で必要になりますが、 一般的な通信では必要ありません。具体的には、IP オプションにはタイムスタンプ、セキュリテ ィ、および特殊なルーティングの規定が含まれています。IP オプションの使用は任意であり、こ のフィールドにはオプションを 0 個、1 個、またはそれ以上含めることができます。

IP オプションはセキュリティ リスクであり、ASA から IP オプション フィールドを含む IP パケ ットが渡された場合、ネットワークの内部設定の詳細が外部に漏れてしまいます。そのため、攻 撃者はネットワークのトポロジをマッピングできます。Cisco ASA は企業のセキュリティを強化 するデバイスですので、IP オプション フィールドを含むパケットはデフォルトでドロップします 。参考のため、syslog メッセージ サンプルを以下に示します。

106012|10.110.1.34||XX.YY.ZZ.ZZ||Deny IP from 10.110.1.34 to XX.YY.ZZ.ZZ, IP options:"Router Alert"

ただし、ビデオ トラフィックを Cisco ASA 経由で渡す必要がある特定の導入シナリオでは、特定の IP オプションを含む IP パケットを渡す必要があり、そうしないとビデオ会議コールができなくなる可能性があります。Cisco ASA ソフトウェア リリース 8.2.2 以降では、「IP オプションのインスペクション」という新機能が導入されました。この機能を使用すると、特定の IP オプションョンを含むパケットが Cisco ASA を通過できるように制御できます。

デフォルトでこの機能は有効であり、以下の IP オプション インスペクションは、グローバル ポ リシーで有効にされています。このインスペクションを設定することで、パケットの転送許可や 、指定した IP オプションをクリアした後にパケットの転送を許可することを ASA に指示します 。

- End of Options List (EOOL) または IP オプション 0 オプションのリストの終わりを示すた めにすべてのオプションの最後に置かれます。
- No Operation (NOP) または IP オプション 1 フィールド変数全体の長さを示します。
- Router Alert (RTRALT) または IP オプション 20 このオプションは、中継ルータに対し、 パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知し ます。

<u>設定</u>

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

注:このセクションで使用さ<u>れるコマンドの詳細を調べる</u>には、<u>Command Lookup Tool(登録</u>ユ ーザ専用)を使用してください。

<u>ASDM の設定</u>

ASDM を使用すると、IP オプション フィールド(NOP)を含む IP パケットのインスペクション を有効にする方法がわかります。

IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることが でき、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数で ある必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合、NOP オプ ションは、オプションを 32 ビット境界上に揃えるために、「内部パディング」として使用され ます。

1. [Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IP-Options] に移動し、[Add] をク リックします。

Cor	nfiguration > Firewall > Objects > Inspect M	Maps > IP-Options	
Co	nfigure IP-Options maps.		
Ib-	Options Inspect Maps		
	Name	Description	Add
			Edit
			Delete

2. [Add IP-Options Inspect Map] ウィンドウが表示されます。インスペクション マップの名前 を指定し、[Allow packets with the No Operation (NOP)] オプションを選択して、[OK] をク

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		Name: (testmap)
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		Description:
 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 		Parameters
 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 		Allow packets with the End of Options List (EOOL) option
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		Clear the option value from the packets
Allow packets with the Router Alert (RTRALT) option Clear the option value from the packets		Allow packets with the No Operation (NOP) option
Allow packets with the Router Alert (RTRALT) option Clear the option value from the packets		
Clear the option value from the packets		Allow packets with the Router Alert (RTRALT) option
		Clear the option value from the packets
クレます。	クします。	OK Cancel Help 注

3. **testmap という名前の新しいインスペクション マップが作成されます。**[Apply] をクリック します。

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

 [Configuration] > [Firewall] > [Service Policy Rules] に移動し、既存のグローバル ポリシーを 選択して、[Edit] をクリックします。[Edit Service Policy Rule] ウィンドウが表示されます。 [Rule Actions] タブを選択し、[IP-Options] アイテムにチェックマークを入れ、[Configure] を 選択して新しく作成されたインスペクション マップを割り当てます。

🖆 Edit Service Policy Rule	Ê	
Traffic Classification Default 1	Inspections Rule Act	tions
Protocol Inspection Conne	ction Settings 0oS	NetFlow
	Configure	
DNS	Configure	DNS Inspect Map: migrated_dns_1
ESMTP	Configure	
FTP	Configure	
GTP	Configure	
H.323 H.225	Configure	
H.323 RA5	Configure	
HTTP	Configure	
ICMP		
ICMP Error		
ns I		
IM	Configure	
IP-Options	Configure	
IPSec-Pass-Thru	Configure	
MMD	Configure	

5. [Select an IP-Options inspect map for fine control over inspection] > [testmap] を選択し、

🚳 Select IP-Options Inspect Map	
O Use the default IP-Options inspection map	over inspection
Name testmap	Add
OK Cancel Help	

6. 選択したインスペクション マップは、[IP-Options] フィールドに表示されます。[OK] をクリ ックして [Service Policy Rules] タブに戻ります。

affic Classification Default I	nspections Rule Act	tions
Protocol Inspection Conner	ction Settings QoS	NetFlow
Select all inspection rule	s	
CTIQBE		
DCERPC	Configure	
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		
ILS ILS		
MI 🗌 IM	Configure	
IP-Options	Configure	IP-Options Inspect Map: testmap
IPSec-Pass-Thru	Configure	
MMP	Configure	
MGCP	Configure	

7. [Rule Actions] タブにカーソルを合わせると、このグローバル マップに関連付けられている すべての使用可能なプロトコル インスペクション マップが見つかります。

🗣 Add 🔹 🌌 Ed	dd 🕶 🗹 Edit 📋 Delete 🗇 🌾 👗 🖓 🎆 🕤 🔾 Find 🖼 Diagram 🕰 Packet Trace						Addresses		
Traffic Classificat	ion								Add • 🔤 Cot 📑 De
Name		Enabled	Match	Source	Destination	Service	Time	Hule Actions	Filten
🗄 Global; Policy: ç	d ledol	olicy							Name
inspection_de.			Retch	st any	🥌 any	default-inspec		 Inspect DNS Map migrate. 	IPv4 Network Objects
								Inspect ESMTP Inspect FTP Inspect H323 H225 Inspect H323 HA5 Inspect M323 RA5 Inspect RSH Inspect RSH Inspect RSH Inspect SUM Inspect SUM	Ð

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

<u>RSVP パケットを許可するための Cisco ASA のデフォルト動作</u>

IP オプション インスペクションはデフォルトでイネーブルになっています。[Configuration] > [Firewall] > [Service Policy Rules] に移動します。[Global Policy] を選択し、[Edit] をクリックして [Default Inspections] タブを選択します。ここでは、[IP-Options] フィールド内の RSVP プロトコ ルが表示されます。これにより、RSVP プロトコルが確実に検査され、Cisco ASA を通じて許可 されます。その結果、エンドツーエンドのビデオ通話が問題なく確立されます。

🜃 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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

show service-policy inspect ip-options - 設定したサービス ポリシー ルールに従って、ドロップ/許可されたパケットの数を表示します。

<u>トラブルシュート</u>

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのテクニカルサポート
- <u>テクニカル サポートとドキュメント Cisco Systems</u>