ASDM(On-BoxManagement)による Cisco セ キュリティ インテリジェンスを使用する間の IP ブラックリストの設定

内容

概要
前提条件
要件
使用するコンポーネント
背景説明
Security Intelligence フィードの概要
グローバル ブラックリストとグローバル ホワイトリストへの手動による IP アドレスの追加
ブラックリスト IP アドレスのカスタム リストの作成
Security Intelligence の設定
アクセス コントロール ポリシーの展開
Security Intelligence のイベントのモニタリング
確認
トラブルシュート
関連情報

概要

このドキュメントでは、Cisco Security Intelligence および IP アドレス レピュテーションの概要 と、レピュテーションが低い IP アドレスのカスタム/自動フィードを使用しながら IP ブラックリ スト(ブロッキング リスト)を構成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA(適応型セキュリティ アプライアンス)ファイアウォール、ASDM(Adaptive Security Device Manager)。
- FirePOWER アプライアンスの知識

Security Intelligence

使用するコンポーネント

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。

- ソフトウェア バージョン 5.4.1 以降が稼働する ASA FirePOWER モジュール(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- ソフトウェア バージョン 6.0.0 以降が稼働する ASA FirePOWER モジュール(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)

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。

背景説明

Cisco Security Intelligence は、Cisco TALOS チームによってレピュテーションが低いと判断され た IP アドレスのコレクションからなります。これらのコレクションは、定期的に更新されます。 .Cisco TALOS チームは、スパム、マルウェア、フィッシング攻撃などの不正なアクティビティ の発信元 IP アドレスを、レピュテーションの低い IP アドレスとして判断します。

Cisco IP Security Intelligence フィードは、攻撃者のデータベース、Bogon、ボット、CnC、 Dga、ExploitKit、マルウェア、Open_proxy、Open_relay、フィッシング、レスポンス、スパム、 不審な IP アドレスを追跡します。FirePOWER モジュールには、レピュテーションの低い IP ア ドレスのカスタム フィードを作成するオプションがあります。

Security Intelligence フィードの概要

Security Intelligence で各種のカテゴリとして分類できる IP アドレス コレクションのタイプについて説明します。

攻撃者:継続的に脆弱性をスキャンしている IP アドレスや、他のシステムを悪用しようとする IP アドレスのコレクション。

マルウェア:マルウェアの伝播を試みている IP アドレスや、アクセスしてきた閲覧者をアクティ ブに攻撃する IP アドレスのコレクション。

フィッシング:アクティブにエンドユーザをだまして機密情報(ユーザ名やパスワード)を入力 させようとするホストのコレクション

スパム:迷惑メールの送信元として識別されたホストのコレクション。

ボット:ボットネットの一部としてアクティブに参加しているホストや、既知のボットネット コントローラによって制御されているホストのコレクション。

CnC: 既知のボットネットを制御しているサーバとして識別されたホストのコレクション。

OpenProxy:オープン Web プロキシを実行し、匿名 Web ブラウジング サービスを提供している ことが判明したホストのコレクション。

OpenRelay:スパムやフィッシングの攻撃者が使用する匿名メール中継サービスを提供している ことが判明したホストのコレクション。

TorExitNode: Tor アノニマイザー ネットワークの出口ノード サービスを提供していることが判

明したホストのコレクション。

Bogon:割り振られていないのにトラフィックを送信している IP アドレスのコレクション。

不審:不審なアクティビティを見せていているため、現在調査中の IP アドレスのコレクション。

レスポンス:不審または不正な動作に関与していることが度々確認された IP アドレスのコレクション。

グローバル ブラックリストとグローバル ホワイトリストへの手 動による IP アドレスの追加

特定の IP アドレスが不正なアクティビティに関与していることがわかった場合、FirePOWER モ ジュールを使用することで、その IP アドレスをグローバル ブラックリストに追加できます。ブ ラックリスト IP アドレスでブロックされている特定の IP アドレスに対してトラフィックを許可 する必要がある場合は、その IP アドレスをグローバル ホワイトリストに追加することもできま す。IP アドレスをグローバル ブラックリスト/グローバル ホワイトリストに追加すると、その変 更は即時に適用されるため、ポリシーを適用する必要はありません。

IP アドレスをグローバル ブラックリスト/グローバル ホワイトリストに追加するには、 [Monitoring] > [ASA FirePOWER Monitoring] > [Real Time Eventing] に移動し、マウスのカーソル を該当する接続イベントに合わせて [View Details] を選択します。

グローバル ブラックリスト/グローバル ホワイトリストには、送信元 IP アドレスまたは宛先 IP アドレスのいずれかを追加できます。[Edit] ボタンをクリックし、[Whitelist Now/Blacklist Now] を選択すると、該当するリストに IP アドレスが追加されます(次の図を参照)。

All ASA FirePOWER E	Events Connection Intr	usion File Malware File	Security Intelligence	
Filter				
Rule Action=Allow *				
<u></u>				
Pause Refree	sh Rate 5 seconds	· 1/25/16 9:11:	25 AM (IST)	
Receive Times	Action	First Packet	Last Packet	Reaso
1/25/16 9:09:50 AM	Allow	1/25/16 9:09:48 AM	1/25/16 9:09:49 AM	
1/25/16 9:07:36 AM	Allow	View d 1/25/16 9:07:03 AM	etails 1/25/16 9:07:03 AM	
1/25/16 9:07:07 AM	Allow	1/25/16 9:07:06 AM	1/25/16 9:07:06 AM	
pring > ASA FirePOWER M	lonitoring > Real Time E	venting		
Initiator		Responder	Edit _	
Initiator ID	192.168.20.3	Responder IP	10.106.44.55	1
Initiator IF				
Initiator Country and Continent	not available Whitelist Blacklist I	Now Responder Cou Now Continent	ntry and not available	

送信元または宛先 IP アドレスがグローバル ホワイトリスト グローバル ブラックリストに追加さ れたことを確認するには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、グローバル ブラッ クリスト/グローバル ホワイトリストを編集します。.また、削除ボタンを使用して、リストから IP アドレスを削除することもできます。

ブラックリスト IP アドレスのカスタム リストの作成

FirePOWER では、カスタム ネットワーク/IP アドレス リストを作成して、そのリストをブラッ クリスト(ブロッキング リスト)で使用できるようになっています。 それには次の方法がありま す。

- IP アドレスをテキスト ファイルに書き込み(1 行につき 1 つの IP アドレス)、そのファイ ルを FirePOWER モジュールにアップロードします。ファイルをアップロードするには、 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、[Add Network Lists and Feeds] をクリッ クします。 [Name]: カスタム リストの名前を指定します。 Type: ドロップ ダウン リストから [List] を選択します。 [Upload List]: [Browse] を選択して、システム 内でアップロードするテキスト ファイルを見つけます。[Upload] オプションを選択してフ ァイルをアップロードします。
- 2. サードパーティの IP データベースをカスタム リストとして使用することもできます。この 場合、FirePOWER モジュールはサードパーティのサーバに接続して IP アドレス リストを 取得します。このように設定するには、[Configuration] > [ASA FirePOWER Configuration] >

[Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、[Add Network Lists and Feeds] をクリックします。 [Name]: カスタム フィードの名前を指定します。

Type:ドロップダウン リストから [Feed] オプションを選択します。

[Feed URL]: FirePOWER モジュールが接続してフィードをダウンロードするために使用 するサーバの URL を指定します。

[MD5 URL]:フィードの URL パスを検証するために使用するハッシュ値を指定します。

[Update Frequency]:システムが URL フィード サーバに接続する時間間隔を指定します。

		Ipdate Feeds O Add Network Lists an	nd Fee
Name	Security Intelli	gence for Network List / Feed	d ?
Cisco-Intelligence-Feed Last Updated: 2016-01-22 05:56	Name:	Custom_Feed	
Custom_Feed	Туре:	List	
Global-Blacklist	Upload List:	C:\fakepath\Custom_IP_Feed.	owse
olahat wikitaliat	Opioad		
guration > ASA FirePOWER Configurat	tion > Object Managemen	Store ASA FirePOWER Changes Ca	Feed
	tion > Object Managemen	Store ASA FirePOWER Changes Ca t > SecurityIntelligence > Network Lists and pdate Feeds O Add Network Lists an	Feed
	tion > Object Managemen	Store ASA FirePOWER Changes Ca t > SecurityIntelligence > Network Lists and pdate Feeds O Add Network Lists an gence for Network List / Feed	Feed d Fee
guration > ASA FirePOWER Configurat Name Disco-Intelligence-Feed .ast Updated: 2016-01-22 05:56:	tion > Object Managemen	Store ASA FirePOWER Changes Ca t > SecurityIntelligence > Network Lists and pdate Feeds O Add Network Lists an gence for Network List / Feed Custom_Network_Feed	Feed d Fee
guration > ASA FirePOWER Configurat Name Disco-Intelligence-Feed .ast Updated: 2016-01-22 05:56:	tion > Object Managemen	Store ASA FirePOWER Changes Ca t > SecurityIntelligence > Network Lists and pdate Feeds O Add Network Lists an gence for Network List / Feed Custom_Network_Feed Feed	Feed
guration > ASA FirePOWER Configurat Name Disco-Intelligence-Feed .ast Updated: 2016-01-22 05:56: Dustom_Feed Global-Blacklist	tion > Object Managemen	Store ASA FirePOWER Changes Ca t > SecurityIntelligence > Network Lists and pdate Feeds Add Network Lists and gence for Network List / Feed Custom_Network_Feed Feed http://192.168.30.1/blacklist-IP.txt	Feed

Security Intelligence の設定

Security Intelligence を設定するには、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control Policy] に移動して、[Security Intelligence] タブを選択します。

[Available Object] の [Networks] から目的のフィードを選択し、[Whitelist/Blacklist] 列に移動して、不正な IP アドレスに対する接続を許可/ブロックします。

次の図に示されているアイコンをクリックすると、ロギングを有効にすることができます。

不正な IP 接続をブロックするのではなく、不正な IP 接続に対してイベントが生成されるだけに するには、フィードを右クリックして [Monitor-only (do not block)] を選択します(図を参照)。

Configuration > ASA FirePOWER Configuration > Policies > Access Control F	Policy	6
ASA FirePOWER		
Default Allow All Traffic Enter a description		You have unsaved changes
	📕 📃 Status: Policy Up-to-date on device	
Identity Policy: None SSL Policy: Default SSL Policy		
Rules Security Intelligence HTTP Responses Advanced		
Available Objects C Available Zones Search for a Network Search for a Network Networks URLs	DNS Policy: <u>Default DNS Policy</u> Whitelist (2) Networks	Blacklist (7) Enable logging
Attackers Attackers Bogon Bots	Add to Whitelist URLs Clobal-Whitelist (Any Zone)	Image: Solution of Control Image: Solution of Control <td< td=""></td<>
CnC Malware Open provy	Add to Blacklist	Block Monitor-only (do not block)
Open_relay Phishing		UR Select All Delete
1 Store 4	S& FirePOWER Channes Cancel	

AC ポリシーの変更を保存するには、[Store ASA Firepower Changes] オプションを選択します。

アクセス コントロール ポリシーの展開

変更を適用するには、アクセス コントロール ポリシーを導入する必要があります。ポリシーを適 用する前に、デバイス上のアクセス コントロール ポリシーが古いものであるかを示す標識を確認 してください。

センサーに変更を導入するには、c[Deploy] をクリックし、[**Deploy FirePOWER Changes**]を選択し、ポップアップウィ**ンドウで[Deploy]**を選択して変更を導入します。

File View Tools Wizards Window	Help Deploy • 💽 Refresh 🔇 Ba	ck 🔘 Forward ? H
Device List □ ♣ Add ① Delete Ø Connect	2 Deploy FirePOWER Changes Save Running Configuration	s Ctrl+D to Flash Ctrl+S
Deploy FirePOWER Changes		X
Deploy Policies Version:2016-0	L-05 09:09 AM	?
System Policy: Default		
 Access Control Policy: Default Allow A 	ll Traffic	
 Intrusion Policy: Balanced Security Intrusion Policy: IPS_Policy DNS Policy: Default DNS Policy 	and Connectivity	
	Benlay	Cancel
	3 Deploy	Cancel

: 5.4.x [Apply ASA FirePOWER Changes]

[Monitoring] > [ASA Firepower Monitoring] > [Task Status]

Security Intelligence のイベントのモニタリング

Security Intelligence を FirePOWER モジュールで標示するには、[Monitoring] > [ASA Firepower Monitoring] > [Real Time Eventing] に移動します。.[Security Intelligence] タブを選択します。次の図に示すように、イベントが表示されます。

Mon	itoring > ASA FirePOWER Monitor	ing > Real Time Event	ting				
Real	Time Eventing						
	All A FirePOWER Events	Connection Intrusion	File Malware File	Security Intelligence			
	Filter						
	Enter filter criteria	Enter filter criteria					
	Pause Refresh Rate 5 seconds 2/9/16 1:03:31 PM (IST)						
	Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP
	2/9/16 1:01:48 PM	Block	2/9/16 1:01:47 PM		IP Block	192.168.20.3	184.26.162.43

現在、この設定に使用できる確認手順はありません。

トラブルシュート

Security Intelligence フィードが最新のものであることを確認するには、[Configuration] > [ASA FirePOWER Configuration] > [Object Management] > [Security Intelligence] > [Network Lists and Feeds] に移動し、フィードが最後に更新された時刻を調べます。フィードの更新頻度を設定するには、[Edit] ボタンをクリックします。

Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds

Update Feeds O Add Network Lists and Feeds Filter				
Name	Туре			
Cisco-Intelligence-Feed Last Updated: 2016-02-08 10:03:14	Feed	Ø 8		
Custom_Feed	Feed	0		
Global-Blacklist	List	Ø 🗇		
Global-Whitelist	List	08		

アクセス コントロール ポリシーが正常に導入されたことを確認します。

Security Intelligence をモニタして、トラフィックがブロックされているかどうかを確認します。

Cisco ASA FirePOWER

• - Cisco Systems