CLIおよびFMC GUIを使用して、Firepowerセン サーからカスタムSIDリストを確認します

概要

このドキュメントでは、CLIおよびFMC GUIを使用して、Firepower Threat Defense(FTD)または FirePOWERモジュールからカスタムSIDリストを取得する方法について説明します。SID情報は 、FMC GUIで[Objects] > [*Intrusion Rules*]に移動する*と確認できます*。場合によっては、CLIから 使用可能なSIDのリストを取得する必要があります。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- Cisco Firepower Threat Defense (FTD)
- Cisco ASA with FirePOWER Services
- Cisco Firepower Management Center(FMC)
- Linuxの基礎知識

使用するコンポーネント

この文書の情報は、次のソフトウェアのバージョンに基づいています。

- Firepower Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- FirePOWERモジュール6.2.3.2

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 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

侵入ルールは、ネットワークの脆弱性を悪用しようとする試みを検出するためにシステムが使用 するキーワードと引数のセットです。システムがネットワークトラフィックを分析すると、パケ ットが各ルールで指定された条件と比較されます。パケットデータがルールで指定されたすべて の条件に一致すると、ルールがトリガーされます。ルールがアラートルールの場合、侵入イベン トが生成されます。パスルールの場合、トラフィックは無視されます。インライン展開の廃棄ル ールでは、システムはパケットを廃棄し、イベントを生成します。Firepower Management Center(FMC)Webコンソールから侵入イベントを表示および評価できます。

Firepowerシステムには、次の2種類の侵入ルールがあります。*共有オブジェクト規則*と標準テ**キ** スト規則です。Cisco Talos Security Intelligence and Research Group(Talos)は、共有オブジェク トルールを使用して、従来の標準テキストルールでは不可能だった脆弱性に対する攻撃を検出で きます。共有オブジェクトルールを作成することはできません。侵入ルールを独自に作成する場合は、標準のテキストルールを作成する必要があります。表示される可能性のあるイベントの種類を調整するためのカスタム標準テキストルール。ルールを記述し、ルールのイベントメッセージを指定することで、攻撃とポリシーの回避を示すトラフィックをより簡単に特定できます。

カスタム侵入ポリシーでカスタム標準テキストルールを有効にする場合、ルールキーワードや引 数によっては、トラフィックを最初に特定の方法でデコードまたは前処理する必要があることに 注意してください。

Firepower Systemのカスタムローカルルールは、ローカルマシンからASCIIテキストファイル形 式でインポートするカスタム標準Snortルールです。Firepowerシステムでは、Webインターフェ イスを使用してローカルルールをインポートできます。ローカル ルールをインポートする手順は 非常に簡単です。ただし、最適なローカルルールを作成するには、Snortおよびネットワークプロ トコルに関する詳細な知識が必要です。

警告:実稼働環境でルールを使用する前に、管理されたネットワーク環境を使用して、作成 した侵入ルールをテストしてください。不適切な侵入ルールがシステムのパフォーマンスに 重大な影響を与える可能性があります





設定

ローカル ルールのインポート

作業を開始する前に、カスタムファイルに記載されているルールに特殊文字が含まれていないことを確認する必要があります。ルールをインポートする際は、すべてのカスタム ルールを ASCII または UTF-8 エンコーディングを使用してインポートする必要があります。次に示す手順では、 ローカルマシンからローカル標準テキストルールをインポートする方法について説明します。

ステップ1:[Import Rules]タブにアク**セス**するには、[Objects] > [Intrusion Rules] > [Import Rules]に移動します。[ルールの更新]ページが次の図のように表示されます。

One-Time Rule Update/Rules Import							
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits: Intrusion ren editing aaa admin editing alanrod_test							
Source Policy Deploy	 Rule update or text rule file to upload and install Browse No file selected. Download new rule update from the Support Site Reapply all policies after the rule update import completes Import 						
Recurring Rule Update Imports							
The scheduled rule update feature is not enabled. Note: Importing will discard all unsaved intrusion pol	icy and network analysis policy edits.						
Enable Recurring Rule Update Imports from the Support Site	Save Cancel						

ステップ2:アップロードしてインストールするルール更新ファイルまたはテキストルールファイルを選択し、[参照]をクリックして、カスタムルールファイルを選択します

注:アップロードされたすべてのルールは、ローカルルールカテゴリ**に保存され**ます

ステップ3: [Import] をクリックします。ルールファイルがインポートされます

注:Firepowerシステムでは、検査に新しいルールセットは使用しません。ローカル ルールを アクティブにするには、侵入ポリシーでローカル ルールを有効にしてから、そのポリシー を適用します。

確認

FMC GUIから

1. FMC GUIからインポートされたローカルルールの表示

ステップ1:[Objects] > [Intrusion Rules]に移動します。

ステップ2:グループのルールからローカルルを選択します。

Overview Analysis Policies Devices	Objects AMP Intelligence		🖳 Deploy	System	Help 🔻 j	carvent 🔻
Object Management Intrusion Rules						
		🗍 Delete Loc	al Rules	earch Uplo	ead Update	Intrusion eate Rule
Crown Bulles By Level Dules	▼ Local Rules (38)					
	(1:1000000) Malicious SSL 04 Detected (1:1000001) Malicious SSL 03 Detected (1:1000002) Oracle - MALWARE-BACKDOOR CrossRAT initial connect (1:1000003) ClientsXX-google LDP 53 Alert (1:1000003) ClientsXX-google Callback Alert (1:1000006) Malformed_UA (1:1000006) Malformed_UA (1:1000007) ClientsXX-google Callback Alert (1:1000008) Malicious SSL 02 Detected (1:1000009) Malicious SSL 02 Detected (1:1000010) Oracle - MALWARE-BACKDOOR CrossRAT callback (1:1000011) Oracle CVE-2018-2894:Possible recon scan (1:1000012) Oracle CVE-2018-2894:First stage of the exploit (1:1000013) Oracle CVE-2018-2894:First stage of the exploit (1:1000014) Malicious SSL 03 Detected_1 (1:1000015) ClientsXX-google Callback Alert_1 (1:1000016) Oracle CVE-2018-2894:Possible recon scan_1 (1:1000017) Oracle CVE-2018-2894:Possible recon scan_1 (1:1000018) Malicious SSL 01 Detected_1 (1:1000019) Oracle - VE-2018-2894:Possible recon scan_1 (1:1000019) Oracle - NGRX open reverse proxy tunnel User Agent (1:1000021) Malicious SSL 02 Detected_1 (1:1000023) Malicious SSL 02 Detected_1	tion : detected tion_1 : detected_1				

デフォルトでは、Firepowerシステムはローカルルールをディセーブル状態に設定します。これらのローカルルールを侵入ポリシーで使用するには、ローカルルールの状態を手動で設定する必要があります。

2.侵入ポリシーからローカルルールを有効にする

ステップ1:[Policies] > [Intrusion] > [Intrusion Policy]の下の[Policy Editor] ページに移動します。

ステップ2: 左側のパネルで[ルール]を選択します。

ステップ3:[カテゴリ]で[local]を選択しま**す。**すべてのローカルルールが使用可能な場合は表示されます。

Overview Analysis Policies Dev	vices Objects AMP Ir	ntelligence			🔒 Deploy	System	i Help 🔻	jcarven	it v
Access Control > Intrusion Networ	k Discovery Application D	etectors	Correlation	Actions 🔻					
Edit Policy: Oracle Defau	It Intrusion Policy								
Policy Information	Rules							< Ba	ck
Rules	Rule Configuration	Filter:	Category:"loca	1"				×	?
Firepower Recommendations	Rule Content	_		0 selected rules of 38					
Advanced Settings	Category	$\rightarrow \bullet$	T •	⊙ • 0 • ⊃ •		Pol	icy		$\overline{}$
Policy Lavers	file-pdf	Rule State	Event Filtering	g Dynamic State Alerting Comments					
C Policy Layers	indicator-compromise	GID	SID	Message 🔺		⇒	<u>0</u> 7 0	•	
	indicator-obfuscation	1	1000007	ClientsXX-google Callback Alert					^
	indicator-scan	L 1	1000015	ClientsXX-google Callback Alert_1		\rightarrow			
	indicator-shellcode	1	1000003	ClientsXX-google UDP 53 Alert					
	local	1	1000024	ClientsXX-google UDP 53 Alert_1		\rightarrow			
	malware-backdoor	1	1000006	Malformed_UA		\rightarrow			
	malware-cnc	1	1000020	Malformed_UA_1		\rightarrow			
	malware-other	□ <u>1</u>	1000004	Malicious SSL 01 Detected		\rightarrow			
	malware-tools	1	1000018	Malicious SSL 01 Detected_1		\rightarrow			
		1	1000008	Malicious SSL 02 Detected		\rightarrow			
	Classifications	1	1000023	Malicious SSL 02 Detected_1		\rightarrow			
	Microsoft Vulnerabilities	□ 1	1000001	Malicious SSL 03 Detected		-			
	Microsoft Worms	1	1000014	Malicious SSL 03 Detected_1		\rightarrow			
	Platform Specific	1	1000000	Malicious SSL 04 Detected		\rightarrow			
	Preprocessors	1	1000022	Malicious SSL 04 Detected_1		\rightarrow			
	Priority			· · ·				_	*
	Rule Update					K <	1 of 1	> >I	

ステップ4:必要なローカルルールを選択します。

Overview Analysis Policies Dev	vices Objects AMP	Intelligence			. ● Deploy	Syster	n Help 🔻	jcarvent 🔻
Access Control + Intrusion Networ	k Discovery Application	Detectors	Correlation	Actions •				
Edit Policy: Oracle Defau	It Intrusion Policy	,						
Policy Information	Rules							< Back
Rules	Rule Configuration	Filter:	Category:"loca)"				× ?
Firepower Recommendations	Rule Content			7 selected rules of 38				
Advanced Settings	Category app-detect	⇒ •	Trent Filtering			Po	licy	~
Policy Layers	browser-chrome	GID	SID	Message A		-	(a) T C	0 🔍
	browser-firefox		1000007	ClientsXX-google Callback Alert				^
	browser-ie		1000015	ClientsXX-google Callback Alert_1				
	browser-other	✓ 1	1000003	ClientsXX-google UDP 53 Alert				
	browser-plugins	⊻ 1	1000024	ClientsXX-google UDP 53 Alert_1				
	browser-webkit	1	1000006	Malformed_UA		\rightarrow		
	content-replace	✓ 1	1000020	Malformed_UA_1		-		
	decoder		1000004	Malicious SSL 01 Detected		\rightarrow		
	exploit-kit		1000018	Malicious SSL 01 Detected_1		\rightarrow		
	file-executable	1	1000008	Malicious SSL 02 Detected		\rightarrow		
	Classifications	<u></u> ∠ 1	1000023	Malicious SSL 02 Detected_1		\rightarrow		
	Microsoft Vulnerabilities	i 🔽 1	1000001	Malicious SSL 03 Detected		\rightarrow		
	Microsoft Worms		1000014	Malicious SSL 03 Detected_1		\rightarrow		
	Platform Specific	🗹 1	1000000	Malicious SSL 04 Detected		\rightarrow		
	Preprocessors		1000022	Malicious SSL 04 Detected_1		\rightarrow		
	Priority			· · ·				
	Rule Update					K <	1 of 1	>>

ステップ5:必要なローカル・ルールを選択した後、「ルールの状態」から状態を選択します

	⇒ ▼	7 •
	Rule State	Event Filtering
C	Generate I	Events
	Drop and (Generate Events
Ē	Disable	

次のオプションを使用できます。

- イベントの生成: ルールを有効にし、イベントを生成します

- イベントのドロップと生成:ルールの有効化、トラフィックのドロップ、イベントの生成

-無効化:ルールを有効にしない、イベントを無効にする

手順 6: ルールの状態を選択したら、 左側のパネルの[Policy Information]オプション

Overview Analysis Policies Devic	es Objects AMP I	ntelligence			$oldsymbol{ extsf{0}}_1$ Deploy	System	Help 🔻	jcan	vent 🔻
Access Control > Intrusion Network	Discovery Application D	etectors	Correlation	Actions 🔻					
Edit Policy: Oracle Default	Intrusion Policy								
Policy Information	Rules							<	Back
Rules	Rule Configuration	Filter:	Category:"loc	al"					× ?
Firepower Recommendations	Rule Content			7 selected rules of 38					
Advanced Settings	Category app-detect	⇒ ▼ Pule State	Transferrer	⊙ ▼ 00 ▼		Polic	Ŷ		~
Policy Layers	browser-chrome	GID	SID	Message		⇒ (970	0	2
	browser-firefox		1000007	ClientsXX-google Callback Alert		-			^
	browser-ie	1	1000015	ClientsXX-google Callback Alert_1		\rightarrow			
	browser-other	✓ 1	1000003	ClientsXX-google UDP 53 Alert					
	browser-plugins	1	1000024	ClientsXX-google UDP 53 Alert_1					
	browser-webkit	1	1000006	Malformed_UA					
	content-replace	1	1000020	Malformed_UA_1		→			
	decoder	1	1000004	Malicious SSL 01 Detected					
	exploit-kit	1	1000018	Malicious SSL 01 Detected_1		\rightarrow			
	file-executable	2 1	1000008	Malicious SSL 02 Detected					
	Classifications	✓ 1	1000023	Malicious SSL 02 Detected_1		-			
	Microsoft Vulnerabilities	1	1000001	Malicious SSL 03 Detected					
	Microsoft Worms	1	1000014	Malicious SSL 03 Detected_1		\rightarrow			
	Platform Specific	✓ 1	1000000	Malicious SSL 04 Detected		-			
	Preprocessors	1	1000022	Malicious SSL 04 Detected_1		\rightarrow			~

ステップ7:[Commit Changes]ボタンを選択し、変更の簡単な説明を入力します。後で[OK]をクリ ックします。侵入ポリシーが検証されます。

7.30

Description of Changes

This is techzone.		
	ок	Cancel

注:侵入ポリシーの侵入イベントしきい値機能と組み合わせて非推奨のしきい値キーワード を使用するインポートされたローカルルールを有効にすると、ポリシー検証は失敗します。

ステップ8:変更の展開

FTDまたはSFRモジュールのCLIから

1. FTDまたはSFRモジュールのCLIからインポートされたローカルルールを表示する

ステップ1:SFRモジュールまたはFTDからSSHまたはCLIセッションを確立します

ステップ2:エキスパートモードに移動します。

> expert admin@firepower:~\$ ステップ3:管理者権限の取得

admin@firepower:~\$ sudo su - ステップ4:パスワードを入力します

admin@firepower:~\$ sudo su -Password: root@firepower:~# ステップ5:/ngfw/var/sf/detection_engines/UUID/intrusion/に移動します。

root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion/ root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#

注:SFRモジュールを使用している場合は、/ngfw/var/sf/detection_engines/*/intrusion pathを使用しないでください。insted use **/var/sf/detection_engines/*/intrusion**

ステップ6:次のコマンドを導入します

grep -Eo "sid:*([0-9]{1,8})" */*local.rules 次の図を例として参照してください。

root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000007
sid:1000004
sid:1000004

これにより、FTDまたはSFRモジュールで有効になっているカスタマーSIDリストが表示されま す。

トラブルシュート

. . .

ステップ1: FMC detection_enginesからSFRモジュールまたはFTDへのSSHセッションが確立されていないことを確認します

ステップ2:コマンドgrep -Eo "sid:*([0-9]{1,8})" */*local.rulesは侵入ディレクトリでのみ動作します 。このコマンドは別のディレクトリからは使用できません

ステップ3: grep -Eo "sid:*([0-9]{1,8})" */*.rulesコマンドを使用して、すべてのカテゴリから完全な SIDリストを取得します

ローカル侵入ルールをインポートするためのベストプラクティス

ローカル規則ファイルをインポートする場合は、次のガイドラインに従ってください。

- ルールのインポートでは、すべてのカスタムルールをプレーンテキストファイルにインポートし、ASCIIまたはUTF-8でエンコードする必要があります
- テキストファイル名には、英数字、スペース、およびアンダースコア(_)、ピリオド(.)、ダッシュ(-)以外の特殊文字を使用できません
- ローカルルールの先頭にポンド文字(#)が1つ付いてインポートされますが、削除のフラグが 付けられます
- システムは、1つのシャープ文字(#)で始まるローカルルールをインポートし、2つのシャープ 文字(##)で始まるローカルルールはインポートしません
- ルールにエスケープ文字を含めることはできません
- ローカルルールをインポートするときに、ジェネレータID(GID)を指定する必要はありません
 この場合、標準のテキストルールに対してGID 1のみを指定します
- ルールを初めてインポートする場合は、次の手順を実行します not を指定 Snort ID (SID)また はリビジョン番号。これにより、削除されたルールを含む、他のルールの SID との競合が回 避されます。システムは、次に使用可能なカスタムルールSID 1000000以上、リビジョン番 号1を自動的にルールに割り当てます
- SIDを持つルールをインポートする必要がある場合、SIDは1,000,000 ~ 9,999,999の一意の

番号である必要があります

- マルチドメイン展開では、システムは、WLC上のすべてのドメインで使用される共有プール からインポートされたルールにSIDを割り当てます Firepower Management Center.複数の管 理者が同時にローカルルールをインポートしている場合、システムが別のドメインにシーケ ンスの間に番号を割り当てているため、個々のドメイン内のSIDが連続していないように見え る場合があります
- ・以前にインポートしたローカルルールの更新バージョンをインポートする場合、または削除したローカルルールを復元する場合は、システムによって割り当てられたSIDと現在のリビジョン番号より大きいリビジョン番号を含める必要があります。ルールを編集することで、現在または削除されているルールのリビジョン番号を確認できます

注: ローカルルールを削除すると、システムによってリビジョン番号が自動的に増分されま す。これは、ローカル ルールを復元できるようにするための方法です。削除されたすべて のローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動 されます。

- SIDの番号付けの問題を回避するために、プライマリFirepower Management Center(FMC)で ハイアベイラビリティペアのローカルルールをインポートします
- ルールに次のいずれかが含まれている場合、インポートは失敗します。SIDが2147483647より大きい64文字を超える送信元ポートまたは宛先ポートのリスト
- ・侵入ポリシーの侵入イベントしきい値機能と組み合わせて非推奨のしきい値キーワードを使用するインポートされたローカルルールを有効にすると、ポリシーの検証が失敗します
- インポートされたすべてのローカルルールは、ローカルルールカテゴリに自動的に保存されます
- インポートするローカルルールは、常に無効なルール状態に設定されます。ローカルルール を侵入ポリシーで使用するには、ローカルルールの状態を手動で設定する必要があります

関連情報

Snort SIDに関連する参照用のドキュメントを次に示します。

侵入ルールの更新

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

侵入ルールエディタ

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-configguide-v66/the_intrusion_rules_editor.html