# FDM管理データ・インタフェースのサイト間 VPNでのSNMPの構成

内谷
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>コンフィギュレーション</u>
<u>確認</u>
<u>トラブルシュート</u>
関連情報

## はじめに

このドキュメントでは、FTDデバイスデータインターフェイスのデータインターフェイス上のサ イト間VPNを介してリモートエンドにSNMPを設定する方法について説明します。

# 前提条件

設定に進む前に、次の前提条件が満たされていることを確認してください。

- 次の項目に関する基本的な知識
  - Cisco Firepower Threat Defense(FTD)は、Firepower Device Manager(FDM)によって 管理されます。
  - Cisco適応型セキュリティアプライアンス(ASA)
  - 簡易ネットワーク管理プロトコル(SNMP)。
  - ◎ バーチャルプライベートネットワーク(VPN)。
- FTDおよびASAデバイスへの管理アクセス。
- ネットワークが稼働中であり、コマンドの潜在的な影響を理解していることを確認します。

#### 要件

- FDMバージョン7.2.7で管理されるCisco FTD
- Cisco ASA バージョン 9.16
- SNMPサーバの詳細(IPアドレス、コミュニティストリングなど)
- ・ サイト間VPN設定の詳細(ピアIP、事前共有キーなど)
- REST APIを使用してSNMPを設定するには、FTDがバージョン6.7以降である必要があります。

#### 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。

- Firepower Device Manager(FDM)バージョン7.2.7で管理されるCisco Firepower Threat Defense(FTD)。
- Cisco Adaptive Security Appliance (ASA) バージョン 9.16.
- SNMPサーバ(任意の標準SNMPサーバソフトウェア)

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、クリアな(デフォルト)設定で作業を開始していま 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

これらの手順の概要を説明すると、ネットワーク管理者はネットワークデバイスをリモートから 監視できます。

SNMP(Simple Network Management Protocol)は、ネットワーク管理と監視に使用されます。この設定では、ASAと確立されたサイト間VPNを介して、FTDからリモートSNMPサーバにSNMPトラフィックが送信されます。

このガイドの目的は、ネットワーク管理者がFTDデバイスのデータインターフェイス上のサイト 間VPNを介してリモートエンドにSNMPを設定できるようにすることです。この設定は、ネット ワークデバイスをリモートで監視および管理する場合に便利です。この設定では、SNMP v2が使 用され、ASAと確立されたサイト間VPNを介して、FTDデータインターフェイスからリモート SNMPサーバにSNMPトラフィックが送信されます。

使用されるインターフェイスは「内部」と呼ばれますが、この設定は他のタイプの「to-the-box」 トラフィックに適用でき、VPNが終端するインターフェイス以外のファイアウォールの任意のイ ンターフェイスを利用できます。



注:SNMPは、FTDがバージョン6.7以降を実行し、FDMによって管理されている場合にのみ、REST APIを介して設定できます。

設定



注:この設定では、サイト間VPNがすでにデバイス間で設定されていると見なされます 。サイト間VPNの設定方法の詳細については、設定ガイドを参照してください。<u>FDMに</u> <u>よって管理されるFTDのサイト間VPNの設定</u>

コンフィギュレーション

1. FTDにログインします。



2. デバイスの概要の下で、APIエクスプローラに移動します。

					adn <i>Adr</i>	×	
ervices Registere	d   Regi	Ster	API Ex	plorer	0	CONFIGURE	

#### 3. FTDでのSNMPv2の設定

• インターフェイス情報を取得します。



4. 下にスクロールしてTry it out!ボタンを選択し、APIコールを行います。コールが成功すると、 応答コード200が返されます TRY IT OUT!

Hide Response

### Curl

```
curl -X GET ---header 'Accept: application/json' 'https:,
```

#### Request URL

https://

34/api/fdm/v6/devices/default/interfaces

### **Response Body**

```
l_{1}
Ł
 "version": "mgjiipiswsgsx",
 "name": "inside".
 "description": null.
 "hardwareName": "GigabitEthernet0/1",
 "monitorInterface": false.
 "ipv4": {
   "ipType": "STATIC",
   "defaultRouteUsingDHCP": false,
   "dhcpRouteMetric": null.
    "ipAddress": {
      "ipAddress": "10.57.58.1",
      "netmask": "255.255.255.0",
      "standbyIpAddress": null,
      "type": "haipv4address"
    34
   "dhcp": false,
   "addressNull": false,
   "type": "interfaceipv4"
  ¥....
```

### **Response Code**

・ SNMPホストのNetwork Object Configを作成します。



• 新しいSNMPv2cホストオブジェクトを作成します。

SNMP	
GET	/devicesettings/default/snmpservers
GET	/devicesettings/default/snmpservers/{objId}
PUT	/devicesettings/default/snmpservers/{objld}
GET	/object/snmpusers
POST	/object/snmpusers
DELETE	/object/snmpusers/{objld}
GET	/object/snmpusers/{objld}
PUT	/object/snmpusers/{objld}
GET	/object/snmpusergroups
POST	/object/snmpusergroups
DELETE	/object/snmpusergroups/{objld}
GET	/object/snmpusergroups/{objld}
PUT	/object/snmpusergroups/{objld}
GET	/object/snmphosts
POST	/object/snmphosts
DELETE	/object/snmphosts/{objld}
GET	/object/snmphosts/{objld}
PUT	/object/snmphosts/{objld}

詳細については、設定ガイドの「<u>Firepower FDMでのSNMPの設定とトラブルシューティング</u>」 を参照してください。

5. デバイスでSNMPを設定したら、Advanced ConfigurationセクションのDeviceに移動し、View Configurationを選択します。



6. FlexConfigセクションで、FlexConfigオブジェクトを選択し、新しいオブジェクトを作成しま す。それに名前を付けて、テンプレートセクションでmanagement-accessコマンドを追加し、イ ンターフェイスを指定して、テンプレート否定部分でコマンド否定を追加します。



# Edit FlexConfig Object

Name	
Description	
This command gives mamt access to the Inside Interface.	li.
Variables There are no variables yet. Start with adding a new variable. + ADD VARIABLE	
Template	Expand
1 management-access Inside	
Negate Template 🛕	C Expand Q Reset
1 no management-access Inside	
	CANCEL

7. FlexConfigセクションで、FlexConfig Policyを選択し、追加アイコンをクリックして、前の手順で作成したflexConfigオブジェクトを選択し、OKを選択します。



## 8. その後、デバイスに適用されるコマンドのプレビューが表示されます。[Save] を選択します。

FlexConfig Policy		
Group List	Preview	4.4 Expand
+	1 management-access Inside	
SAM		

9. 構成を展開し、展開アイコンを選択して「今すぐ展開」をクリックします。



P	ending Changes		0	×
0	Last Deployment Completed Successfully 15 Oct 2024 08:06 PM. See Deployment History			
	Deployed Version (15 Oct 2024 08:06 PM)	Pending Version	0	LEGEND
0	FlexConfig Policy Edited: default-group			
	HORE ACTIONS Y	CANCE	YES OF NOW	¥



注:問題なく完了していることを確認します。タスクリストを確認できます。

## 確認

設定を確認するには、次のチェックを実行し、SSHまたはコンソールを使用してFTDにログイン し、次のコマンドを実行します。

• デバイスの実行コンフィギュレーションに加えた変更が含まれていることを確認します。

> system support diagnostic-cli Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available commands. firepower> enable Password: firepower# show running-config <some outouts are ommitted> object network snmpHost host 10.56.58.10 <some outputs are ommitted>
snmp-server host inside 10.56.58.10 community \*\*\*\*\* version 2c
snmp-server location null
snmp-server contact null
snmp-server community \*\*\*\*\*
<some outputs are omitted>
management-access inside

#### • SNMPテスターからテストを実行し、テストが正常に完了することを確認します。

2 Bus Yout
J. Kun lest
Stat Repeat every s seconds
New Test
Paesder SNMP Tester - 20.2.4 Computername: WIN10 Interface: 10.56.58, 10
10/16/2024 1:19:08 PM (1 ms) : Desize: 10.57.58.1
10/16/2024 1:19-08 DM (3 mi) - 53MD - 27
10/16/2024 1119/08 PM (5 ms) 1 Uptime
10/16/2024 1:19:08 PM (47 ms) : SPMP Datatype: ASN_TIMETICIS
10/16/2024 1:19:08 PM (49 ms) :
10/16/2024 1:19:08 PM (51 ms) : DISMAN-EVENT-MI8::sysUpTimeInstance = 15632700 ( 43 hours 25 minutes )
10/16/2024 1:19:08 PM (118 ms) : SNMP Datatype: SNMP_EXCEPTION_NOS/CHORJECT
10/16/2024 1:19:08 PM (120 m) - HOST RESCI ROPS MIR- InStated Infine 0 = IN SMMP EXCEPTION NOS ICHORECT222 (0 seconds )
The second
10/16/20/24 1119/08 PPI (122 ms) 1 Done

# トラブルシュート

問題が発生した場合は、次の手順を検討してください。

 VPNトンネルが稼働していることを確認します。次のコマンドを実行して、VPNトンネル を確認できます。

firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status Role 442665449 10.197.225.82/500 10.197.225.81/500 READY RESPONDER Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:14, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/10 sec Child sa: local selector 10.57.58.0/0 - 10.57.58.255/65535 remote selector 10.56.58.0/0 - 10.56.58.255/65535 ESP spi in/out: 0x3c8ba92b/0xf79c95a9

firepower# show crypto ikev2 stats

Global IKEv2 Statistics Active Tunnels: 1 Previous Tunnels: 2

IKEv2トンネルのデバッグ方法の詳細については、「<u>IKEv2 VPNのデバッグ方法</u>」を参照してく

ださい。

SNMP設定を確認し、コミュニティストリングとアクセスコントロールの設定が両端で正しいことを確認します。

firepower# sh run snmp-server(sh run snmp-server) 10.56.58.10 community \*\*\*\*\*バージョン2c内のsnmp-server host snmp-server locationがnullです snmp-server contactがnullです SNMPサーバコミュニティ\*\*\*\*\*

• SNMPトラフィックがFTDを通過できることを確認します。

Policies > Access Controlに移動し、SNMPトラフィックを許可するルールがあることを確認します。

ules						٦	Filer			¢	F R -
		NOUNCE			DESTRUCTION				_		
1 1.000		2040	ALC: NO.	ACRES .	20468	ALC: NOTICE	PORTS	APPLICATIONS	98.8	100000	
1 igen in	Barrier	inside_sone	1001	A001	outside_rone	ANT	konp	ADD	ANY.	ABO	S. C.
2 long-out	8	outside_acce	1001	A001	inside_asse	400	long	A307	8897	.4007	¢.C
3 allow/0868		induide_pone	anangeticast	A257	inside_some	A81	2008 somp162	100	ANY	,4557	46.00
4 allowall	E	inside, some	1001	ADD	outside_pone	A81	2449	ABD	100	.4807	$\eta_{\mu}  \Omega_{\mu}$

・パケットキャプチャを使用してSNMPトラフィックを監視し、問題を特定します。

ファイアウォールでトレースによるキャプチャを有効にします。

capture snmp interface inside trace detail match udp any any eq snmp

firepower# show capture capture snmp type raw-data trace detail interface inside include-decrypted [Capturing - 405 bytes] match udp host 10.57.58.10 host 10.56.58.1 eq snmp

firepower# sh capture snmp 4 packets captured

1: 17:50:42.271806 10.56.58.10.49830 > 10.57.58.1.161: udp 43 2: 17:50:42.276551 10.56.58.10.49831 > 10.57.58.1.161: udp 43 3: 17:50:42.336118 10.56.58.10.49832 > 10.57.58.1.161: udp 44 4: 17:50:42.338803 10.56.58.10.49833 > 10.57.58.1.161: udp 43 4 packets shown

詳細については、『SNMP Configuration Guide』の「<u>Configure and Troubleshoot SNMP on</u> <u>Firepower FDM</u>」を参照してください。

#### 関連情報

- Cisco Secure Firepower Device Managerコンフィギュレーションガイド
- <u>Cisco ASAコンフィギュレーションガイド</u>
- ・ <u>シスコデバイスでのSNMPの設定</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。