Cisco XDRとSecure Firewallの統合およびトラブ ルシューティング

| 内容 |
|-----------------------------------|
| <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>設定</u> |
| <u>ライセンス</u> |
| <u>アカウントをSSXにリンクし、デバイスを登録します。</u> |
| <u>方法1(半分の統合):調査の充実</u> |
| <u>SSXへのデバイスの登録</u> |

はじめに

このドキュメントでは、Cisco XDRとSecure Firewallの統合、検証、およびトラブルシューティング に必要な手順について説明します。

Secure FirewallとXDRを統合するには2つの方法があり、それぞれの統合によって結果が異なります。

最初の方法では、Secure Firewall、Security Services Exchange(SSX)、Security Cloud Control、 XDR-Analytics、およびXDRを統合して調査を充実させる方法について説明します。

2つ目の方法では、Secure Firewall、SSX、Security Cloud Control、XDR-A、SAL Cloud、および XDRを統合してインシデントを強化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。

- Cisco Firewall Management Center(FMC)
- Cisco Secure Firewall脅威対策
- イメージの仮想化(オプション)
- Cisco Defense Orchestrator
- セキュリティサービス交換
- セキュリティクラウド制御

使用するコンポーネント

- セキュアファイアウォール:7.2
- Firepower Management Center(FMC)- 7.2
- セキュリティサービスエクスチェンジ(SSX)
- Cisco XDR
- スマートライセンスポータル
- Cisco Defense Orchestrator
- セキュリティクラウド制御

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。

設定

ライセンス

仮想アカウントロール:

スマートアカウントをSSXアカウントにリンクする権限を持つのは、仮想アカウント管理者また はスマートアカウント管理者のみです。

ステップ1:スマートアカウントのロールを検証するには、software.cisco.comに移動し、 Administration Menuの下で、Manage Smart Accountを選択します。

db BIGEDU ¥



ステップ 2:ユーザロールを検証するには、Usersに移動し、図に示すように、Rolesの下でアカ ウントにVirtual Account Administratorが設定されていることを検証します。

| Cisco Softw | Cisco Software Central > Manage Smart Account > Users | | | | | | | | | | |
|-------------|---|--------------------|---------------------|-------------------------------------|--|------------|----------|--|--|--|--|
| Account Pro | Account Properties Virtual Accounts Users Custom Tags Requests Account Agreements Event Log | | | | | | | | | | |
| Users | Users User Groups | | | | | | | | | | |
| A | dd Users Remove Selec | Export Selected | Omanization | Account Accord | Pala | User Group | Antione | | | | |
| | danieben | | | × | • | • | Activity | | | | |
| | Daniel Benitez danieben | danieben@cisco.com | Cisco Systems, Inc. | All Virtual Accounts Mex-AMP TAC | Smart Account Administrator Virtual Account Administrator | | Remove | | | | |
| | | | | | | | 1 User | | | | |

ステップ3:セキュリティライセンスを含まないアカウントがSSXでリンクされている場合、 SSXポータルにセキュリティデバイスとイベントが表示されないため、SSXでリンクするために 選択された仮想アカウントにセキュリティデバイスのライセンスが含まれていることを確認しま す。

| mart Software Licensing | | | | | Feedback Support H |
|---|---------------------------|-----------------------|--------|-------------------|-----------------------|
| rts Inventory Convert to Smart Licensing Repo | ts Preferences On-Pre | m Accounts Activity | | | |
| rtual Account: Mex-AMP TAC - | | | | 0 | Minor Hide Alerts |
| General Licenses Product Instances | Event Log | | | | |
| Available Actions + Manage License Ta | License Reserva | ation | | Search by License | By Name By Tag Q |
| License | Billing | Purchased | In Use | Balance Alerts | Actions |
| FPR1010 URL Filtering | Prepaid | 10 | 0 | + 10 | Actions 👻 |
| FPR4110 Threat Defense Malware Protection | Prepaid | 1 | 0 | + 1 | Actions + |
| FPR4110 Threat Defense Threat Protection | Prepaid | 1 | 0 | + 1 | Actions + |
| FPR4110 Threat Defense URL Filtering | Prepaid | 1 | 0 | + 1 | Actions 👻 |
| HyperFlex Data Platform Enterprise Edition Subscrip | tion Prepaid | 2 | 0 | + 2 | Actions 👻 |
| ISE Apex Session Licenses | Prepaid | 1 | 0 | + 1 | Actions + |
| ISE Base Session Licenses | Prepaid | 10 | 0 | + 10 | Actions 👻 |
| ISE Flus License | Prepaid | 10 | 0 | + 10 | Actions 👻 |
| Threat Defense Virtual Malware Protection | Prepaid | 10 | 1 | + 9 | Actions + |
| | | | | | |

ステップ 4:FMCが正しい仮想アカウントに登録されたことを確認するには、System > Licenses > Smart License:の順に移動します。

| Smart License Status | | | Cisco Smart Software Manager | |
|-----------------------------|---|---|------------------------------|--|
| Usage Authorization: | 0 | Authorized (Last Synchronized On Jun 10 2020) | | |
| Product Registration: | 0 | Registered (Last Renewed On Jun 10 2020) | | |
| Assigned Virtual Account: | | Mex-AMP TAC | | |
| Export-Controlled Features: | | Enabled | | |
| Cisco Success Network: | | Enabled 🕕 | | |
| Cisco Support Diagnostics: | | Disabled () | | |

Smart Licenses

| License Type/Device Name | License Status |
|---|----------------|
| > 🔑 Firepower Management Center Virtual (1) | 0 |
| > 🔑 Base (1) | 0 |
| > 🟳 Malware (1) | 0 |
| > 🖓 Threat (1) | 0 |
| > 🟳 URL Filtering (1) | 0 |
| > 🖓 AnyConnect Apex (1) | 0 |
| > 🖓 AnyConnect Plus (1) | ٥ |
| AnyConnect VPN Only (0) | |

Note: Container Instances of same blade share feature licenses

アカウントをSSXにリンクし、デバイスを登録します。

ステップ1:SSXアカウントにログインするときは、スマートアカウントをSSXアカウントにリ ンクする必要があります。そのためには、ツールアイコンをクリックして、Link Smart/Virtual Accountsを選択します。



アカウントがリンクされると、スマートアカウントとその上のすべての仮想アカウントが表示されます。

方法1(半分の統合):調査の充実

SSXへのデバイスの登録

ステップ1:ご使用の環境で次のURLが許可されていることを確認してください。

米国地域

- · api-sse.cisco.com
- mx*.sse.itd.cisco.com
- dex.sse.itd.cisco.com
- eventing-ingest.sse.itd.cisco.com
- registration.us.ss e.itd.cisco.com
- · defenseorchestrator.com
- edge.us.cd o.cisco.com

EU地域

- api.eu.ss e.itd.cisco.com
- mx*.eu.sse.itd.cisco.com
- dex.eu.ss e.itd.cisco.com
- eventing-ingest.eu.ss e.itd.cisco.com
- registration.eu.ss e.itd.cisco.com
- defenseorchestrator.eu(米国)
- edge.eu.cd o.cisco.com

APJC地域

- · api.apj.sse.itd.cisco.com
- mx*.apj.sse.itd.cisco.com
- dex.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com
- registration.apj.sse.itd.cisco.com
- · apj.cdo.cisco.com
- edge.apj.cdo.cisco.com

オーストラリア地域:

- api.aus.sse.itd.cisco.com
- mx*.aus.sse.itd.cisco.com
- dex.au.ss e.itd.cisco.com
- eventing-ingest.aus.sse.itd.cisco.com
- registration.au.ss e.itd.cisco.com
- aus.cdo.cisco.com

インド地域:

- api.in.ss e.itd.cisco.com
- mx*.in.sse.itd.cisco.com
- dex.in.ss e.itd.cisco.com
- eventing-ingest.in.ss e.itd.cisco.com
- registration.in.ss e.itd.cisco.com

• in.cdo.cisco.com

ステップ 2:次のURL <u>https://admin.sse.itd.cisco.com</u>を使用してSSXポータルにログインし、 Cloud Servicesに移動して、図に示すようにCisco Cisco XDRとEventingの両方のオプションを有 効にします。

| Cloud Services for XDR BETA - TAC O | rg | |
|-------------------------------------|--|--------------|
| | Clsco XDR Cisco XDR enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response. | () ‡ |
| | Eventing Eventing allows you to collect and view events in the cloud. | • |

ステップ3:SSXに登録されているデバイスが表示されることを確認できます。



イベントはセキュアファイアウォールデバイスによって送信されます。次の図に示すように、 SSXポータルでイベントに移動し、デバイスからSSXに送信されたイベントを確認します。

| alialia cisco | Sec | urity Services | Exchange | Devices Cloud Serv | vices Events Audit Log | | | | | 0 % | |
|------------------|-------------------------------------|-------------------|----------|--------------------|-------------------------|-------------------------|---------|----------|---------------------|-----------|--|
| Even | Event Stream for Sourcefire Support | | | | | | | | | | |
| T O R | ▼ [Q. Enter filter criteria | | | | | | | | | | |
| | | Talos Disposition | Incident | Destination IP | Event Time | Ingest Time | Message | Protocol | Reporting Device ID | Source IP | |
| | | Neutral | ° No | .252 | 2020-08-05 18:48:50 UTC | 2020-08-05 18:48:51 UTC | | tcp | 09d441eedce5 | 100 | |
| | | Neutral | ° No | .145 | 2020-08-05 18:47:38 UTC | 2020-08-05 18:47:38 UTC | | tcp | 09d441eedce5 | 100 | |
| | | Unknown | ° No | 100 | 2020-08-05 18:47:30 UTC | 2020-08-05 18:47:30 UTC | | tcp | 09d441eedce5 | 100 | |
| | | | ° No | .252 | 2020-08-05 18:46:50 UTC | 2020-08-05 18:46:50 UTC | | tcp | 09d441eedce5 | .100 | |

セキュリティクラウド制御(SCC/CDO)へのデバイスの登録

ステップ 1 : 使用している環境で次の<u>URL</u>が許可されていることを確認します 米国の地域 :

- · defenseorchestrator.com
- edge.us.cd o.cisco.com

EU地域

- defenseorchestrator.eu(米国)
- edge.eu.cd o.cisco.com

APJC地域

- · apjc.cdo.cisco.com
- edge.apjc.cdo.cisco.com

オーストラリア地域:

- aus.cdo.cisco.com
- インド地域:
 - in.cdo.cisco.com

ステップ 2:<u>Security Cloud Control</u>に移動します(リンクは地域によって異なります)。これに より、Security Cloud Control組織を選択できます。

| vilualio cisco Se | ecurity Cloud Control | | |
|----------------------|---------------------------------|------------------------------|---|
| \equiv | | Select an organization | × |
| An | ganization - North nerica | Q Search for an organization | |
| A Ho | me | d mieber - North America | ~ |

ステップ3:適切な組織を選択したら、Products > Firewallに移動し、デバイスがすでに存在する かどうかを確認します。存在しない場合は、Security Cloud Control(Cisco Defense Orchestrator)にオンボーディングできます。そのためには、Overall InventoryでView all Devicesをクリックします。

|--|

Firewall Management Center Cisco Secure Firewall Management Center <u>___</u>

Auto discover from Cisco Security Cloud

Auto discover and auto onboard On-Prem FMCs integrated with Cisco Security Cloud Use Credentials

Onboarding a device using an IP address or host name and a username and password (Version 6.4+)

ステップ 4: Administration > Firewall Management Centerに移動すると、SCCに統合されている FMCのリストが表示されます。Firewall Management Centerが表示されていない場合は、プラス (+)アイコンをクリックします。

ステップ 4.1:通常、セキュアファイアウォール(HTTPS)は自動的にオンボーディングされます 。オンボーディングしない場合は、オンボーディングするデバイス(FTD)と希望するオンボーデ ィング方法を選択します。

ステップ 4.2: Security Devicesセクションでプラス記号のアイコンをクリックし、Onboard Secure Firewall Deviceを選択し、必要な項目を選択します

| Y Devices Templates Q Search All FTD FTD FTD FTD | by Device Name, IP Address, or Serial Numb | er Displaying 4 of | 4 results | | C () + |
|--|--|---|--|---|---|
| Onboard FTD Device | Follow the steps below | ▲ Important: After you onboard th provisioning method, the device will manager will no longer manage the | e threat defense device to cdFMC or the I be managed by the corresponding mana device, and all existing policy configurati | Firewall Management Center using the ager it is onboarded to. Note that the fire ions on the device will be lost except for | Cancel zero-touch ewall device the basic interface |
| | Firewall Threat Defense | Configurations. Therefore, you must Construct the second | t configure the policies from the correspo Use Serial Number Onboard a factory-shipped FTD 7.2+ device to dFMC or to a 7.4+ On- Prem FMC using zero-touch provisioning. | Deploy an FTD to a cloud environment Deploy a device to supported cloud platforms: AWS, GCP, and Azure. | |
| | | Bulk Onboard using CSV File Use this method for adding multiple devices by uploading a .csv file, with template assignment. (FTD 7.4+) | | | |

ステップ 5: Security Cloud Controlでデバイスをオンボーディングすると、インベントリでデバ イスを可視化できます。

手順6:CDO組織がSSX組織にリンクされていることを確認します。そのためには、Security

Services Exchangeに移動し、[ツール]メニューアイコンをクリックして、[CDOアカウントのリンク]をクリックします。

| CISCO Security Services Exchange | Devices Cloud Services | Events | Audit Log | 🛛 🛠 🐥 Uriel | I Mc |
|----------------------------------|------------------------|--------|-----------|-------------------------------|------|
| | | | | Link Smart/Virtual Accounts | |
| Devices for XDR BETA - TAC Org | | | | Unlink Smart/Virtual Accounts | |
| ▼ Q Device Name / ID | | | | Link CDO Account Downloads | |

セキュアファイアウォールの統合

7.2.xから7.4.xへのCisco XDR

ステップ1: Secure Firewall Management Centerで、Integration > SecureXの順に移動します。



ステップ2:右側の領域を選択し、Enable SecureXをクリックします。

| Firewall Management Cente | Overview | Analysis | Policies | Devices | Objects | Integration |
|---|---|----------------------------------|-----------------------------------|----------------------------------|------------------------------------|------------------------------|
| SecureX Integration | | | | | | |
| SecureX Setup This feature allows Secure Firewall Man | nagement Center to in | tegrate with ot | her SecureX s | ervices via Se | cureX ribbon. I | Learn more 🖸 |
| 1 Cloud Region | This setting deter well as data gene tools. | mines where e erated by the C | events are sent isco Success I | to, if configur Network and C | ed to send to t Cisco Support I | the cloud, as Diagnostics |
| | Current Region | us-east-1 (l | JS Region) | | ~ | |
| 2 SecureX Enablement | After completing each page. Learn | this configurati more ː | on, the Secure | X ribbon will | show up at the | bottom of |
| | Enable Secure | X C | | | | |

ステップ3:Enable SecureXをクリックすると、Cisco Defense Orchestrator Authenticationページ (Security Cloud Sign Onを利用)にリダイレクトされます。次に、Continue to Cisco SSOをク リックします。



Welcome to the Cisco Security Cloud

Delivered through Security Cloud Control (SCC)

| | Openboard | | | | Dataseta Ing |
|----|--|--------|--|---|--|
| π. | Top insights it alories in concern | | | | |
| | Sophast Recoglic discrete Manuscrit 200 | 1.0 | by more presenting orbitaged area | A subserve | alad haffa havanis internat - 175 |
| 8 | Fulfic has clean association in the accession of more large frequency or provided and accessible accessibility responsibility in and participance basis. | 1100 C | e 1958 a lad avante eig spint an ni prim var actuative for the care | College to observe the second | e a significant parties of facility power of 15. generating contracting methods in proc. strength with ranks to 7 meth |
| | 1410. bet | 1.00 | - | 1.001 | - |
| 4 | Top actions | | Sprinto market | | |
| | Indep Analysis and Sphinister | | Workshad pretarrise status | | tantinas - 1 |
| 1 | 20524 | | 400k 20k | 320k | 60k |
| | All and All an | | Beneration A Brown | - | 12 November 8 |
| • | ADh bight samery is the | | | | |
| | The same O first first into ingenitial | | Tax hits destinations | | Language - T |

Staying on top of security is easier than ever. Security Cloud Control helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

SCC complements FMC by allowing you to:

- Drive consistent policy through shared object management with FMCs
- · Enable Zero-Touch Provisioning of FTDs
- · View events in the cloud
- Get a centralized view of inventory across FMCs
- · Leverage cloud CSDAC and Cloud Delivered FMC
- and more

To continue with cloud registration of your FMC, you will need a Cisco Security Cloud Sign On (SSO) user account.

If you don't already have a Cisco SSO account, please proceed below and Sign Up for free. Note that you will need to restart the cloud registration from your FMC after your new SSO account is created.

If you already have a Cisco SSO account, please proceed below to choose or create a free SCC account to register your FMC.





Cisco XDRを使用する7.6.x以降

ステップ 1: Secure Firewall Management Centerで、Integration > Cisco Security Cloudの 順に移動します。

Integration

| Dynamic Attributes Connector New | Intelligence |
|----------------------------------|--------------|
| Cisco Security Cloud | Incidents |
| Security Analytics & Logging | Sources |
| Other Integrations | Elements |
| | Settings |
| | |

AMP

AMP Management

Dynamic Analysis Connections

ステップ 2:適切なリージョンを選択して、Enable Cisco Security Cloudをクリックします。 。 ステップ3:Enable Cisco Security Cloudをクリックすると、Cisco Defense Orchestrator

ステック3:Enable Cisco Security Cloudをクリックすると、Cisco Defense Orchestrator Authenticationページ(セキュリティクラウドサインオンを使用)にリダイレクトされます 。次に、Continue to Cisco SSOをクリックします。

ステップ4:既存のセキュリティクラウド制御テナントを選択するか、新しいテナントを作成できます。

ステップ 5:適切なテナントを選択し、このページで受信するコードがFMCで受信するコードと 一致することを確認します。一致する場合は、[FMCの承認]をクリックします。

Grant Application Access × Please verify the code provided by SecureX. 9C1FEC52

Grant Application Access

Compare the code below to the authorization code shown in the FMC tab. If the codes match, authorize the FMC to complete the registration. If the codes do not match, cancel registration.

9C1FEC52

FMC would like access to your SCC tenant danieben.

- Users: All internal users in FMC will have read-only access to this SCC tenant.
- Data: FMC will be able to collect data using SCC APIs.

The FMC will be registered with tenant danieben



手順 6: Security Cloudサインオンクレデンシャルを入力して統合を承認します。完了すると、 FMCがCisco Security Cloudへの登録を承認されたことを示す確認が表示されます。

ılıılı. cısco

Welcome to Security Cloud Control

You have successfully authorized your FMC to register with Cisco Security Cloud, you may now close this tab.

手順7:認可が完了したら、FMCに戻り、クラウドに送信するイベントを選択し、完了したら Saveをクリックします。

ステップ 8:SecureXオーケストレーションの有効化(XDR自動化)を選択できます。



Save

ステップ 9:XDR > Administration > On Premises Applianceの順に移動して、アプライアンスを 検索します。これらは自動的に登録されている必要があります。

ステップ 10:XDR > Administration > Integrationsの順に選択し、Secure Firewall Integrationをイ ネーブルにします。

| Secure Firewall | |
|---|--|
| the Cisco Managed | |
| Secure Firewall (formerly Firepower) provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. | |
| Free Trial Get Started | |

ステップ 10.1:統合に名前を割り当て、+Addをクリックします。

| Secure Firewall CDO Integra | tion | | | |
|-----------------------------|-----------|------------|---------------------------------------|--------------------|
| | | | Manage On-Premises Appliances | for New Appliances |
| Name | Version | Status | Description | IP Address |
| | 7.2.5-208 | Registered | JMX2716X2M1 | 10. 242253 |
| MexAmp-FTD | 7.2.0 | Registered | 10. MexAmp-FTD (FMC managed) | 10. 24225 |
| mexMEX-AMP-FMCmex | 7.2.0.1 | Registered | 10. mexMEX-AMP-FMCmex | 10.4 242.24 |
| | | | Rows per page $\boxed{30 \lor}$ 1-3 c | of 3 < 1 > |

この統合により、XDR内の調査を充実させることができます。

方法2(完全統合):XDRのインシデントを強化する

◆ 注:Secure Firewall、XDR、Cisco Defense Orchestrator(CDO)、Security Services Exchange(SSX)、およびSecurity Analytics and Logging(SAL)の間のシームレスな統合を保 証するには、手動マッピングが必要です。このプロセスでは、Cisco TACに連絡して、必要 な設定とマッピングを実行します。

ステップ 1: Cisco XDRにイベントを転送するには、CDOアカウントにSecurity Analytics and Loggingライセンスが必要です。

ステップ2:アプライアンスをSSXおよびSecurity Cloud Controlに登録するには、前述の手順を 使用してください。

ステップ 3:完了したら、これらの詳細をTACに連絡し、Security Cloud Control/SALをXDR Analyticsにリンクするようリクエストしてください。

- ・ CDOテナントID
- CDO名
- XDR組織ID
- ・ SSXテナントID
- SSX名
- SCA組織ID

ステップ 4: CDOアカウントがXDR Analyticsポータルにリンクされていることを確認します。

CDOポータルをXDR Analyticsにリンクする前は、次のようになります。



リンクが完了すると、XDR分析ポータルに移動するオプションが表示されます。

diala SCC



ステップ 5:XDR AnalyticsアカウントをSecurity Cloud Control Portal(CDO)にリンクしたら、 XDR AnalyticsがXDRと統合されていることを確認する必要があります。そのためには、XDR AnalyticsでSettings > Integrations > XDRの順に移動し、XDR Integrationが緑色のチェックマーク になっており、統合モジュールが正しいXDR組織を指していることを確認します。

| Status: Enabled | |
|---|-----------|
| | |
| The integration module for XDR BETA - TAC Org Cisco XDR organization has been active since 2 de mayo de 2023, 10:37 a GMT-6. | 0:37 a.m. |

確認

XDR

セキュアファイアウォールがイベント(マルウェアまたは侵入)を生成することを検証します。 侵入イベントについては、次の場所に移動します。 解析>ファイル>Malware Eventsで、侵入イベ ントの場合は、Analysis > Intrusion > Eventsに移動します。

「SSXへのデバイスの登録」セクションのステップ4で説明されているように、イベントがSSXポータルに登録されていることを検証します。.

Cisco XDRダッシュボードに情報が表示されていることを確認するか、APIログを確認して、 API障害の原因を特定します。

すべてのテナントが正しくリンクされていることを確認します。問題がある場合は、TACケース をオープンし、次の詳細情報を提供します。

- ・ CDOテナントID
- ・ CDO名
- XDR組織ID
- ・ SSXテナントID
- SSX名
- SCA組織ID

トラブルシュート

接続の問題の検出

action_queue.logファイルから一般的な接続問題を検出できます。障害が発生した場合は、次のようなログがファイルに存在することを確認できます。

ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeo

この場合、終了コード28は操作がタイムアウトになったことを意味し、インターネットへの接続 を確認する必要があります。また、終了コード6も表示される必要があります。これは、DNS解 決の問題を意味します

DNS解決による接続の問題

ステップ1:接続が正常に動作していることを確認します。

root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'

次の出力は、デバイスがURL <u>https://api-sse.cisco.com</u>を解決できないことを示しています。この 場合、適切なDNSサーバが設定されていることを検証する必要があります。このサーバは、エキ スパートCLIからnslookupを使用して検証できます。

root@ftd01:~# nslookup api-sse.cisco.com
;; connection timed out; no servers could be reached

次の出力は、設定されたDNSに到達していないことを示しています。DNS設定を確認するには、 show networkコマンドを使用します。

| > show network | |
|--------------------|---------------------------|
| ========[System | Information]============ |
| Hostname | : ftd01 |
| DNS Servers | : x.x.x.10 |
| Management port | : 8305 |
| IPv4 Default route | |
| Gateway | : x.x.x.1 |
| | |
| ======[| eth0]====== |
| State | : Enabled |
| Link | : Up |
| Channels | : Management & Events |
| Mode | : Non-Autonegotiation |
| MDI/MDIX | : Auto/MDIX |
| MTU | : 1500 |
| MAC Address | : x:x:x:x:9D:A5 |
| [| IPv4] |
| Configuration | : Manual |

| Address | : x.x.x.27 |
|------------------|--------------------------------|
| Netmask | : 255.255.255.0 |
| Broadcast | : x.x.x.255 |
| | [IPv6] |
| Configuration | : Disabled |
| =========[Proxy | Information]================= |
| State | : Disabled |
| Authentication | : Disabled |

この例では、誤ったDNSサーバが使用されています。次のコマンドでDNS設定を変更できます。

> configure network dns x.x.x.11

この接続を再度テストし、今度は接続が成功します。

root@ftd01:~# curl -v -k https://api-sse.cisco.com * Rebuilt URL to: https://api-sse.cisco.com/ * Trying x.x.x.66... * Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0) * ALPN, offering http/1.1 * Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH * successfully set certificate verify locations: * CAfile: none CApath: /etc/ssl/certs * TLSv1.2 (OUT), TLS header, Certificate Status (22): * TLSv1.2 (OUT), TLS handshake, Client hello (1): * TLSv1.2 (IN), TLS handshake, Server hello (2): * TLSv1.2 (IN), TLS handshake, Certificate (11): * TLSv1.2 (IN), TLS handshake, Server key exchange (12): * TLSv1.2 (IN), TLS handshake, Request CERT (13): * TLSv1.2 (IN), TLS handshake, Server finished (14): * TLSv1.2 (OUT), TLS handshake, Certificate (11): * TLSv1.2 (OUT), TLS handshake, Client key exchange (16): * TLSv1.2 (OUT), TLS change cipher, Client hello (1): * TLSv1.2 (OUT), TLS handshake, Finished (20): * TLSv1.2 (IN), TLS change cipher, Client hello (1): * TLSv1.2 (IN), TLS handshake, Finished (20): * SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256 * ALPN, server accepted to use http/1.1 * Server certificate: * subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com * start date: 2019-12-03 20:57:56 GMT * expire date: 2021-12-03 21:07:00 GMT * issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2 * SSL certificate verify result: self signed certificate in certificate c hain (19), continuing anyway. > GET / HTTP/1.1 > Host: api-sse.cisco.com > User-Agent: curl/7.44.0 > Accept: */* > < HTTP/1.1 403 Forbidden < Date: Wed, 08 Apr 2020 01:27:55 GMT

- < Content-Type: text/plain; charset=utf-8
- < Content-Length: 9
- < Connection: keep-alive
- < Keep-Alive: timeout=5
- < ETag: "5e17b3f8-9"
- < Cache-Control: no-store
- < Pragma: no-cache
- < Content-Security-Policy: default-src 'self'
- < X-Content-Type-Options: nosniff
- < X-XSS-Protection: 1; mode=block
- < Strict-Transport-Security: max-age=31536000; includeSubdomains;

SSXポータルへの登録に関する問題

FMCとSecure Firewallの両方とも、管理インターフェイスでSSX URLへの接続が必要です。接続 をテストするには、Firepower CLIでルートアクセスで次のコマンドを入力します。

<#root>

curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert /ngfw/etc/

curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

次のコマンドを使用すると、証明書チェックをバイパスできます。

root@ftd01:~# curl -v -k https://api-sse.cisco.com * Rebuilt URL to: https://api-sse.cisco.com/ * Trying x.x.x.66... * Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0) * ALPN, offering http/1.1 * Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH * successfully set certificate verify locations: * CAfile: none CApath: /etc/ssl/certs * TLSv1.2 (OUT), TLS header, Certificate Status (22): * TLSv1.2 (OUT), TLS handshake, Client hello (1): * TLSv1.2 (IN), TLS handshake, Server hello (2): * TLSv1.2 (IN), TLS handshake, Certificate (11): * TLSv1.2 (IN), TLS handshake, Server key exchange (12): * TLSv1.2 (IN), TLS handshake, Request CERT (13): * TLSv1.2 (IN), TLS handshake, Server finished (14): * TLSv1.2 (OUT), TLS handshake, Certificate (11):

```
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

✤ 注:テストから送信されたパラメータはSSXで想定されるものではないため、「403 Forbidden」というメッセージが表示されますが、これは接続を検証するために十分である ことを証明しています。

SSEConnectorの状態の確認

次に示すように、コネクタのプロパティを確認できます。

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

SSConnectorとEventHandlerの間の接続を確認するには、次のコマンドを使用できます。接続が 正しくない場合の例を次に示します。 確立された接続の例では、ストリームステータスがconnectedであることが確認できます。

root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock unix 2 [ACC] STREAM LISTENING 382276 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.soc unix 3 [] STREAM CONNECTED 378537 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.soc

SSXポータルとCTRに送信されたデータの確認

イベントをSecure FirewallデバイスからSSXに送信するには、<u>https://eventing-</u> <u>ingest.sse.itd.cisco.com</u>との間でTCP接続が確立される必要があります。次の例は、SSXポータル とSecure Firewallとの間で確立されない接続を示しています。

root@firepower:/ngfw/var/log/connector# lsof -i | grep conn connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN) connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-234.compute-1.a

connector.logログで、次の操作を行います。

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:co
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
```

◆ 注:表示されるx.x.x.246および1x.x.x.246のIPアドレスは<u>https://eventing-ingest.sse.itd.cisco.com</u>に属していることが変更される必要があることに注意してください。これが、IPアドレスの代わりにURLに基づいてSSXポータルへのトラフィックを許可することが推奨される理由です。

この接続が確立されない場合、イベントはSSXポータルに送信されません。次に、セキュアファ イアウォールとSSXポータルの間に確立された接続の例を示します。

| root@firep | ower:# | lsof - | ∙i∣g | rep conn | | |
|------------|--------|--------|------|---------------|-----|--|
| connector | 13277 | www | 10u | IPv4 26077573 | 0t0 | TCP localhost:8989 (LISTEN) |
| connector | 13277 | www | 19u | IP∨4 26077679 | 0t0 | TCP x.x.x.200:56495->ec2-35-172-147-246.compute-1. |

デバイス(FTD)をSecurity Cloud Controlに登録できない

デバイスをSecurity Cloud Controlに登録できない場合は、適切なCDOテナントへの接続があることを確認します。

正しいURLを確認するには、Administration > Firewall Management Centerに移動し、Cloud Delivered FMCを選択します。画面の右上にホスト名が表示されます。

admin@MexAmpFTD:~\$ nc -vz xxxxxx.app.us.cdo.cisco.com 443 Connection to xxxxxxx.app.us.cdo.cisco.com 443 port [tcp/https] succeeded!

それでもCDOへの接続の問題が発生する場合は、ポート8305が開いていることを確認します。こ れは接続問題の例です。

admin@AMP-DMZ-FPR:~\$ sudo tail /ngfw/var/log/messages

| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | sttunneld:st_peer | rs LINF(| D] Peer xxxxxxxx.app.us.cdo.ci |
|-----|----|----------|-------------|----------------|--------|-----------------------------|----------|--------------------------------|
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Connect to xxxxxxxx.app.us.cd |
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Initiate connection using res |
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Initiate IPv6 type connection |
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Initiate IPv4 type connection |
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Initiate IPv4 connection from |
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Initiating IPv4 connection to |
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Wait to connect to 8305 (IPv4 |
| Jan | 25 | 18:48:56 | AMP-DMZ-FPR | SF-IMS[20448]: | [1465] | <pre>sftunneld:sf_ssl</pre> | [INFO] | Connect to x.x.x.51 failed on |
| | | | | | | | | |

デバイスが誤ったSSXテナントに登録されている

FMCが登録されているSSXテナントを確認できます。

admin@fmc01:~\$ curl localhost:8989/v1/contexts/default/tenant

{"registeredTenantInfo":{"companyId":"689xxxxx-eaxx-5bxx-b1xx-a7662axxxxx","companyName":"XDR BETA - TA

SSXテナントが正しくない場合、アプライアンスをSSXに登録する手順を再実行する必要があり ます

SSXテナントが正しいにも関わらず、CDOテナントが適切なSSX組織にリンクされていない場合 は、次の情報をTACに連絡してください。

- ・SSXテナントID
- ・CDOテナントID

関連情報

- <u>Cisco Secure Firewall Threat DefenseおよびCisco XDR統合ガイド</u>
- シスコのテクニカルサポートとダウンロード

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。