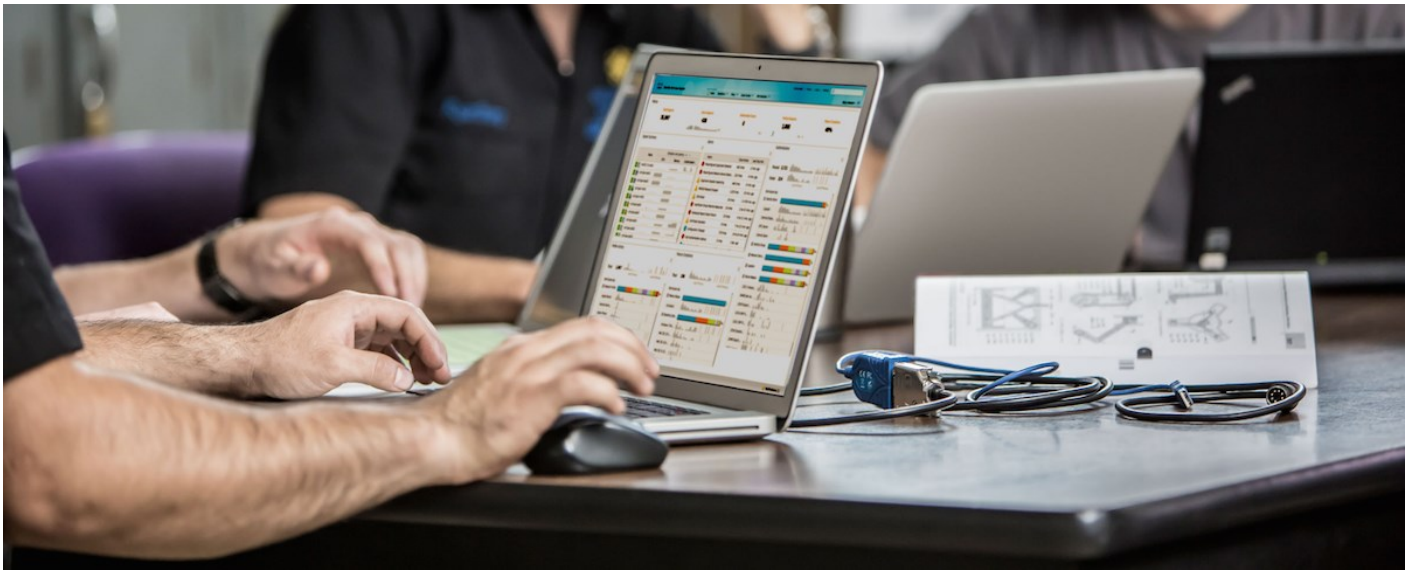


pxGrid を使用した ISE および TrustSec と Cisco Firepower Management Center 6.0 の統合方法

目次

このドキュメントについて **4**

ソリューションの概要：pxGrid を使用した ISE および TrustSec と Cisco Firepower Management Center 6.0 ..... **5**

Cisco Firepower Management Center 6.0 5

Cisco TrustSec 6

Cisco Identity Services Engine（ISE） 6

Cisco pxGrid 6

技術概要 **7**

Cisco Identity Service Engine ダイナミック セキュリティ グループ タグ **9**

自己署名証明書の操作 **10**

ISE 2.0 の設定 10

Firepower ISE レルムの作成 11

Firepower Management Center 6.0 の設定 13

Firepower ISE ID ソースの設定 20

CA（認証局）- 署名付き証明書の操作 **22**

CA 署名操作用にカスタマイズされた pxGrid テンプレート 22

ISE 2.0 の設定 26

Firepower ISE レルムの作成 33

Firepower Management Center 6.0 の設定 35

ISE ID ソース CA 署名付き証明書の設定 38

Firepower Management Center **40**

ネットワーク検出の有効化 40

ISE ID ポリシー 40

デフォルトのアクセス制御ポリシー 41

ISE ID ポリシーの追加 41

トランスポート層とネットワーク層のプリプロセッサの設定 42

ブロック応答ページの追加 43

Employee SGT タグ アクセス制御ルールの作成 44

Firepower pxGrid 侵入ポリシー 46

Firepower 仮想センサーによる Employee SGT ユーザのテスト 52
ASA with Firepower サービス 58
集中型 Firepower Management Center ポリシーの使用 58
ASA Firepower（sfr）のインストールと Firepower Management Center への登録 58
管理対象 Firepower Management ポリシーからの Employee SGT ユーザのテスト 60
オンボックス Firepower ポリシー管理 62
Firepower Management Center 6.0 から ASA を削除 62
ISE レルム設定 62
ISE ID ソースの設定 64
ISE ID ポリシー 65
ISE ID ポリシーの追加 66
トランスポート層とネットワーク層のプリプロセッサの設定 67
ブロック応答ページの追加 67
ASA 作成の Employee SGT タグのアクセス制御ルール 67
ASA Firepower pxGrid 侵入ポリシー 70
オンボックス Firepower Management ポリシーを使用した Employee SGT ユーザのテスト 73
トラブルシューティング 79
ISE pxGrid ノード 79
pxGrid 公開ノードが表示されず、pxGrid 接続がない 79
Firepower Management Center 6.0 79
システム統合 ISE 証明書テストが失敗する 79
ISE から相関イベントが見えない 79
ASA with Firepower サービス 80
Firepower Management Center に登録済みの ASA デバイスパラメータを変更できない 80
SFR が回復状態のまま変わらない 80
ASA Firepower レポートにトラフィックが表示されない 80
不具合の解決 83
pxGrid & Identity マッピング サービスが再起動する 83
アクティブな pxGrid ノードが GUI に反映されない。CLI には反映される 83
参考資料 84

このドキュメントについて

このドキュメントは、pxGrid（platform exchange Grid）を使用した、Cisco Identity Service Engine（ISE 1.3 以降）と Cisco Firepower Management Center（FMC）6.0 の導入に関心のあるシスコ エンジニアとお客様を対象としています。

pxGrid 修復モジュールは Cisco Firepower Management Center FMC 6.0 ではサポートされないことに注意してください。

Cisco Firepower Management Center（FMC）6.0 は、pxGrid 経由で利用可能な ISE セッション属性情報に基づいて組織のセキュリティ ポリシーを実行できるようになりました。これらのセキュリティ ポリシーは、Cisco Firepower により、管理対象の NGIPS センサーや ASA with Firepower サービスに対して適用および実行することができます。ASA with Firepower サービスには、ASDM を介してこれらのポリシーをローカルで管理するオプションもあります。

このドキュメントでは、自己署名証明書または認証局（CA）署名付き証明書を使用する ISE スタンドアロン環境での Cisco Firepower Management Center（FMC）6.0 の設定および ISE と pxGrid の統合の設定について詳細に説明します。ISE の実稼働環境に pxGrid を導入する場合は、http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf を参照してください。

このドキュメントでは、ASA Firepower（sfr）モジュールを使用して ASA with Firepower サービスを設定し、Cisco Firepower Management Center（FMC）6.0 に登録して、集中管理された Cisco Firepower Management Center ポリシーを使用します。また、ASA with Firepower サービスは、FMC とは独立した Firepower 侵入ポリシーとアクセス制御ルールを使用してオンボックスで設定されます。

Cisco Firepower Management Center 管理対象セキュリティ ポリシーと ASA オンボックス Firepower Management ポリシーは、特定の Web カテゴリへのアクセスを拒否するための侵入ポリシーと Employee SGT アクセス制御ルールで構成されます。

このドキュメントの読者は、ISE、Cisco Firepower Management Center、pxGrid にある程度精通していることが必要です。

ソリューションの概要：pxGrid を使用した ISE および TrustSec と Cisco Firepower Management Center 6.0

Cisco Firepower Management Center（FMC）6.0 は、侵入ポリシーとアクセス制御ルールを NGIPS センサーおよび ASA with Firepower サービスに適用することによって、組織のセキュリティ ポリシーを集中管理し、実行します。

FMC 6.0 では、ネットワーク検出を使用してユーザ ID 情報を取得します。また、ユーザに関するきめ細かな詳細情報の取得には、SFUA（Sourcefire ユーザ エージェント）が使用されます。SFUA は、ユーザ-IP マッピングを取得するために使用されます。一度に使用できるのは、SFUA または ISE のいずれかです。

エンドユーザは AD または LDAP レルムで認証され、ユーザ グループ情報に基づいて、組織のセキュリティ ポリシーを含むデフォルトのポリシーが Cisco Firepower NGIPS センサーまたは ASA with Firepower サービスに適用されます。このセキュリティ ポリシーには侵入ポリシーを含めることができ、ユーザ グループ固有のアクセス制御ルールとともに、プリセット レベルのバランスのとれたセキュリティを実現可能です。

Cisco pxGrid（platform exchange Grid）は、セキュリティ グループ タグ（SGT）、エンドポイント プロファイル デバイス情報、Cisco Firepower Management 6.0 アクセス制御ポリシー ルールで使用されるロケーション IP など、追加の ISE 属性を提供します。

SGT（セキュリティ グループ タグ）は、ISE で定義された、TrustSec のコンポーネントの 1 つで、ID アクセスに関する組織のセキュリティ ポリシーに基づいて認可ポリシーとして ISE に導入されます。たとえば、会社推奨デバイスを使用するすべての有線ユーザは、ISE 経由の認証が成功すると、Employee SGT タグが付与されます。会社非推奨デバイスを使用するワイヤレス ユーザは、認証が成功すると、Non-Employee SGT タグが付与されます。これらのユーザは、Firepower Management Center ISE レルムに存在している必要があります。

FMC 6.0 は、これらのセキュリティ グループ タグに基づいて、アクセス制御ルールを適用できます。また、FMC 6.0 には、Firepower Management Center 6.0 ポリシーをコンテキスト認識型にするために、ISE pxGrid 属性を追加することもできます。

Cisco Identity Service Engine（ISE）は、ID ソリューションおよび Cisco pxGrid（platform exchange Grid）フレームワークを提供します。

Cisco Firepower Management Center 6.0

Cisco Firepower Management Center は、Firepower アプライアンス（NGIPS）および Firepower サービスを管理するための Web インターフェイスを備えた中央管理コンソールを提供します。このコンソールは、管理統括、分析、レポートの各タスクの実行に使用されます。自動的に、侵入、ファイル、マルウェア、検出、接続、パフォーマンスの各データを集約して関連付けを行い、特定のホストに対するイベントの影響を評価するほか、侵入の痕跡のあるホストにタグ付けを行います。

Cisco TrustSec

セキュリティ グループ タグ（SGT）は、Cisco TrustSec ソリューションの一部です。SGT は ISE で定義され、入力（ネットワークへの着信）時に適用されます。SGT は、ユーザ、エンドポイントデバイス、ライン オブ ビジネスなどのグループを表すことができます。その場合、SGT は、ネットワーク アクセス ポリシーに適用され、ネットワーク デバイスによって使用されて転送決定が行われ、ネットワーク インフラストラクチャ全体にわたってアクセス制御ポリシーを共有することができます。SGT はセキュリティ グループに割り当てられる一意の 16 ビットのセキュリティ グループ番号です。セキュリティ グループには、意味を示すような名前を割り当てることもできます。

SGT は、組織のセキュリティ ポリシーを定義する条件ルールから構成されている ISE 許可ポリシーの許可プロファイルとして定義され、実装されます。

SGT は、組織のネットワーク全体で同一のグローバルなセキュリティ ポリシーを設定できます。

このドキュメントでは、/users/domain Windows グループに所属するエンドユーザが正常に認証されると、すべて Employee SGT を受け取るように ISE 認可ポリシーが作成されます。この Employee SGT は、ストリーミング メディア、ピアツーピア アプリケーション、ハッキング、マルウェア サイト、ギャンブル カテゴリへのアクセスを拒否するために Cisco Firepower 管理対象アクセス制御ルール ポリシーで使用されます。

Cisco Identity Services Engine（ISE）

Identity Services Engine（ISE）は、セキュリティ ポリシーの管理およびアイデンティティ アクセスの管理を行うプラットフォーム ソリューションです。ISE は、802.1x 認証、ゲスト管理ポリシー、ポスチャ、クライアント プロビジョニング、および TrustSec ポリシーを定義/発行/適用することによって一元管理を実現します。ISE セッション ディレクトリは、pxGrid 経由でコンテキスト認識型ポリシーを含めるためにセキュリティ ソリューションで使用可能な IEEE 802.1x 認証ユーザに関する豊富なコンテキスト情報を提供します。

さらに、ISE は有線、ワイヤレス、および VPN 接続についてのアクセス制御やセキュリティ コンプライアンスを簡略化し、企業のセキュリティ ポリシーに関する取り組みをサポートします。

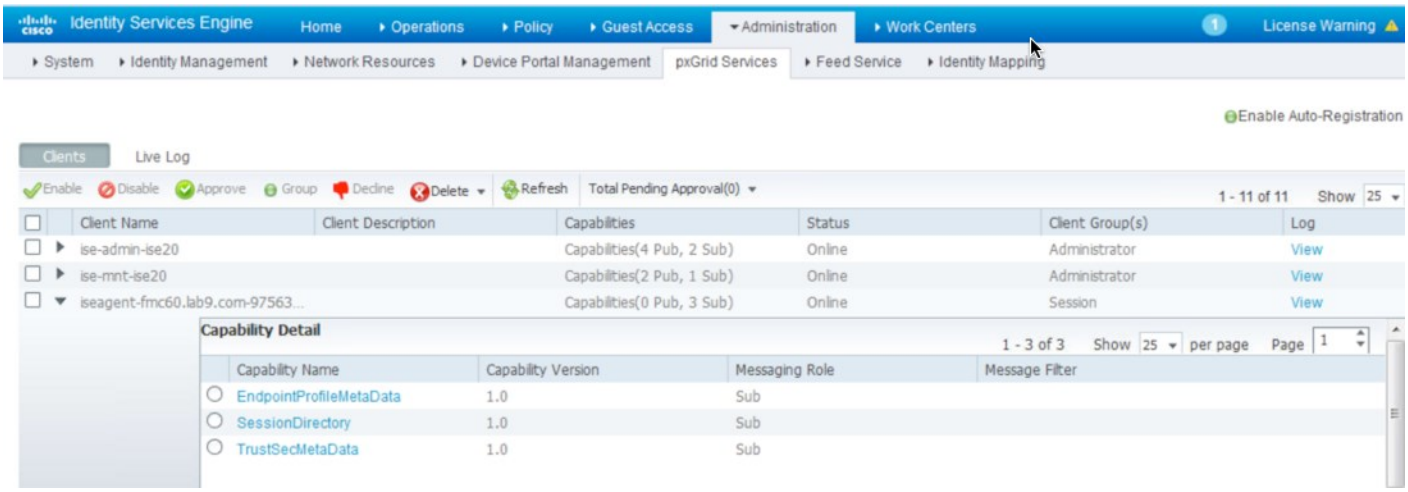
Cisco pxGrid

Cisco pxGrid（platform exchange Grid）は、たとえば、セキュリティ モニタリングと検知システム、ネットワーク ポリシー プラットフォーム、アセットおよび仮想設定管理、ID およびアクセス管理のプラットフォーム、ならびに仮想およびその他の IT 運用プラットフォームなど、IT インフラストラクチャの各部分間でのマルチベンダーのクロス プラットフォーム ネットワーク システムでのコラボレーションを可能にします。

ビジネス上または運用上のニーズが発生した場合、Firepower Management Center 6.0 やエコシステム パートナーなど、シスコのセキュリティ ソリューションでは pxGrid を使用し、公開またはサブスクライブの手法を通じてコンテキスト情報を交換します。

技術概要

Cisco Firepower Management Center 6.0 は、pxGrid クライアントとして ISE pxGrid ノードに登録し、ISE 公開のトピックや機能にサブスクライブして ISE セッション情報を受け取ります。このセッション情報には、Firepower Management Center 6.0 のアクセス制御ロールで使用されるセキュリティ グループ タグ（SGT）、エンドポイント プロファイル デバイス情報、エンドポイント ロケーションが含まれています。



これらのトピックの機能は次のとおりです。

- TrustSecMetadata 情報。セキュリティ グループ タグの番号と説明を公開します。

```
SecurityGroup : id=150138d0-cfc7-11e3-9e0e-000c29e66166, name=Engineering, desc=, tag=3
```

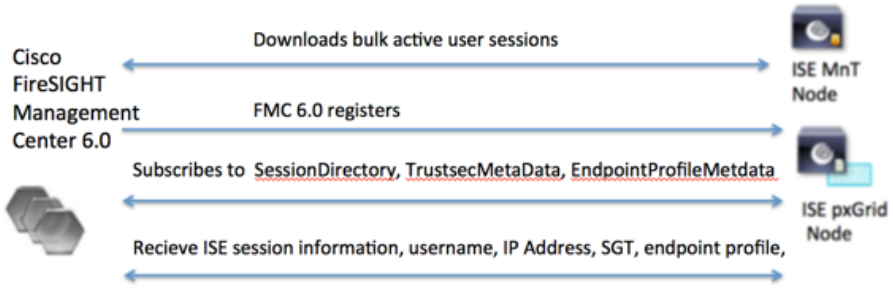
- EndpointProfileMetadata。ISE プロファイリング ポリシーへの変更や修正などの ISE エンドポイント ポリシーを提供します。

```
Endpoint Profile : id=886f7570-bd0c-11e3-a88b-005056bf2f0a, name=Apple-iDevice, fqname Apple-Device:Apple-
iDevice
```

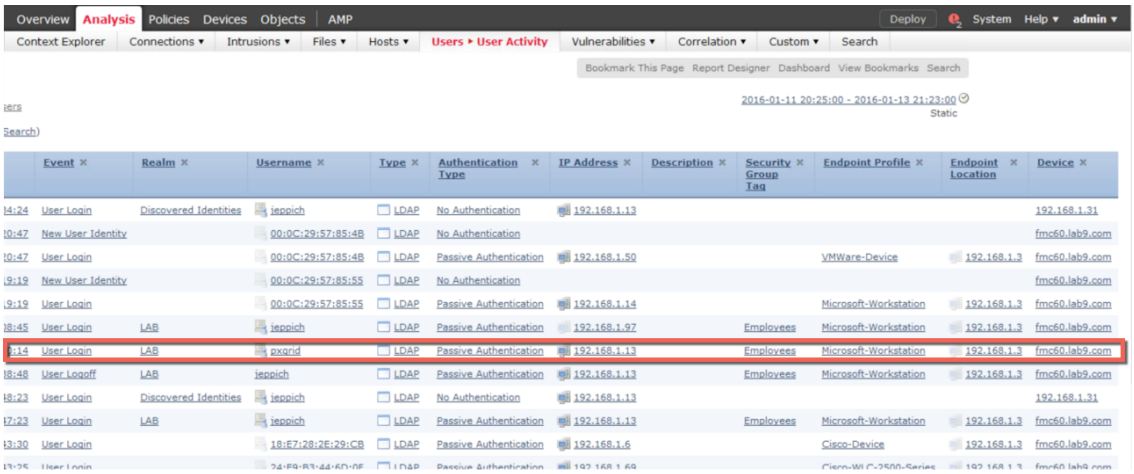
- SessionDirectory。ユーザ名やデバイス情報などの認証された使用セッション属性情報を公開します。

```
session (ip=192.168.1.14, Audit Session Id=0A0301030000001E00FEBAD7, User Name=jsmith, Domain=lab4.com,
Calling station id=00:0C:29:77:A8:C7, Session state= STARTED, Epsstatus=null,Security Group=Engineering,
Endpoint Profile=Microsoft-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/9,
RADIUSAVPairs=[Acct-Session-Id=00000027], Posture Status=null, Posture Timestamp=, Session Last Update
Time=Tue Apr 29 15:11:46 GMT-05:00 2014
```

アクティブ ユーザ セッションの一括ダウンロードは、Cisco Firepower Management Center の起動時や再起動時に実行されます。セッション情報の一括ダウンロードは、ISE RESTful API 経由で ISE MNT ノードからダウンロードされます。このセッション情報には、ユーザ名、IP アドレス、SGT、エンドポイント プロファイルが含まれます。最近認証された ISE ユーザや既存の SGT の変更などの更新が存在する場合、Cisco Firepower Management Center のトピック サブスクリプションにより、これらの変更がリアルタイムで実行されます。



ISE からの ISE セッション情報は、Firepower Management Center のユーザ アクティビティ画面に表示されます。



ISE からの IEEE 802.1x ユーザ認証のユーザ名のみが FMC 6.0 ポリシーに適用可能ですが、Firepower ISE レルムに存在している必要がある点に注意してください。IEEE 802.1x マシン認証のホスト名や MAC アドレスのユーザ名は FMC 6.0 ポリシーに適用できません。

Cisco Identity Service Engine ダイナミック セキュリティ グループ タグ

組織のセキュリティ ポリシーは、セキュリティ グループ タグ（SGT）に基づいて定義することができます。そのため、組織にネットワーク全体に同一のグローバルなセキュリティ ポリシーを設定できます。Cisco TrustSec が組織のスイッチで有効になっている場合は、これらのセキュリティ グループ タグもネットワーク上で適用できます。通常、スイッチ、ルータ、ファイアウォールなどのネットワーク デバイスには 2 というセキュリティ グループ タグが付与されます。

このドキュメントでは、Windows ユーザのドメイン グループに属し、正常に認証されたエンドユーザに「Employee」のダイナミック SGT が割り当てられます。そして、この SGT が Firepower Management のアクセス制御ルールに適用され、そのアクセス制御ルールが Firepower NGIPS 仮想センサーおよび ASA with Firepower サービスに適用されて実行されます。

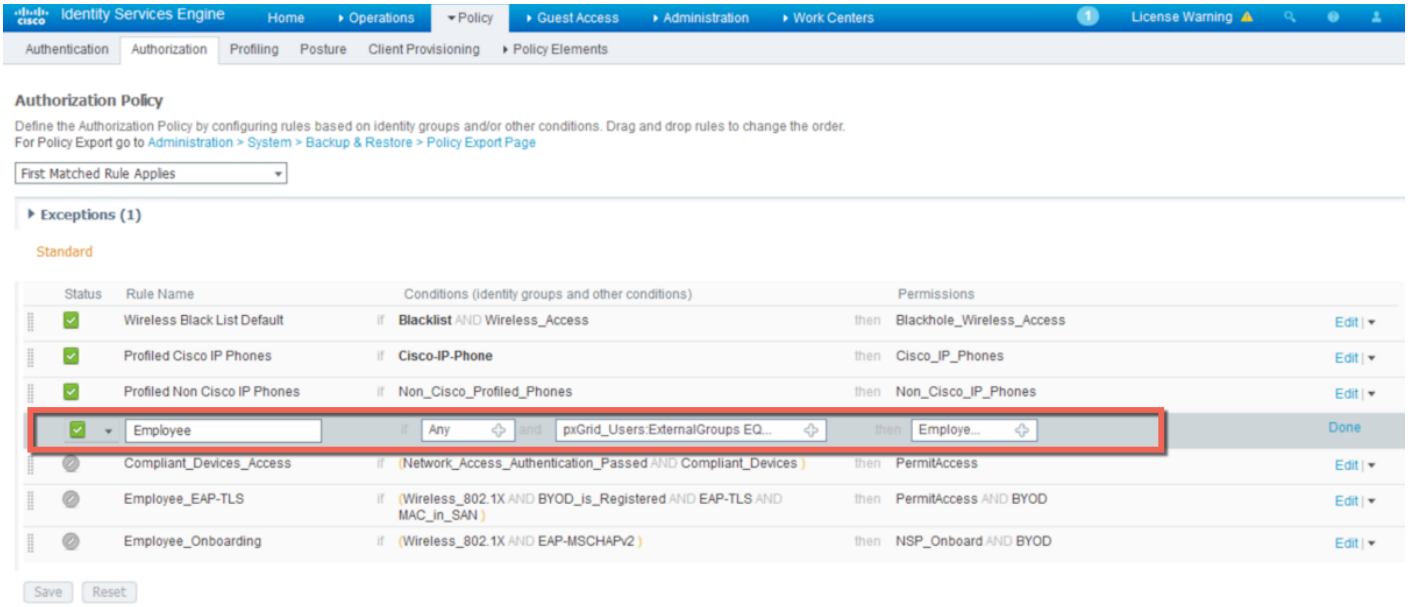
追加のセキュリティ グループ タグは、ISE 認可ポリシーから直接設定することも、[ワークセンター（Work Center）] -> [TrustSec] -> [コンポーネント（Components）] -> [セキュリティ グループ（Security Groups）] メニューを使用して ISE から直接設定することもできます。

手順 1. Employee Security タグを作成します。

[ポリシー（Policy）] -> [認可（Authorization）] -> ->

の順に選択し、次を入力します。

[ルール名（Rule Name）]：Employee
[新しい条件（New Condition）]：External Groups:equals:pxGrid_Users
[認可プロファイル（Authorization Profile(s)）]：Employee and Permit Access



手順 2. [完了（Done）] を選択します。

[保存（Save）] を選択します。

自己署名証明書の操作

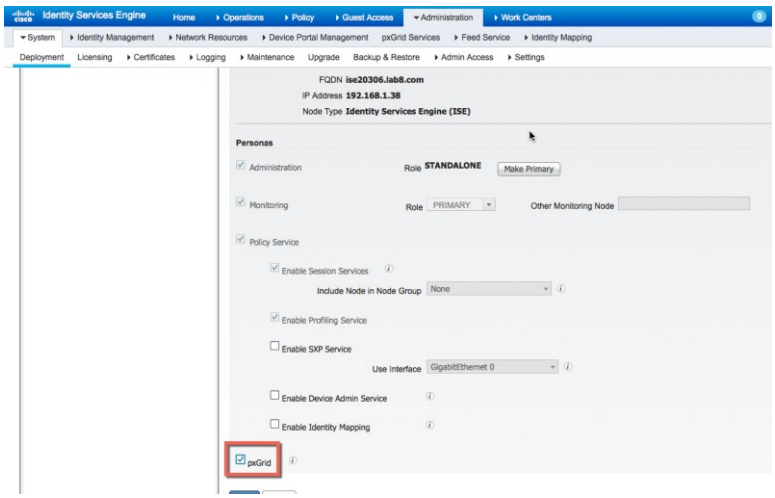
自己署名証明書は POC 環境のみに使用されます。この項は、CA 署名付き証明書を導入する場合、省略可能です。

ISE 2.0 の設定

自己署名証明書は POC 環境で使用されます。この設定の場合、ISE はスタンドアロン構成に導入されます。

注: ISE 1.3 や ISE 1.4 と異なり、ISE 自己署名アイデンティティ証明書を ISE 証明書信頼ストアにエクスポートする必要はなくなりました。

手順 1. [管理(Administration)] > [システム(System)] > [導入(Deployment)] を選択後、ノードを選択して [編集(Edit)] > から [pxGrid] をオンにします。

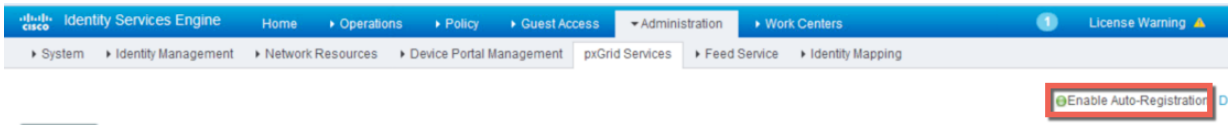


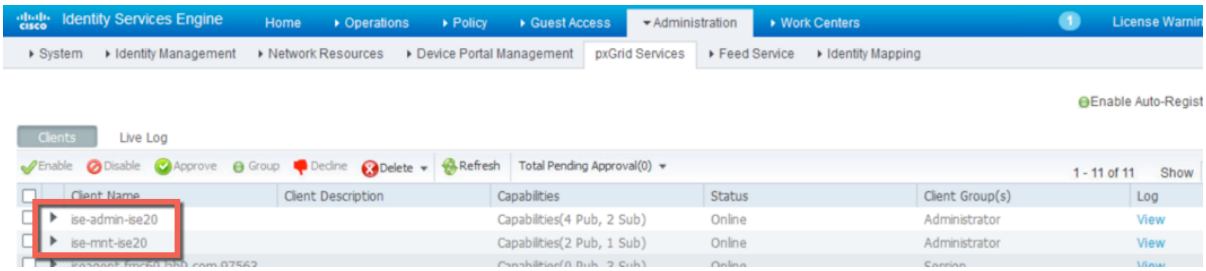
手順 2. [保存(Save)] を選択します。

手順 3. 公開されたノードが [pxGrid サービス(pxGrid Services)] の下に表示され、接続があることを確認します。[管理(Administration)] > [pxGrid サービス(pxGrid Services)] を選択します。

注: 公開されたノードが表示されるまでに時間がかかることがあります。ISE VM ノードで **sh application status ise** を実行し、pxGrid サービスが開始済みであることを確認してください。

手順 4. [自動登録の有効化(Enable Auto-Registration)] を有効化します。



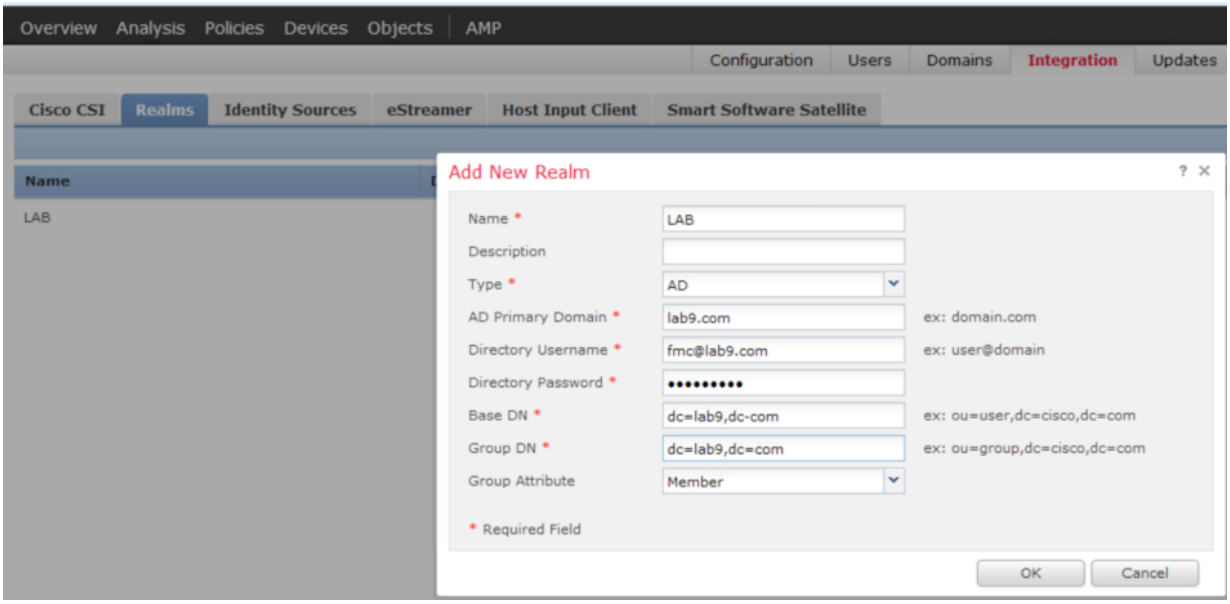


手順 5. [pxGrid に接続（connected to pxGrid）] となっていることを確認します。

Firepower ISE レルムの作成

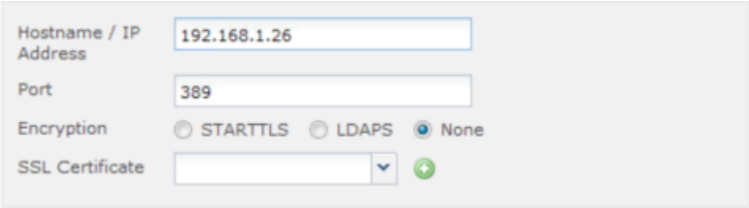
ISE レルムは、ISE 認証用であり、Firepower Management Center 6.0 ID ポリシーで使用されます。

手順 1. [システム（System）] > [統合（Integration）] > [レルム（Realms）] > [新規レルム（New Realm）] を選択します。



手順 2. [OK] を選択します。

手順 3. [ディレクトリの追加（Add Directory）] を選択し、FQDN ホスト名または情報を入力します。



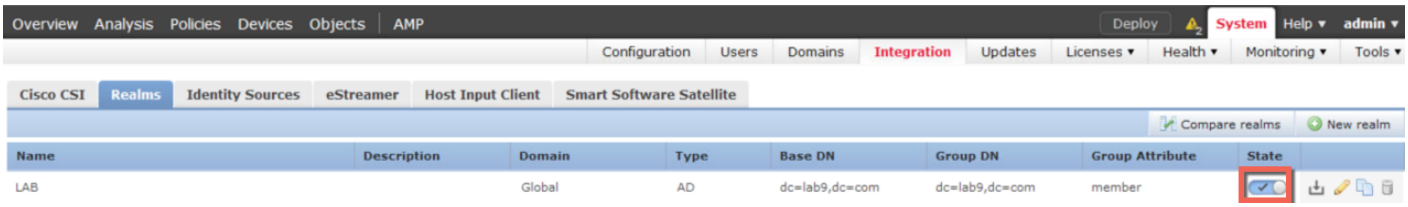
手順 4. [テスト(Test)] を選択します。[テスト接続は成功しました(Test Connection has succeeded)] と表示されたら [OK] を選択します。

注:試行の失敗が返された場合は、[レルム設定(Realm Configuration)] でディレクトリ ユーザ名とディレクトリ パスワードが正しいことを確認してください。

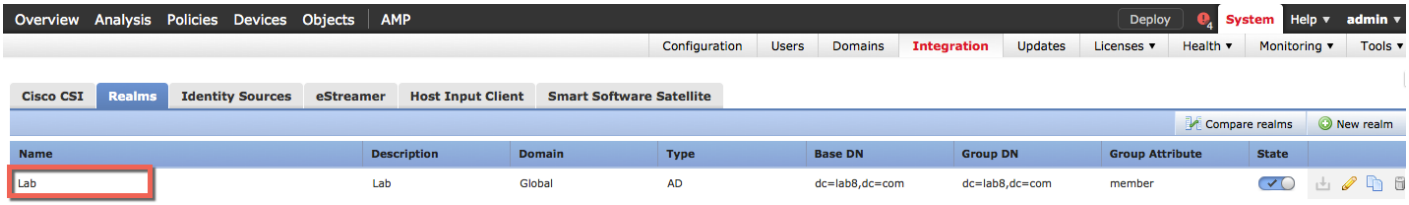
手順 5. [OK] を選択します。

手順 6. [保存(Save)] を選択します。

手順 7. を選択して [状態(State)] を有効にします。



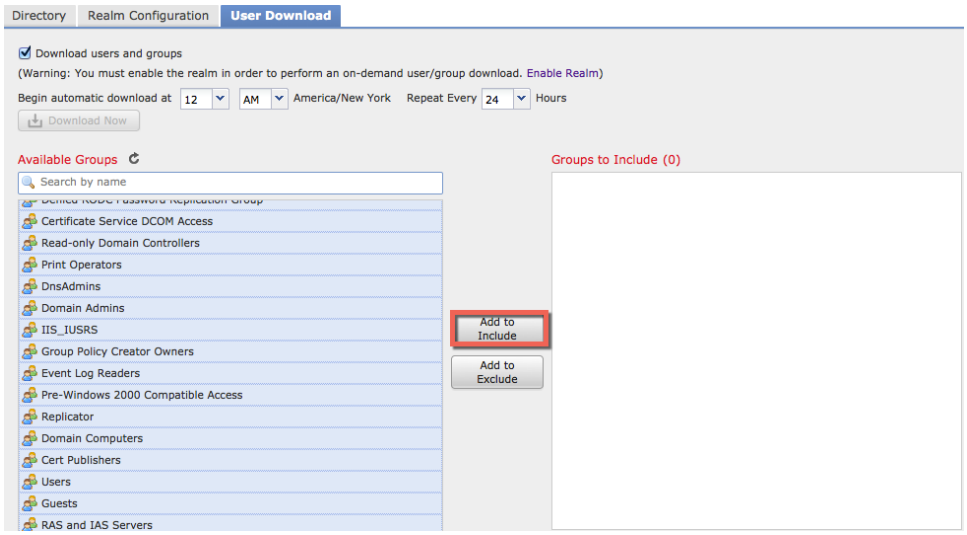
手順 8. レルム名をクリックします。



手順 9. [ユーザ ダウンロード(User Download)] をクリックします。

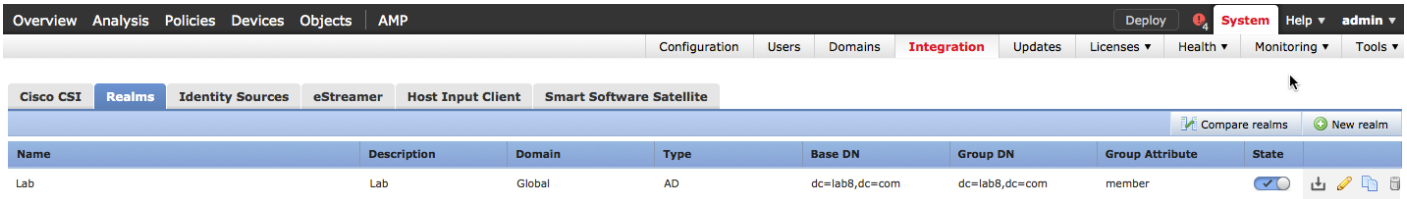
手順 10. [ユーザおよびグループのダウンロード(Download users and groups)] をオンにします。

手順 11. [使用可能なグループ(Available Groups)] をすべてハイライトし、[一覧に含める(Add to Include)] を選択します。



手順 12. [保存(Save)] を選択します。

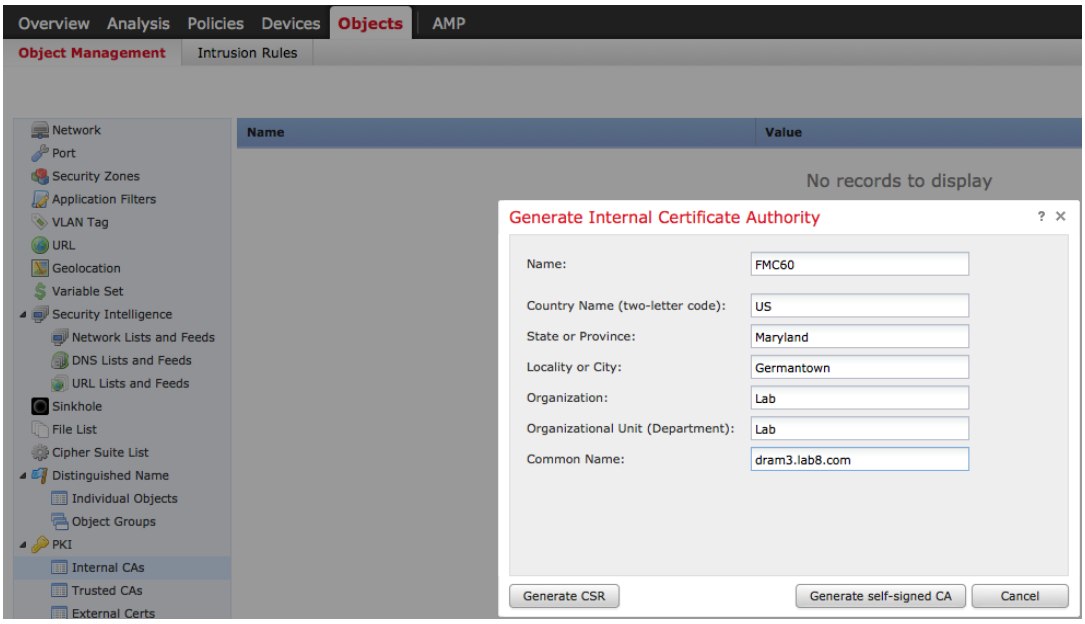
手順 13. 次が表示されます。



Firepower Management Center 6.0 の設定

この項では、ISE pxGrid ノード操作で自己署名証明書を使用するために、Firepower Management Center(FMC)を設定します。内部 FMC 認証局が Firepower Management Center に作成され、証明書に変換された後、Firepower Management Center の内部証明書ストアにインポートされます。内部 FMC 公開証明書は ISE 証明書信頼システムストアにエクスポートされます。ISE アイデンティティ自己署名公開証明書は Firepower Management Center 信頼 CA ストアにインポートされます。

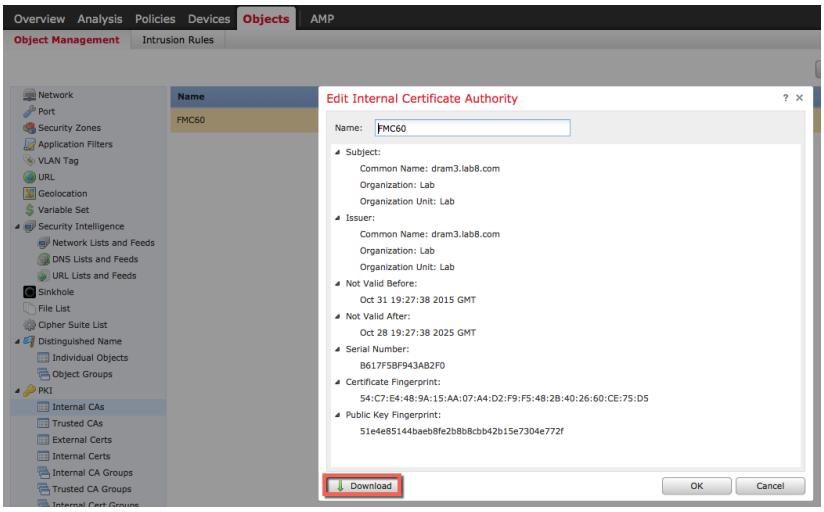
手順 1. [オブジェクト(Objects)] > [オブジェクト管理(Object Management)] > [PKI] -> [内部 CA(Internal CAs)] -> [CA の生成(Generate CA)] を選択し、次の証明書情報を入力します。
この例では、内部 CA に FMC60 という名前を指定しています。



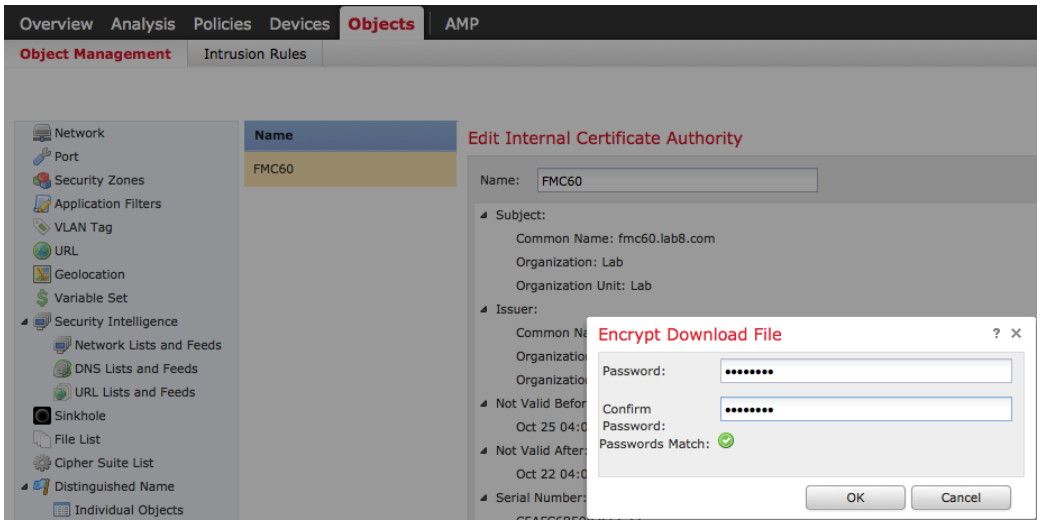
手順 2. [自己署名 CA の生成(Generate self-signed CA)] を選択します。

手順 3. 下図の鉛筆アイコンをクリックして、CA 証明書ファイルをダウンロードします。

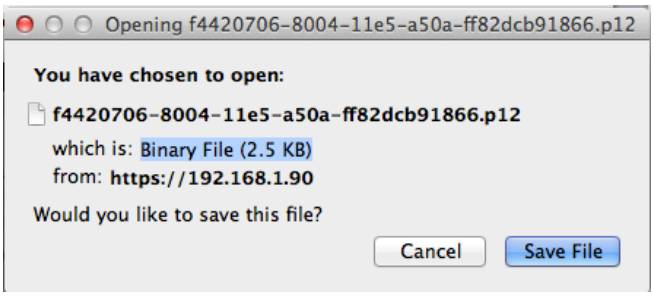
手順 4. [ダウンロード(Download)] を選択します。



手順 5. 暗号化パスワードを入力し、[OK] をクリックします。この例では、cisco123 を使用しています。

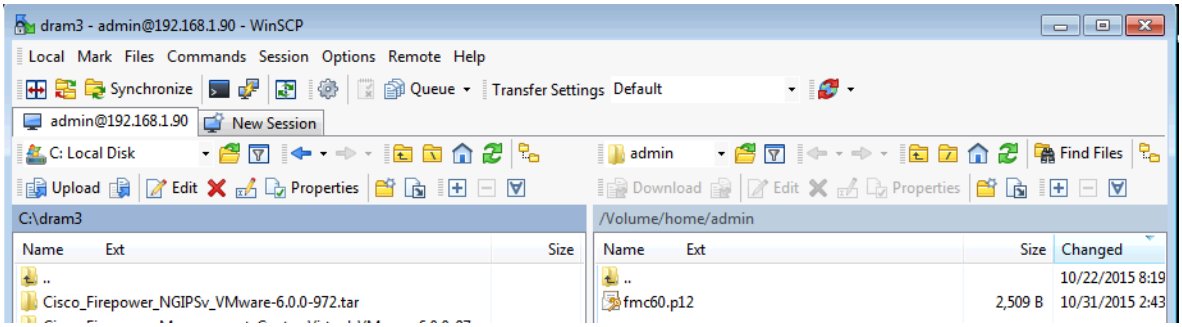


手順 6. .p12 ファイルをローカルに保存します。



手順 7. 使用しやすいように .p12 ファイル名を変更します。この例では、ファイル名が fmc60.p12 に変更されました。

手順 8. WinSCP または別の方法を使用して、Firepower Management Console にファイルをアップロードします。



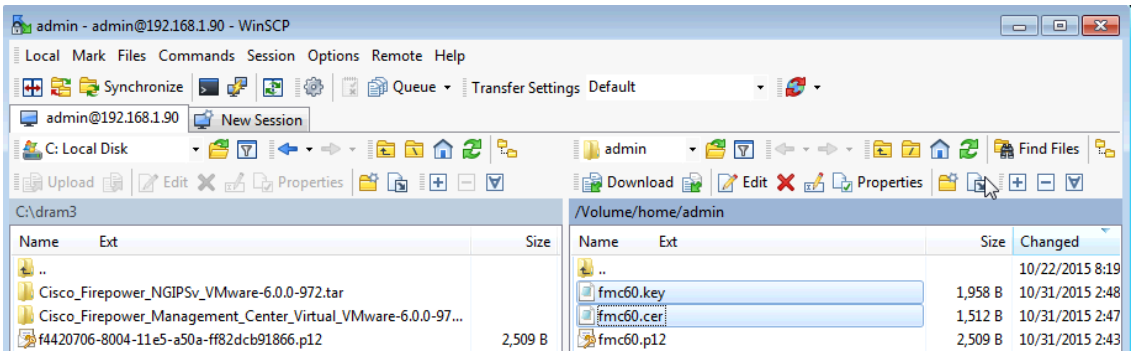
手順 9. Firepower Management Console に SSH で接続します。

手順 10. 次のコマンドを入力して、.p12 ファイルを CER および KEY ファイルに変換します。

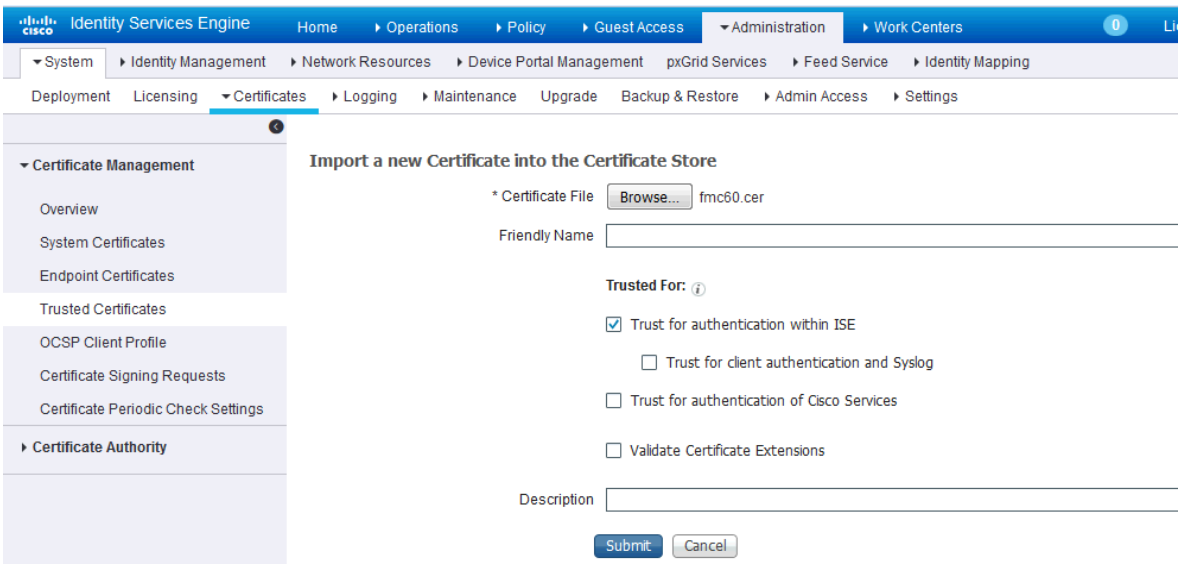
注：CER および KEY ファイル名は任意です。元の .p12 ファイルは fmc60.p12 に名前が変更されています。最初に Sudo パスワードの入力が求められます。インポート パスワード、PEM パスフレーズには、先に入力した暗号化キー パスワードを使用します。

```
sudo openssl pkcs12 -nokeys -clcerts -in fmc60.p12 -out fmc60.cer
Enter Import Password:
MAC verified OK
admin@sd:~$



sudo openssl pkcs12 -nocerts -in fmc60.p12 -out fmc601.key
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
admin@sd:~$
```

手順 11. WinSCP を使用して、fmc60.cer および fmc60.key ファイルを Firepower Management Center からローカル PC にコピーしました。

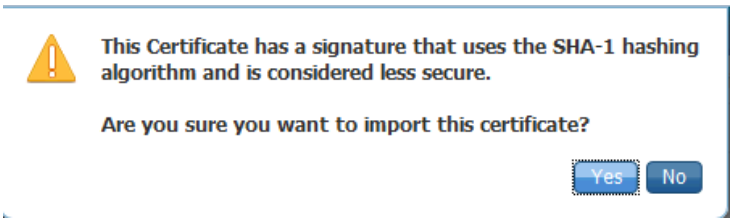


手順 12. Firepower Management 内部 CA 公開証明書は ISE 証明書信頼ストアにエクスポートされました。[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [信頼できる証明書（Trusted Certificates）] で [参照（Browse）] を選択し、fmc60.cer をアップロードします。

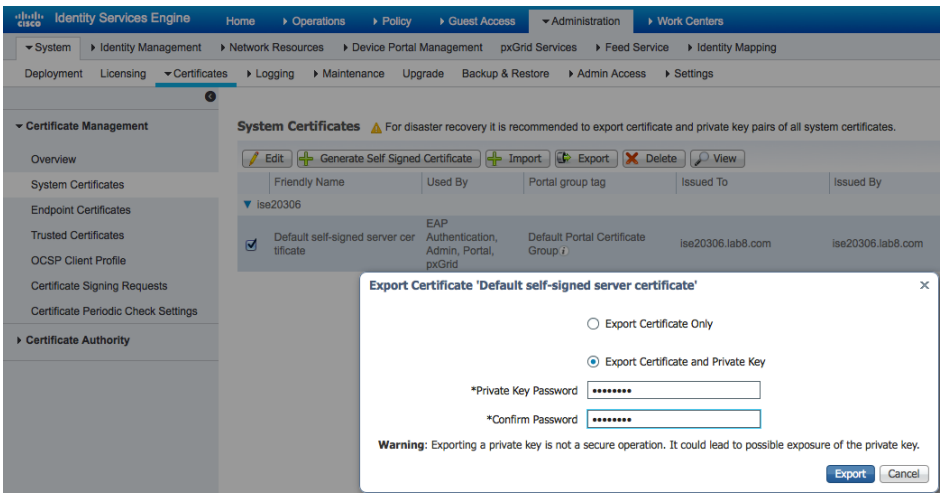


手順 13. [ISE 内認証の信頼(Trust for authentication within ISE)] をオンにし、[送信(Submit)] をクリックします。

手順 14. FMC 証明書のインポート時に次のメッセージが表示されるので、[はい(Yes)] を選択します。

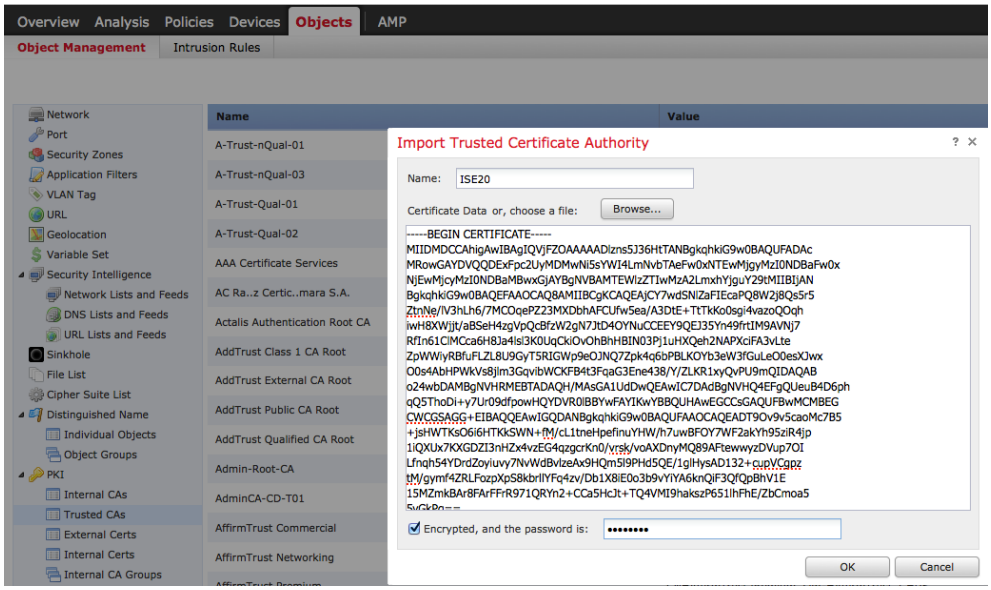


手順 15. [管理(Administration)] > [システム(System)] > [証明書(Certificates)] を選択し、ISE アイデンティティ自己署名証明書を選択した後、公開キーと秘密キーの両方を [エクスポート(Export)] します。



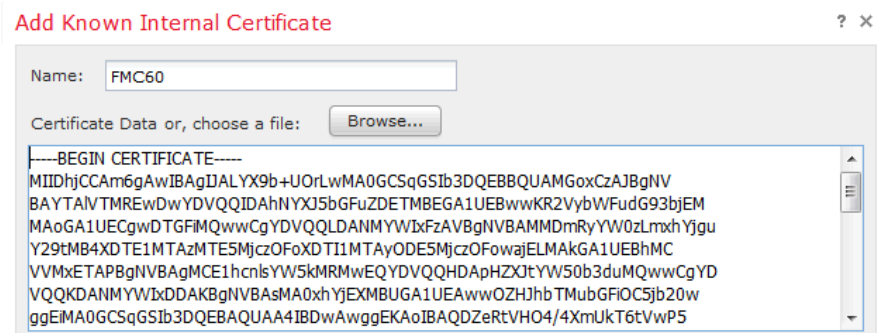
注：ファイルは Defaultserversignedcerti.zip ファイルとして保存されます。ファイルを解凍し、公開証明書の PEM ファイルのみを FMC 信頼ストアにエクスポートしてください。また、操作を容易にするために、ファイルの名前を ISE 2.0.pem に変更することもできます。

手順 16. ISE 自己署名アイデンティティ証明書を Firepower Management 信頼 CA ストアにインポートします。
[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [信頼 CA（Trusted CAs）] > [信頼 CA の追加（Add Trusted CA）] を選択し、名前を入力します。この例では、ISE が使用されています。ISE の暗号化キー パスワードを入力し、[OK] をクリックします。



手順 17. Firepower Management 内部 CA の公開/秘密キー ペアを Firepower Management Center の内部証明書ストアにインポートします。
[オブジェクト（Objects）] > [PKI] > [内部証明書（Internal Certs）] > [内部証明書の追加（Add Internal Cert）] を選択します。
秘密キーについても同じ手順に従います。

注：-----Begin Certificates が始まるまでの Bag 属性を削除してください。



手順 18. 「---Begin…」の前のキー ファイルの Bag 属性を削除します。

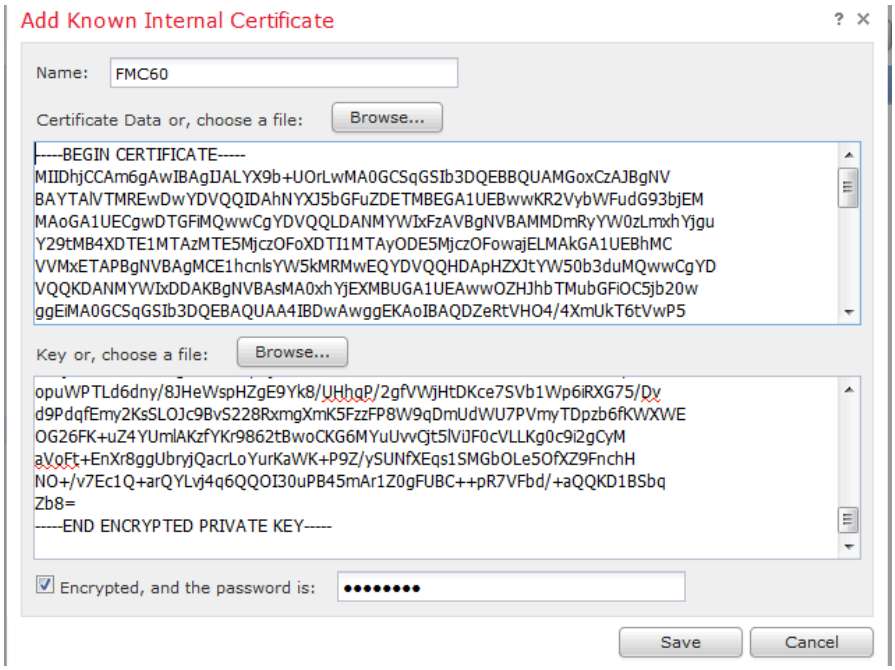

```
Bag Attributes
    localKeyID: 3D DA 20 3E A2 9A 99 ED 5D 2C 30 53 73 8E 1D 67 4A 52 8E 9C
Key Attributes: <no attributes="">
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIIpjU/hWyevACAggA
MBQGCCqGSIb3DQMHBAgh7ZvVZ8MMGgSCBMjooxQEN+/wWMHo6FH2cJ+qAHhD0V3T
hHVq2py8G19lBecv5R6ltY6oY2kpaYjRY3jSkuCxGcwtpUFW03uVBHde7E2vNpXP
mpVX2sZqQ/xuRhS7a3ihh9qq357jAA1ecI+nJ9N1omMriX16r87VJKDfjqCBJ+HI
```


手順 19. </no> も削除します

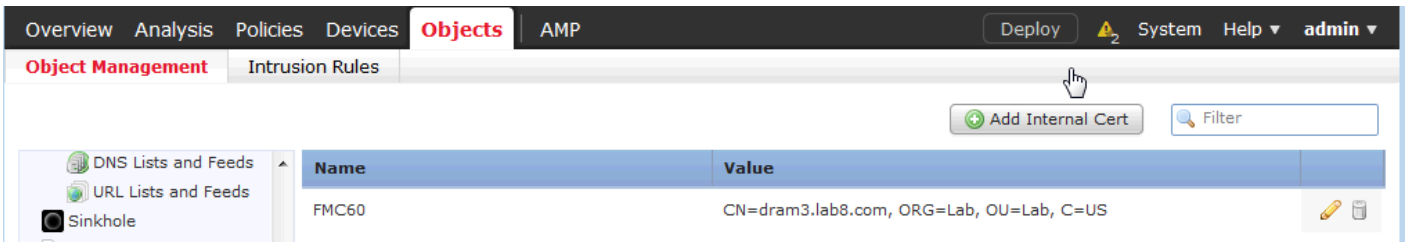

```
McCjBykAv73MXKY8FQJl2MyWoYmJ84qr2NTajqhpyS/UFavOkMsx2l9nBtzV+Hxd
DPycz8/fK1jQWwE7Y/6SUOeQ8hUMMaAeNYqfagA0Jhwntn/8y+A6R3ytK4AoZCtQ
9WQMizAi2N9jneQxjI4SOjnjUSiwqKHwB2wHFEFu9pR6ZfMoN7xU3eYDlJ/n1SgO
ENlYYGfOjCs7kNxVwqtc21FfQ0URkEZ9jOUFuj55EqTdXxbCdFTTKmHjZdQmCICA
3hOWu5IkHHTA5Kre05AYLe1lhW3xE5qL8yH5XOSfdREwq1aX2GU4BEQqGMDtkGbq
D7w=
-----END ENCRYPTED PRIVATE KEY-----
</no>
```


手順 20. 暗号化パスワードを入力します。

手順 21. 次が表示されます。



手順 22. [保存(Save)] を選択します。
次が表示されます。

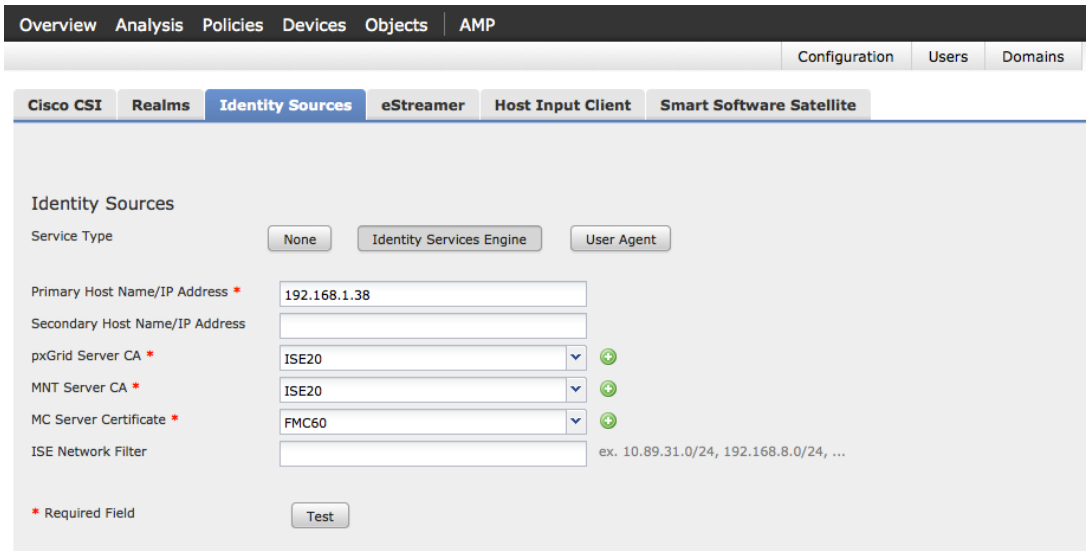


Firepower ISE ID ソースの設定

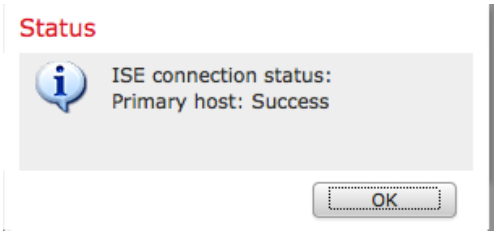
ID ソース エンジン設定では、ISE pxGrid ノード接続パラメータ、ISE MnT ノード証明書、FMC 6.0 アイデンティティ証明書を定義します。

手順 1. [システム(System)] > [統合(Integration)] > [ID ソース(Identity Sources)] > [Identity Services Engine] を選択します。

[プライマリ ホスト名/IP アドレス(Primary Host Name/IP Address)]:プライマリ FQDN pxGrid 名または IP アドレス
[セカンダリ ホスト名/IP アドレス(Secondary Host Name/IP Address)]:セカンダリ FQDN pxGrid 名または IP アドレス
*[pxGrid サーバ CA(pxGrid Server CA)]:ISE pxGrid ノード証明書(インポートした ISE 自己署名アイデンティティ証明書)
*[mnt サーバ CA(MNT Server CA)]:ISE pxGrid ノード証明書(インポートした ISE 自己署名アイデンティティ証明書)
[MC サーバ証明書(MC Server Certificate)]:FMC のアイデンティティ証明書(インポートした内部証明書)



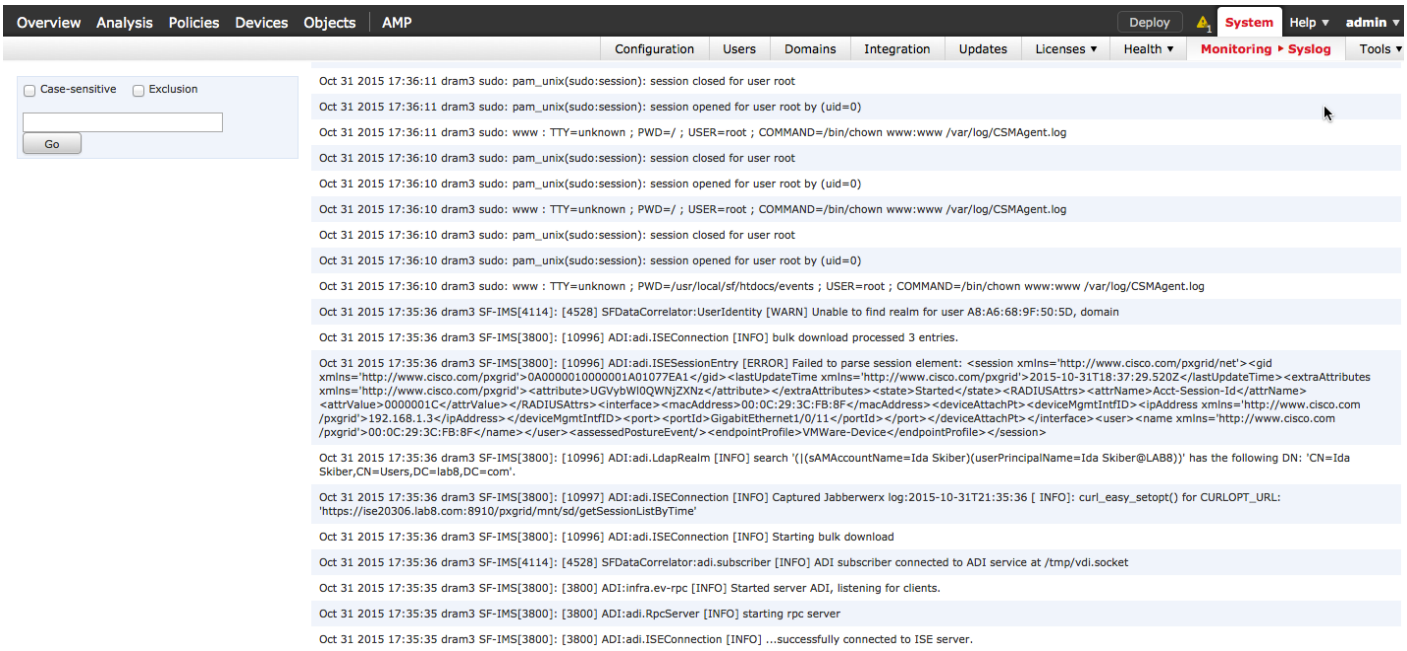
手順 2. [テスト(Test)] を選択します。
次が表示されます。



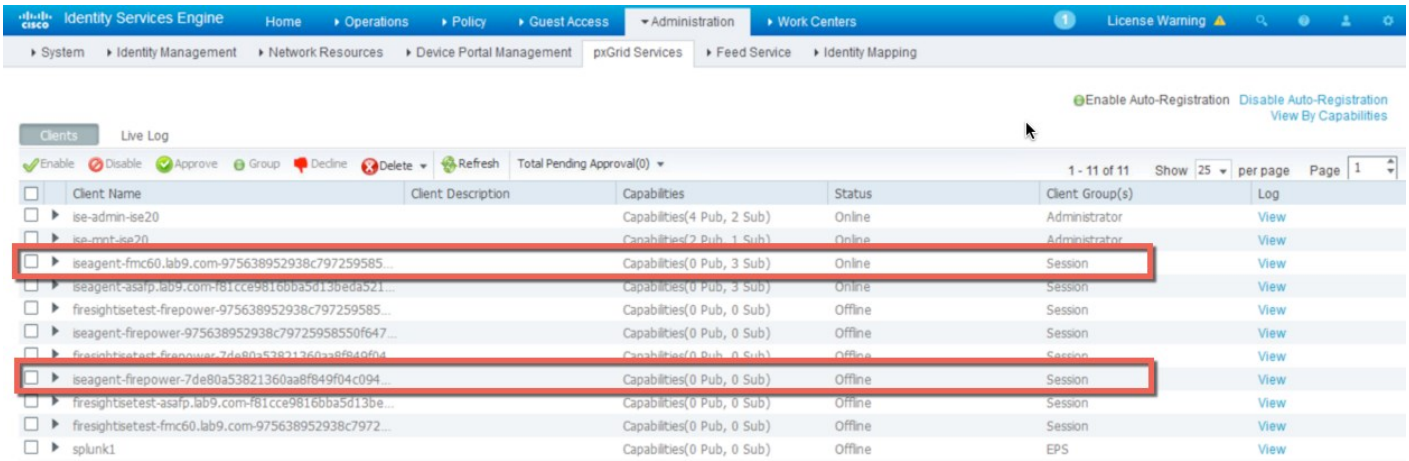
手順 3. [OK] を選択します。

手順 4. [保存(Save)] を選択します。

手順 5. [システム(System)] > [モニタリング(Monitoring)] > [Syslog] を選択します。
FMC が ISE サーバに正常に接続されたことを確認します。



手順 6. ISE に次のように表示されます。



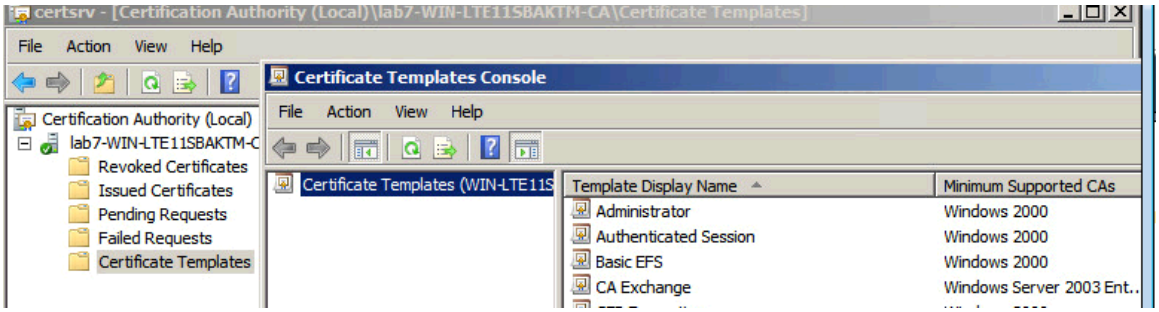
CA（認証局）- 署名付き証明書の操作

この項では、ISE スタンドアロン環境に ISE 2.0 および Cisco Firepower Management Center 6.0 を導入するための設定について詳細に説明します。この項は、自己署名証明書を導入する場合、省略可能です。

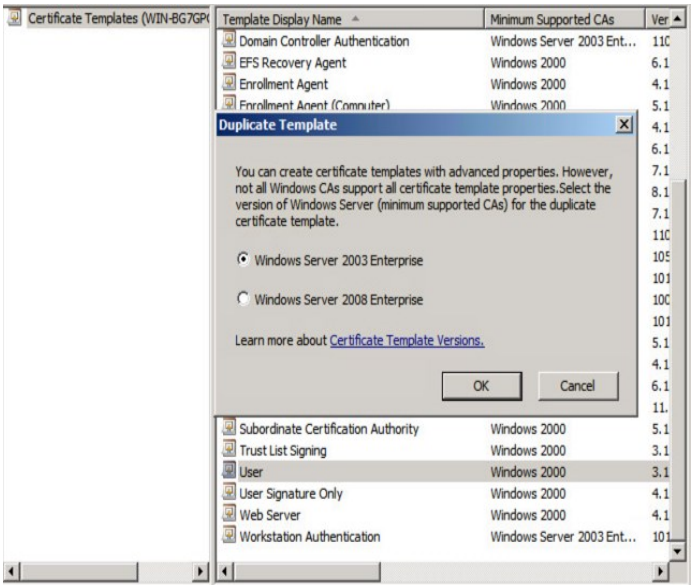
CA 署名操作用にカスタマイズされた pxGrid テンプレート

pxGrid クライアント、Firepower Management Center、および ISE pxGrid ノード間の pxGrid 操作には、クライアント認証とサーバ認証の両方の Enhanced Key Usage（EKU）を持つ、カスタマイズされた pxGrid テンプレートが必要です。これは、Firepower Management Center と ISE pxGrid のノードの両方が同じ CA によって署名された認証局（CA）署名環境で必要です。

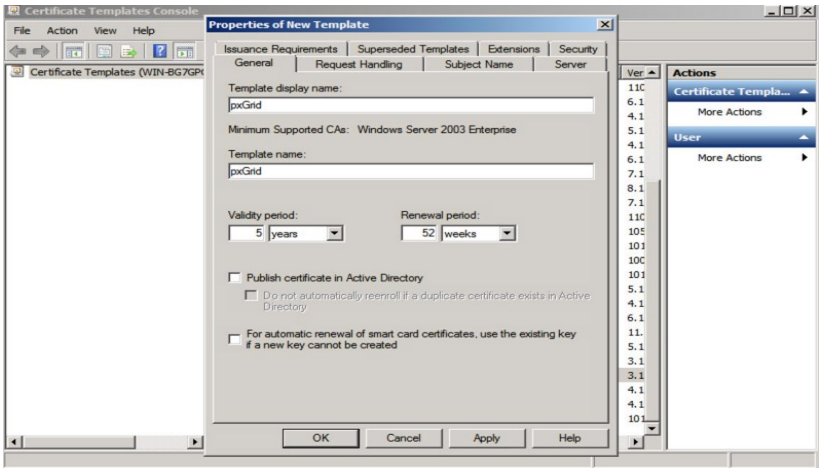
手順 7. [管理ツール（Administrative Tools）] > [認証局（Certificate Authority）] を選択し、CA サーバの横の [+] をクリックして、ドロップダウン リストから [証明書テンプレート（Certificate Templates）] を右クリックして、[管理（Manage）] を選択します。



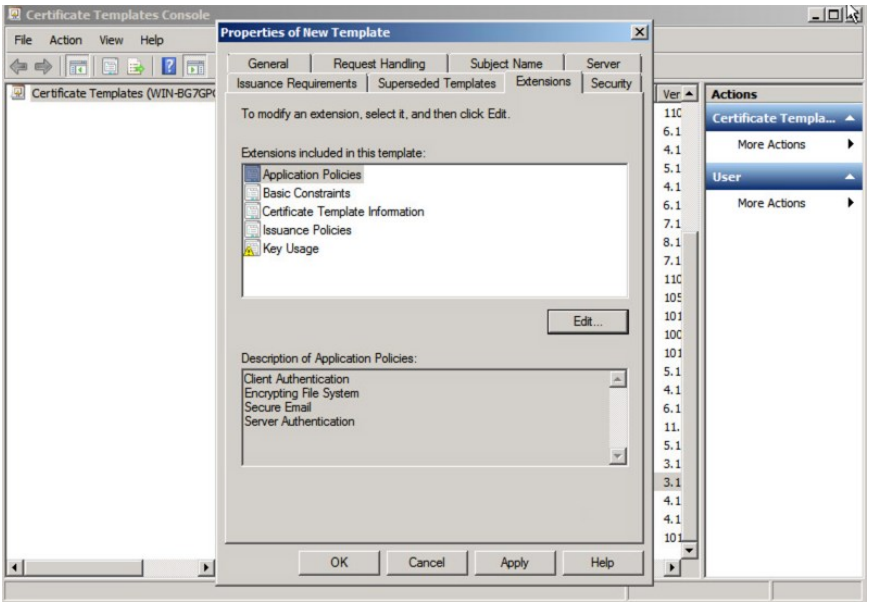
手順 8. 右クリックして、[ユーザテンプレートの複製（Duplicate User template）] を選択し、[Windows 2003 Enterprise] を選択して、[OK] をクリックします。



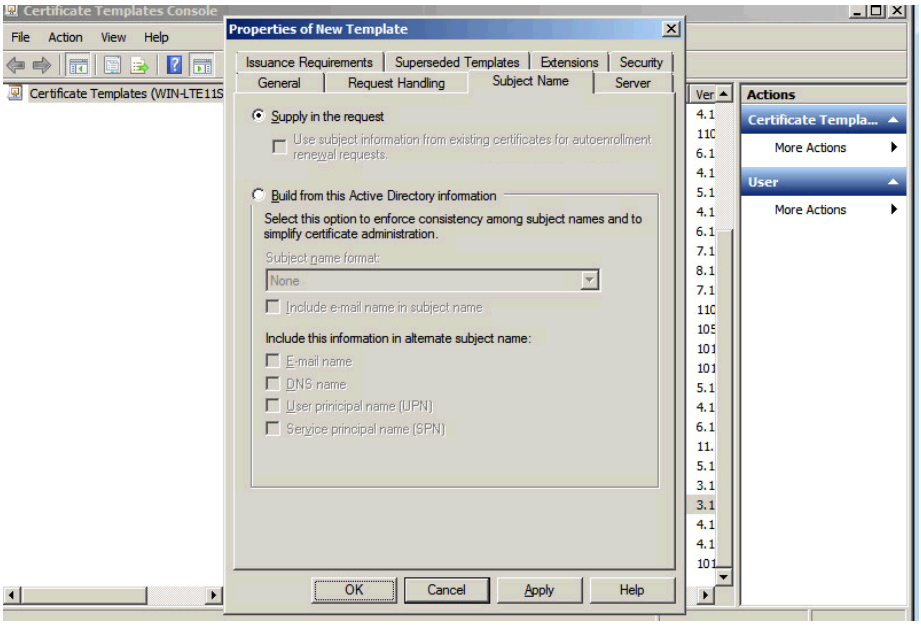
手順 9. 証明書テンプレートの名前を入力し、[Active Directory の証明書を発行する（Publish certificate in Active Directory）] をオフにして、有効期間および更新期間を指定します。



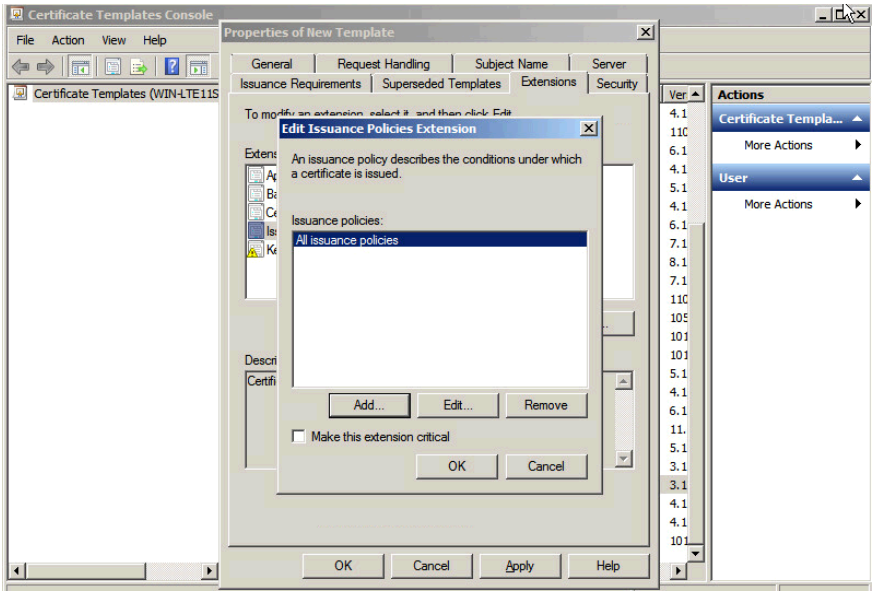
手順 10. [拡張（Extensions）] > [追加（Add）] > [サーバ認証（Server Authentication）] > [OK] > [適用（Apply）] の順にクリックします。



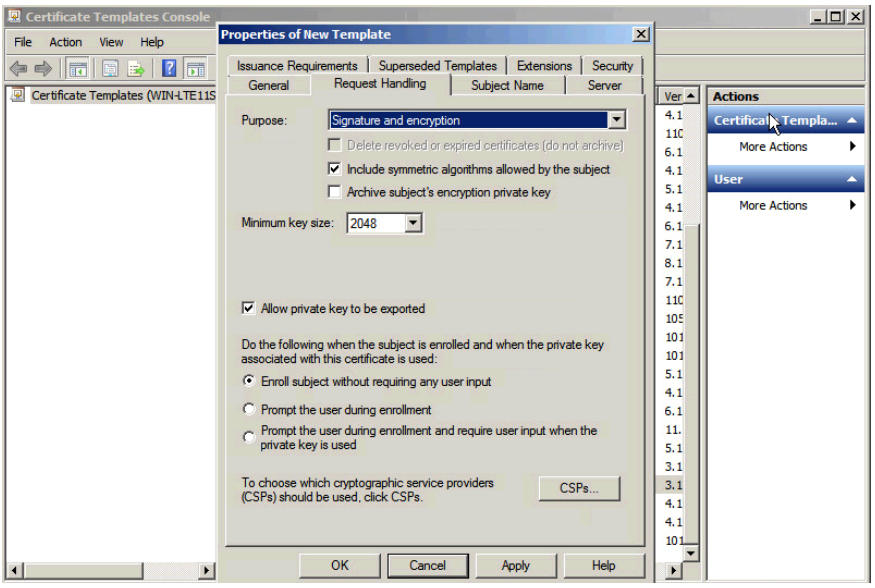
手順 11. [サブジェクト名（Subject Name）] をクリックし、[要求に含まれる（Supply in request）] をオンにします。



手順 12. [拡張（Extensions）] > [発行ポリシー（Issuance Policies）] > [編集（Edit）] > [すべての発行ポリシー（All Issuance Policies）] の順にクリックします。

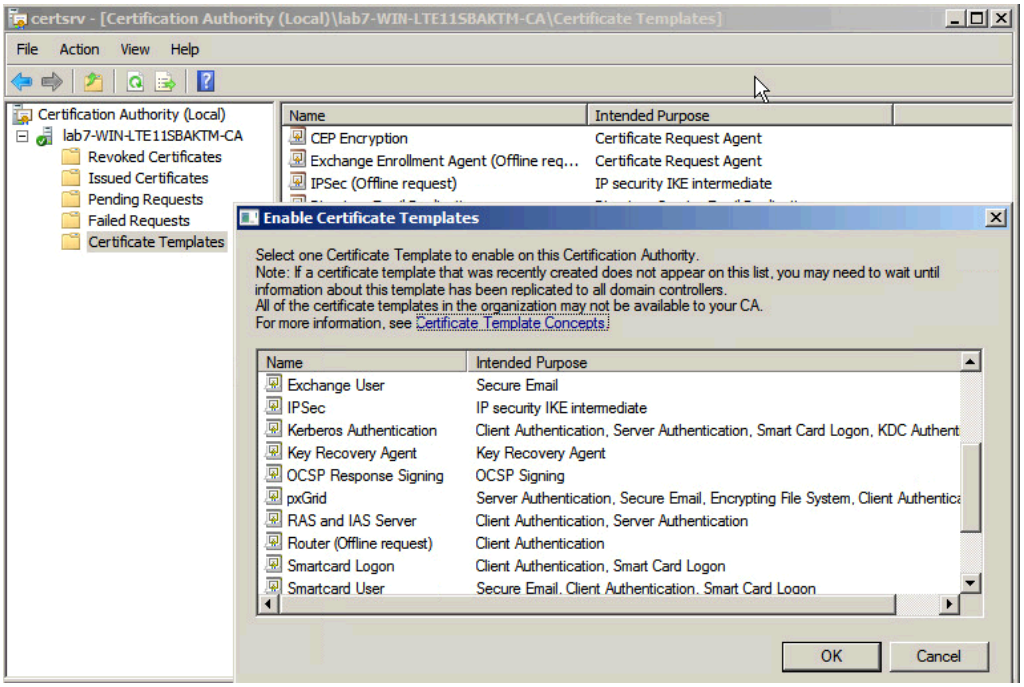


手順 13. 要求処理をデフォルトのままにします。

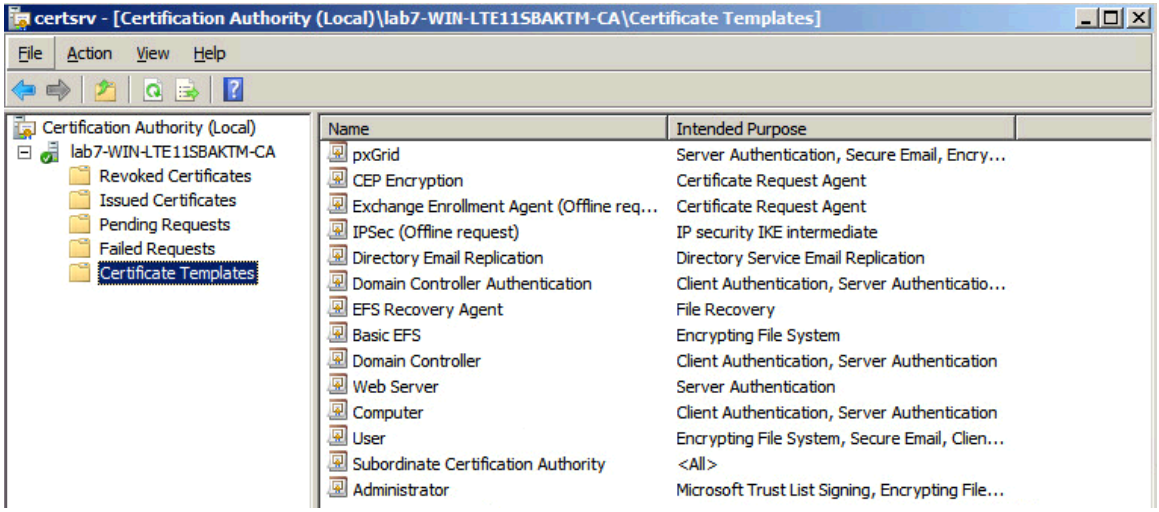


手順 14. [証明書テンプレート(Certificate templates)] を右クリックします。

手順 15. 発行する [新規テンプレート(New Template)] を選択し、[pxGrid] を選択します。



手順 16. pxGrid のテンプレートが表示されます。



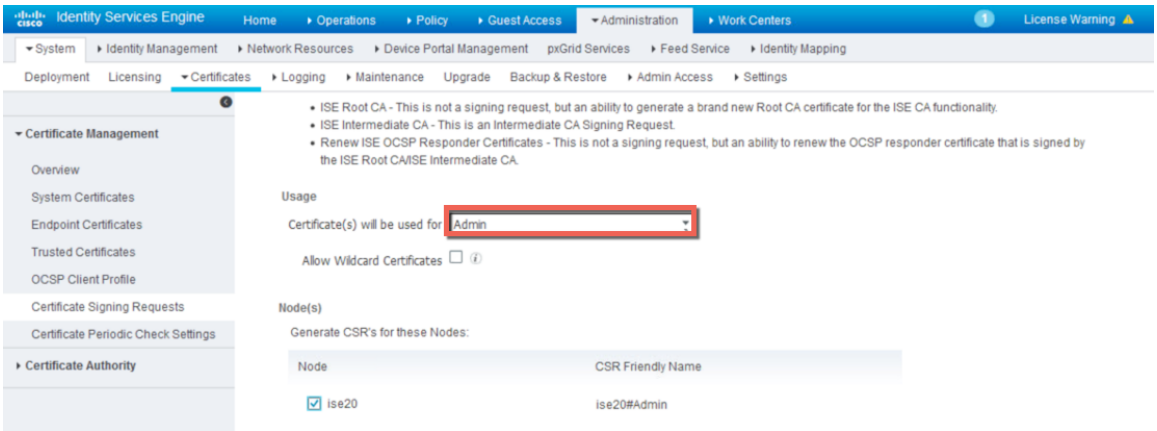
ISE 2.0 の設定

ISE pxGrid ノードをスタンドアロン構成における認証局（CA）署名環境用に設定します。最初に、「pxGrid」CSR 要求が ISE ノードから生成され、pxGrid のカスタマイズされたテンプレートを使用して、CA サーバによって署名されます。証明書は最初の ISE CSR 要求にバインドされます。

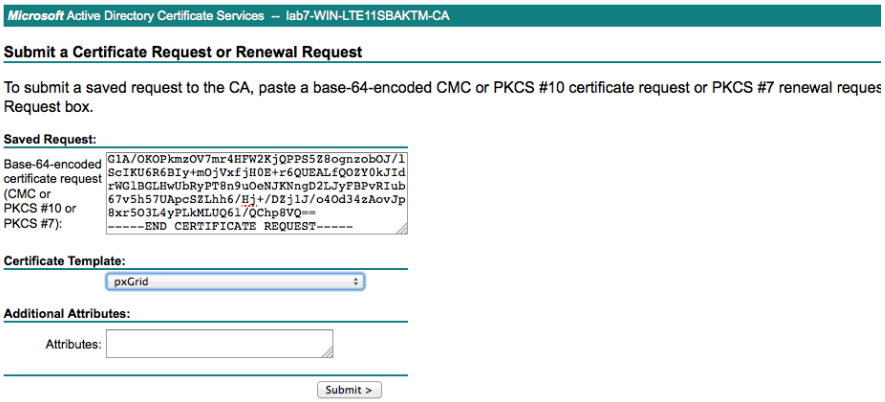
CA ルート証明書は ISE 証明書信頼ストアにインポートされます。ISE ID 識別証明書は ISE 証明書システム ストアにエクスポートされます。ISE ノードは pxGrid 操作用に有効化されます。

手順 1. ISE pxGrid ノードになる ISE ノードの CSR 要求を生成します。[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [証明書署名要求（Certificate Signing Requests）] -> [生成（Generate）] を選択します。

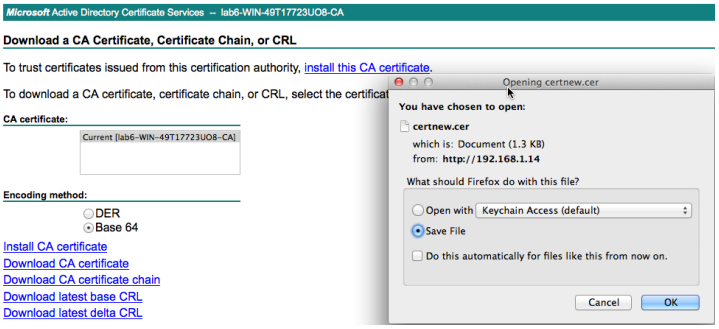
注：証明書の用途は管理であることが必要です。これは、FMC 6.0 のアクティブなー括ダウンロード セッションに必須です。



手順 2. [証明書の要求（Request a certificate）] > [証明書の要求の詳細設定（Advanced certificate request）] を選択し、CSR 情報をコピーして貼り付け、カスタマイズした pxGrid テンプレートを選択して、[送信（Submit）] をクリックします。

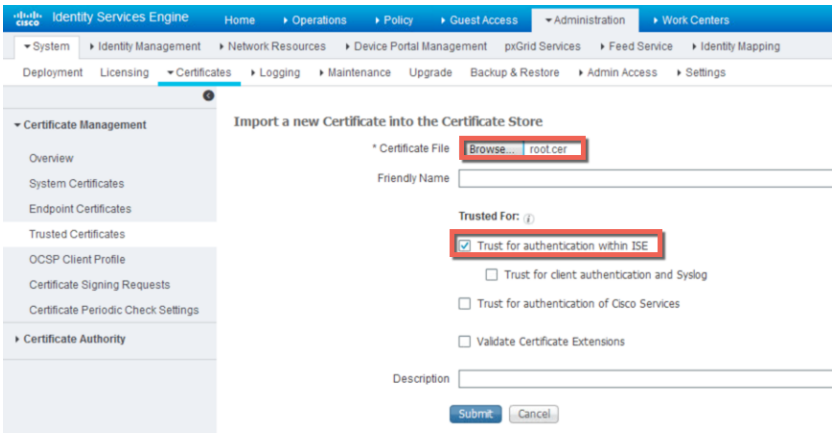


手順 3. Base 64 符号化形式の CA ルートをダウンロードします。

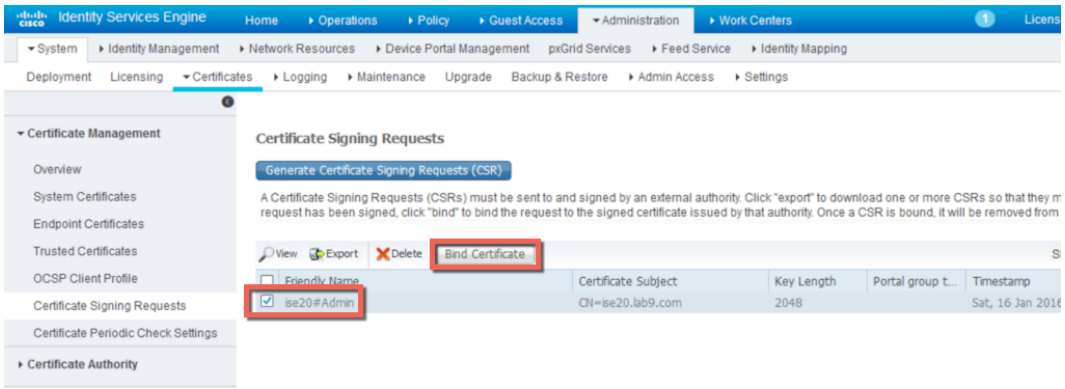


手順 4. CA ルートを ISE 証明書信頼システム ストアにアップロードします。
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] を選択し、CA ルート証明書をアップロードします。

手順 5. [ISE 内認証の信頼（Trust for authentication within ISE）] をオンにし、[送信（Submit）] をクリックします。



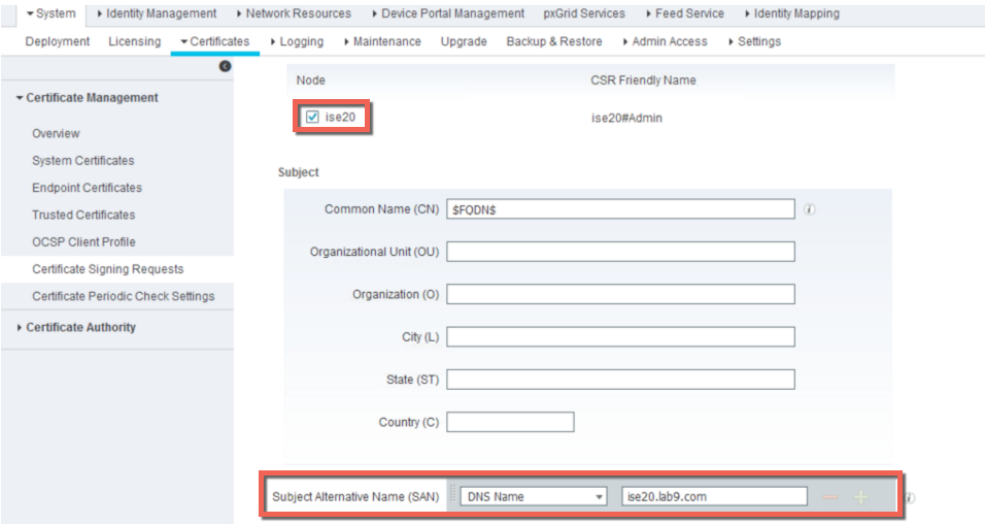
手順 6. ISE pxGrid ノード証明書を ISE 証明書システム ストアにアップロードします。[管理(Administration)] > [システム(System)] > [証明書署名の要求(Certificate Signing Requests)] を選択し、証明書を CSR 要求にバインドします。



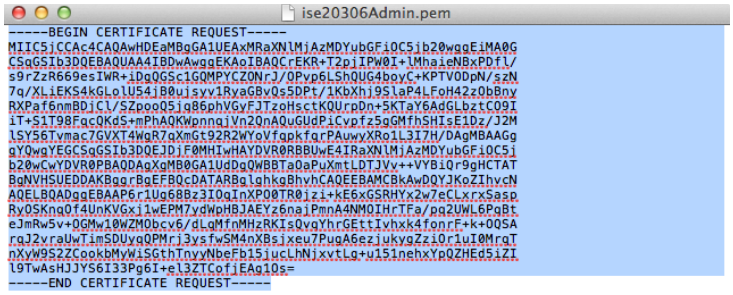
手順 7. [管理(Administration)] > [システム(System)] > [証明書(Certificate)] > [証明書管理(Certificate Management)] > [証明書署名の要求(Certificate Signing Requests)] > [証明書署名要求(CSR)の生成(Generate Certificate Signing Requests (CSR))] を選択し、証明書の用途として [管理(Admin)] を選択します。

手順 8. ノードを選択します。

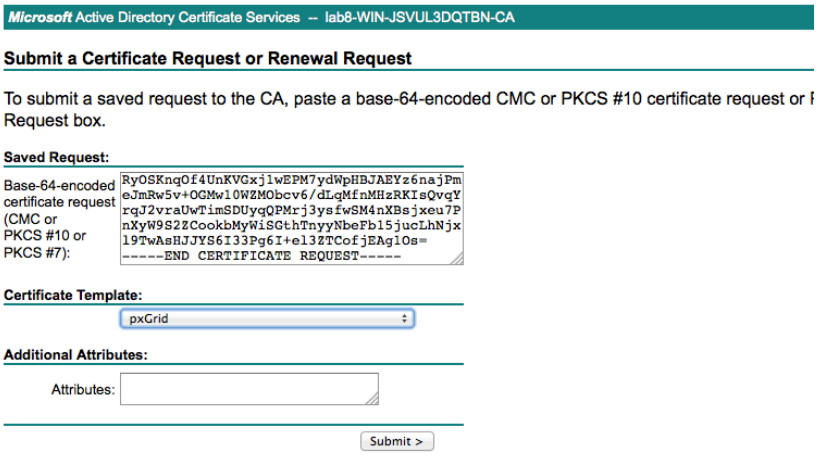
手順 9. [サブジェクト代替名(SAN)(Subject Alternative Name (SAN))] で [DNS 名(DNS Name)] を選択し、DNS 名を追加します。



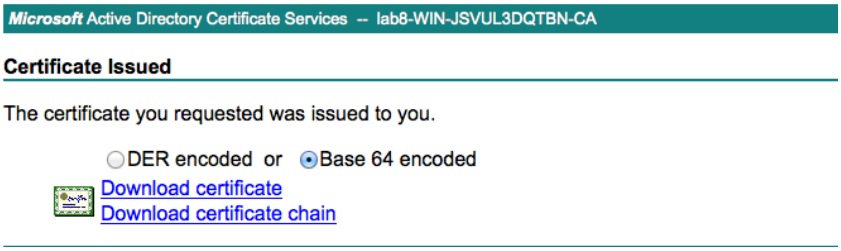
手順 10. [作成（Generate）] を選択します。
手順 11. [エクスポート（Export）] を選択します。
手順 12. pem ファイルを開き、csr 要求をコピーしてカスタマイズした pxGrid テンプレートに貼り付けます。



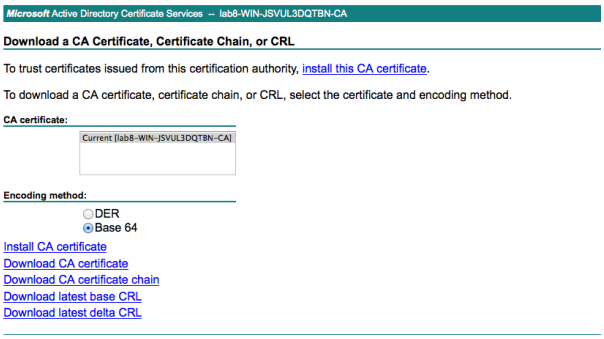
手順 13. [証明書の要求（Request a Certificate）] > [証明書の要求の詳細設定（Advanced Certificate Request）] を選択して貼り付け、カスタマイズした pxGrid テンプレートを選択した後、[送信（Submit）] をクリックします。



手順 14. [送信（Submit）] を選択します。
手順 15. [Base 64 エンコード形式（Base 64 encoded）] を選択して証明書をダウンロードします。

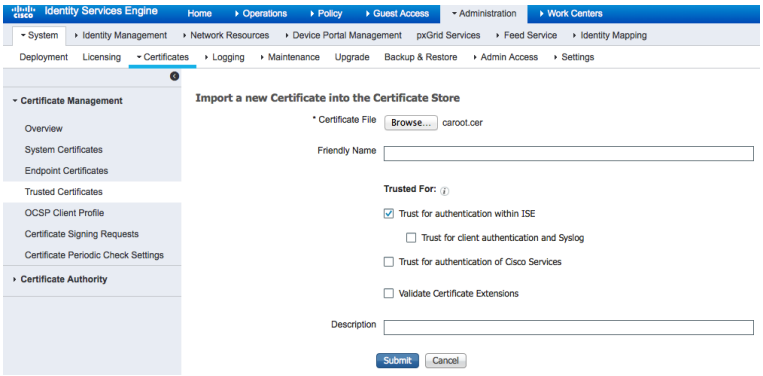


手順 16. [Base 64 形式(Base 64)] を選択して CA ルート証明書をダウンロードします。



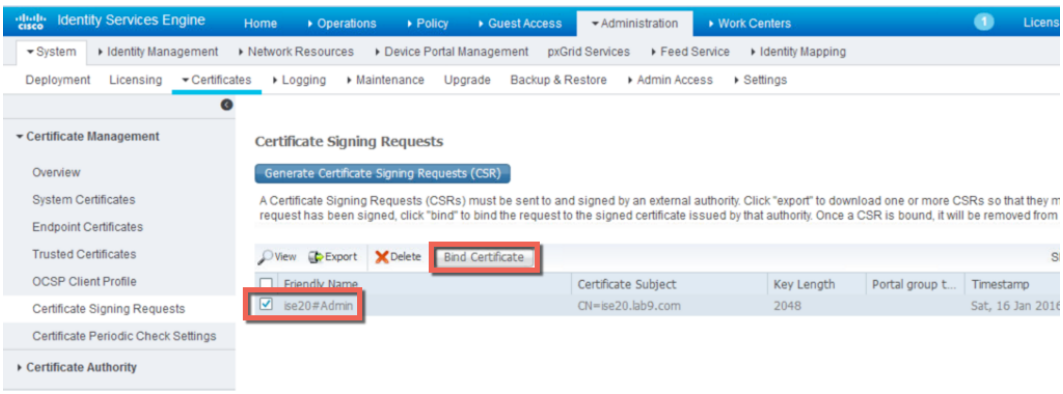
手順 17. [管理(Administration)] > [システム(System)] > [証明書(Certificate)] > [証明書管理(Certificate Management)] > [信頼できる証明書(Trusted Certificates)] の順に選択し、ルート証明書をインポートします。

手順 18. [ISE 内の認証用に信頼する(Trust for authentication within ISE)] をオンにします。

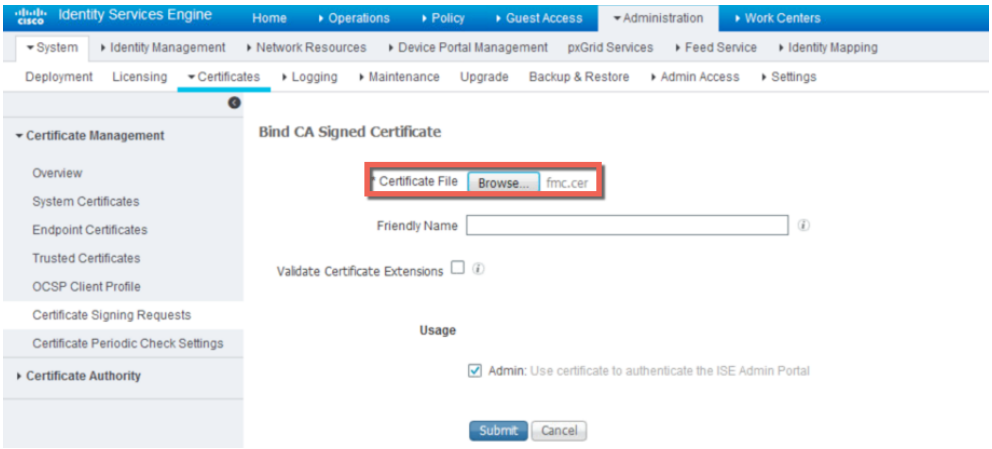


手順 19. [送信(Submit)] を選択します。

手順 20. [管理(Administration)] > [証明書(Certificate)] > [証明書管理(Certificate Management)] > [証明書署名の要求(Certificate Signing Requests)] の順に選択し、CSR 要求を選択した後、[証明書のバインド(Bind Certificate)] を選択します。



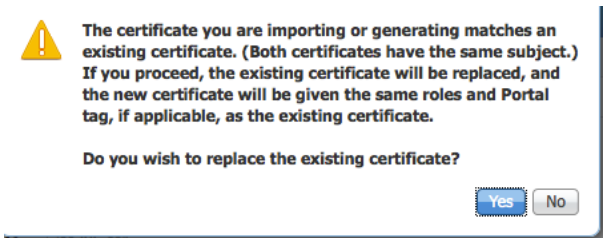
手順 21. ISE CA 署名付きアイデンティティ証明書をアップロードします。



手順 22. [送信（Submit）] を選択します。

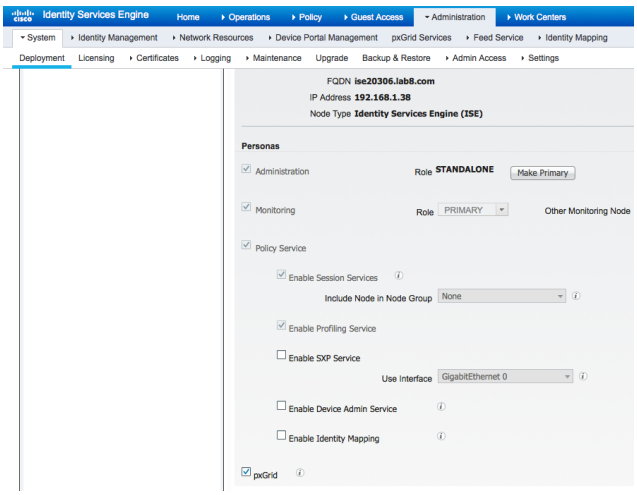
手順 23. 次のメッセージが表示されたら、[はい（Yes）] を選択します。

手順 24. 次のメッセージが表示されたら、[はい（Yes）] を選択します。



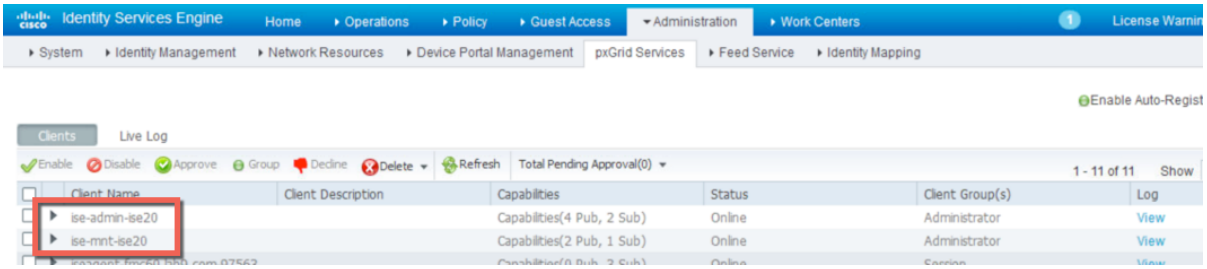
手順 25. システムが再起動され、GUI に戻ります。

手順 26. [管理(Administration)] > [システム(System)] > [導入(Deployment)] を選択し、ホスト名を編集して [pxGrid] をオンにします。



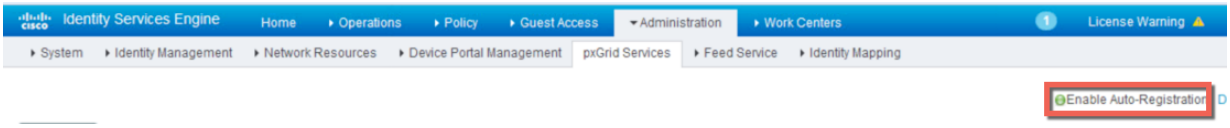
手順 27. [保存(Save)] を選択します。

手順 28. [管理(Administration)] > [pxGrid サービス(pxGrid Services)] を選択し、公開されたサービスが表示されることを確認します。



注:表示には数秒かかることがあります。ISE VM で「sh application status ise」を実行し、pxGrid サービスが初期化中であることを確認してください。

手順 29. [自動登録の有効化(Enable Auto Registration)] を有効化します。

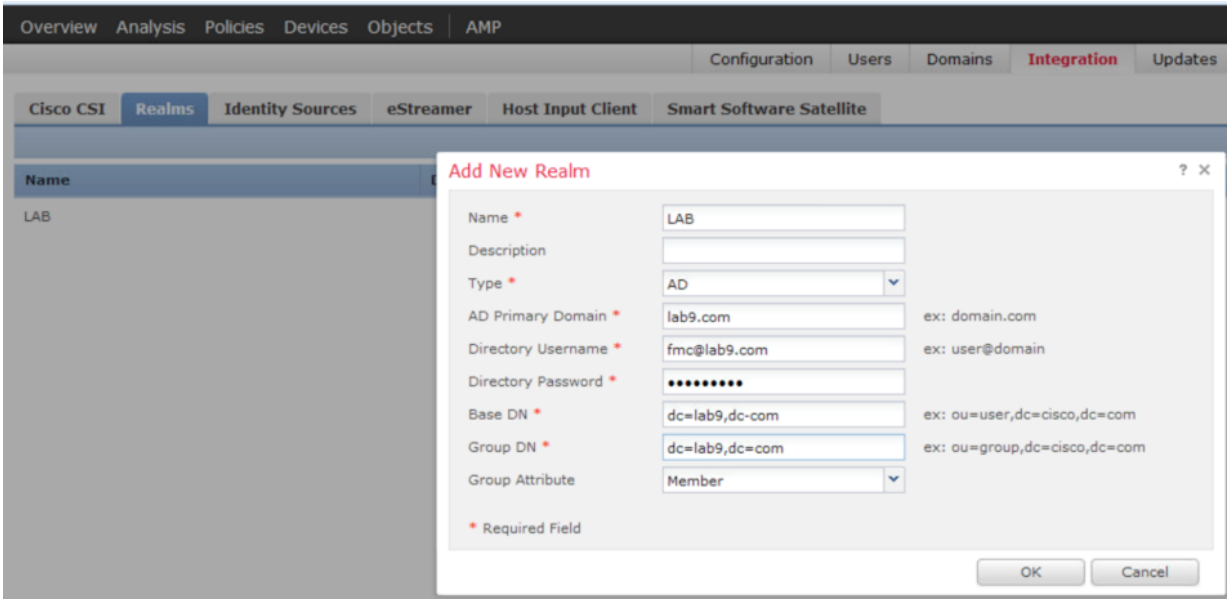


手順 30. [pxGrid に接続(connected to pxGrid)] となっていることを確認します。

Firepower ISE レルムの作成

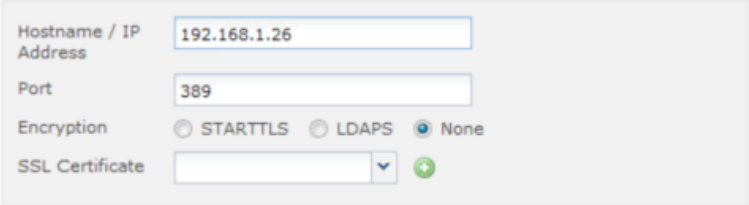
ISE レルムは、ISE 認証用であり、Firepower Management Center 6.0 ID ポリシーで使用されます。

手順 1. [システム(System)] > [統合(Integration)] > [レルム(Realms)] > [新規レルム(New Realm)] を選択します。



手順 2. [OK] を選択します。

手順 3. [ディレクトリの追加(Add Directory)] を選択し、FQDN ホスト名または情報を入力します。



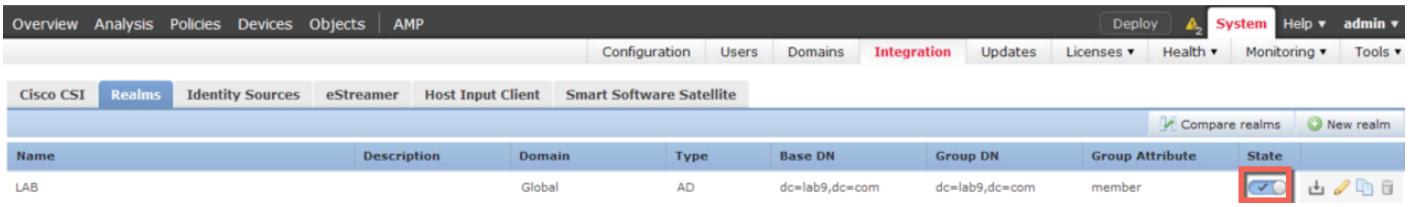
手順 4. [テスト(Test)] を選択します。[テスト接続は成功しました(Test Connection has succeeded)] と表示されたら [OK] を選択します。

注: 試行の失敗が返された場合は、[レルム設定(Realm Configuration)] でディレクトリ ユーザ名とディレクトリ パスワードが正しいことを確認してください。

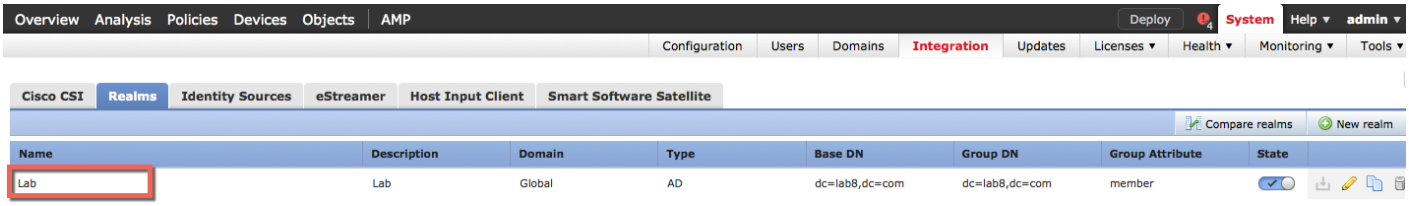
手順 5. [OK] を選択します。

手順 6. [保存(Save)] を選択します。

手順 7. を選択して [状態(State)] を有効にします。



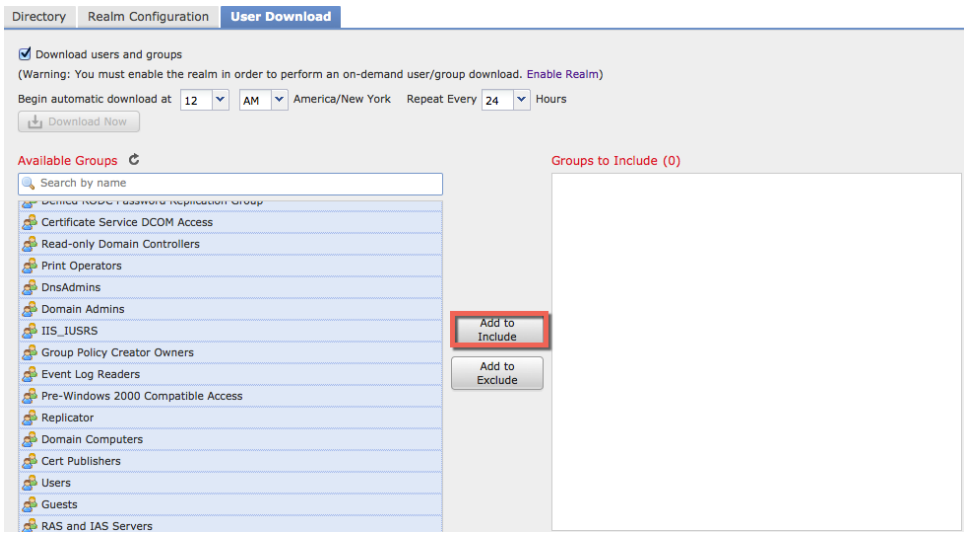
手順 8. レルム名をクリックします。



手順 9. [ユーザ ダウンロード（User Download）] をクリックします。

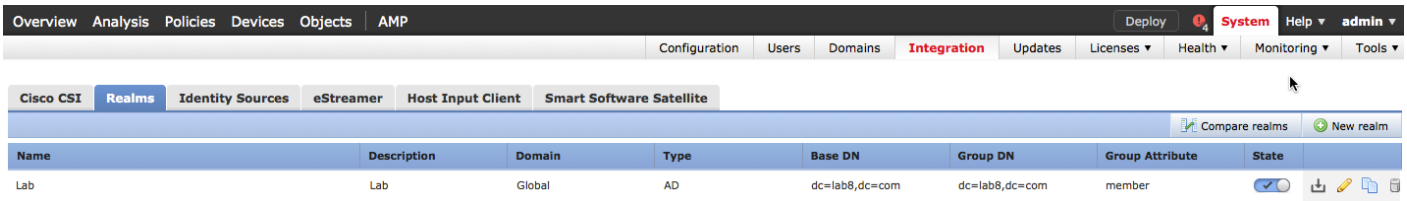
手順 10. [ユーザおよびグループのダウンロード（Download users and groups）] をオンにします。

手順 11. [使用可能なグループ（Available Groups）] をすべてハイライトし、[一覧に含める（Add to Include）] を選択します。



手順 12. [保存(Save)] を選択します。

手順 13. 次が表示されます。



Firepower Management Center 6.0 の設定

Firepower Management Center(FMC)は認証局(CA)署名証明書で動作するように設定されています。Firepower Management Center の秘密キーと CSR 要求は Firepower Management Center コンソール(FMC)から作成します。CA サーバは CSR 要求に署名し、カスタマイズされた pxGrid テンプレートを使用して、FMC 識別証明書を提供します。

FMC 証明書と FMC キーは両方とも FMC 内部証明書ストアにアップロードされます。CA ルート証明書は FMC 信頼 CA ストアにアップロードされます。

手順 1. Firepower 秘密キーを生成します。

注:ここで、パスワードは pxGrid エージェント設定で定義されます。

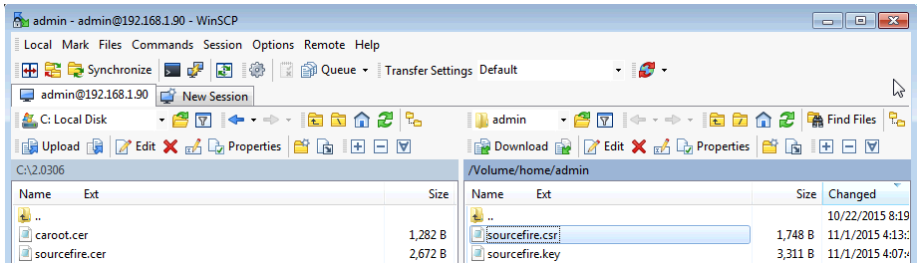
```
openssl genrsa -des3 -out sourcefire.key 4096
```

手順 2. CSR 要求を生成します。

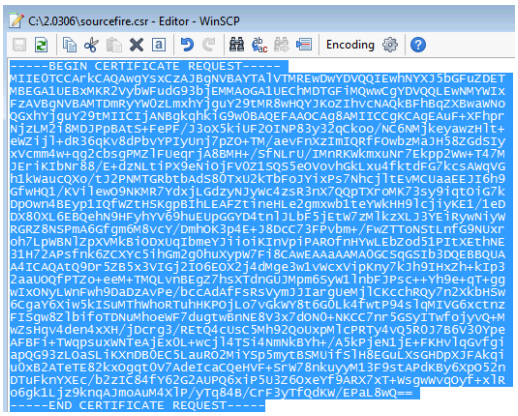
注:パスワードの入力が求められます。これは、以前入力したのものと同じパスワードです。

```
openssl req -new -key sourcefire.key -out sourcefire.csr
```

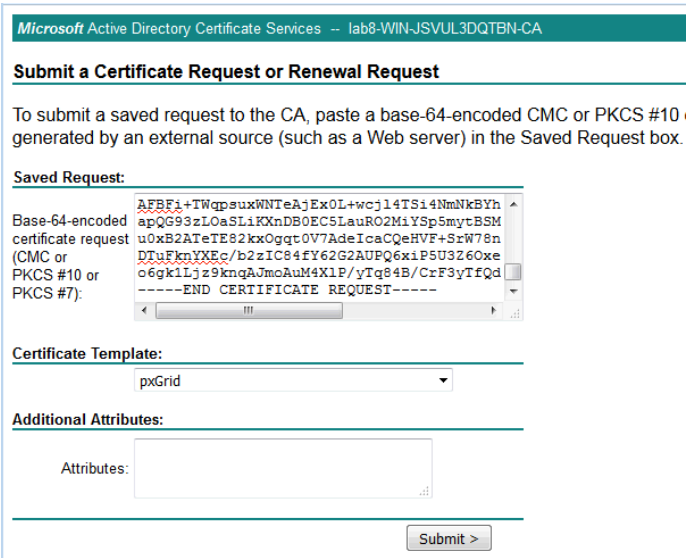
手順 3. WinSCP を使用して、Firepower Management Center(FMC)から sourcefire.csr ファイルと sourcefire.key ファイルをローカルの PC にコピーします。



手順 4. エディタを使用して CSR 要求を開き、CSR 要求をコピーします。

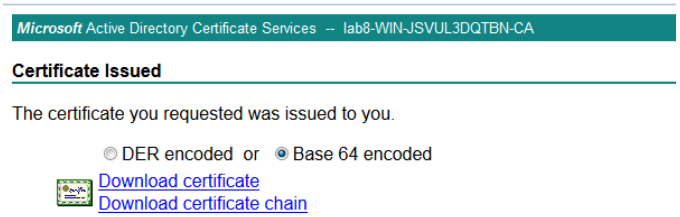


手順 5. カスタマイズした pxGrid テンプレートを使用し、[証明書の要求（Request a certificate）] -> [詳細ユーザ要求（Advanced User request）] を選択して、FMC CSR 要求を貼り付けた後、送信します。Base 64 符号化形式の証明書をダウンロードします。

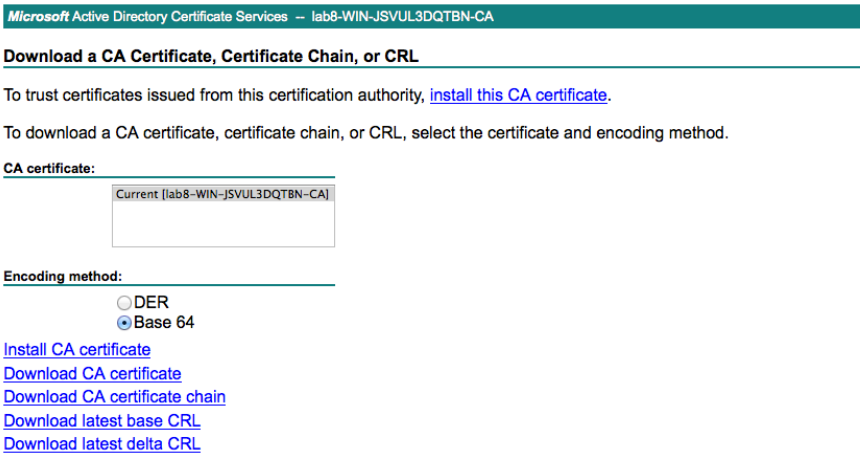


手順 6. [送信（Submit）] を選択します。

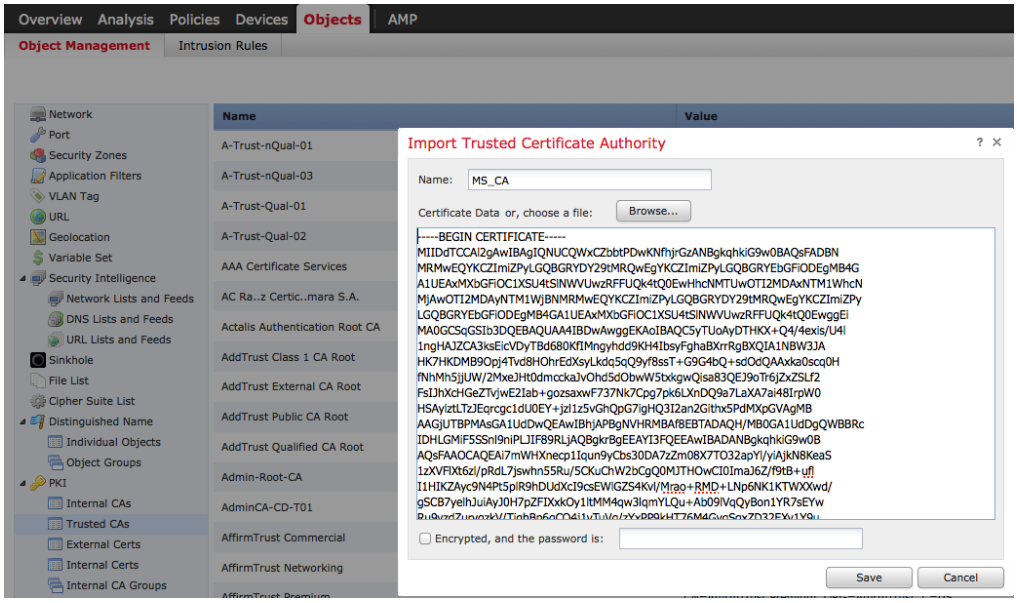
手順 7. [Base 64 形式（Base 64）] を選択して証明書をダウンロードします。



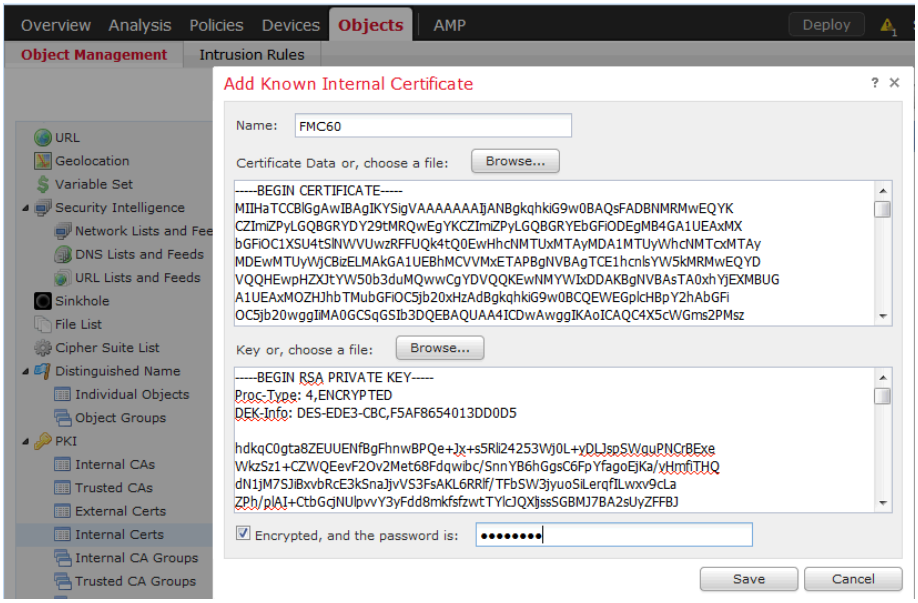
手順 8. Base 64 符号化形式の CA ルート証明書をダウンロードします。



手順 9. CA ルート証明書を Firepower Management 信頼 CA ストアにアップロードします。[オブジェクト(Objects)] > [PKI] > [信頼できる CA(Trusted CAs)] -> [信頼できる CA の追加(Add Trusted CA)] を選択し、名前を入力してルート CA 証明書をアップロードした後、[保存(Save)] を選択します。



手順 10. Firepower Management Center 公開証明書と秘密キーを FMC 内部証明書ストアにアップロードします。[オブジェクト(Objects)] > [PKI] > [内部証明書(Internal Certs)] を選択し、Sourcefire CER ファイルと Sourcefire KEY ファイルを追加した後、[保存(Save)] を選択します。



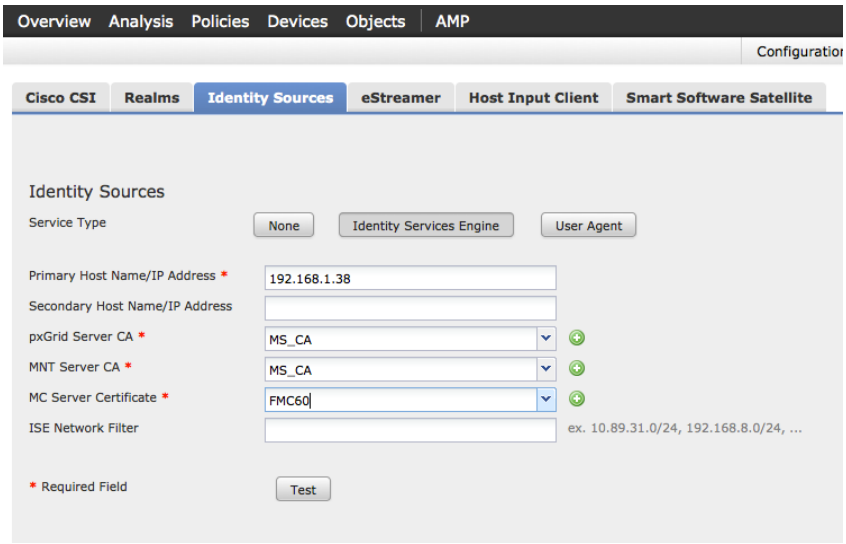
ISE ID ソース CA 署名付き証明書の設定

ID ソース エンジン設定では、ISE pxGrid ノード接続パラメータ、ISE MnT ノード証明書、FMC アイデンティティ証明書定義します。この設定は、ISE スタンドアロン環境における CA 署名付き環境用である点に注意してください。

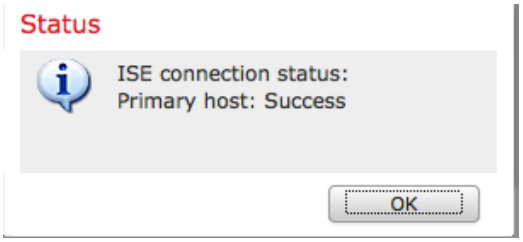
手順 1. [システム（System）] > [統合（Integration）] > [ID ソース（Identity Sources）] > [Identity Services Engine] を選択します。

[プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）]：プライマリ FQDN pxGrid 名または IP アドレス
[セカンダリ ホスト名/IP アドレス（Secondary Host Name/IP Address）]：セカンダリ FQDN pxGrid 名または IP アドレス
*[pxGrid サーバ CA（pxGrid Server Ca）]：ルート CA 署名付きの ISE pxGrid ノードと FMC の両方
*[mnt サーバ CA（pxGrid Server Ca）]：ルート CA 署名付きの ISE pxGrid ノードと FMC の両方
[MC サーバ証明書（MC Server Certificate）]：FMC の CA 署名付きアイデンティティ証明書

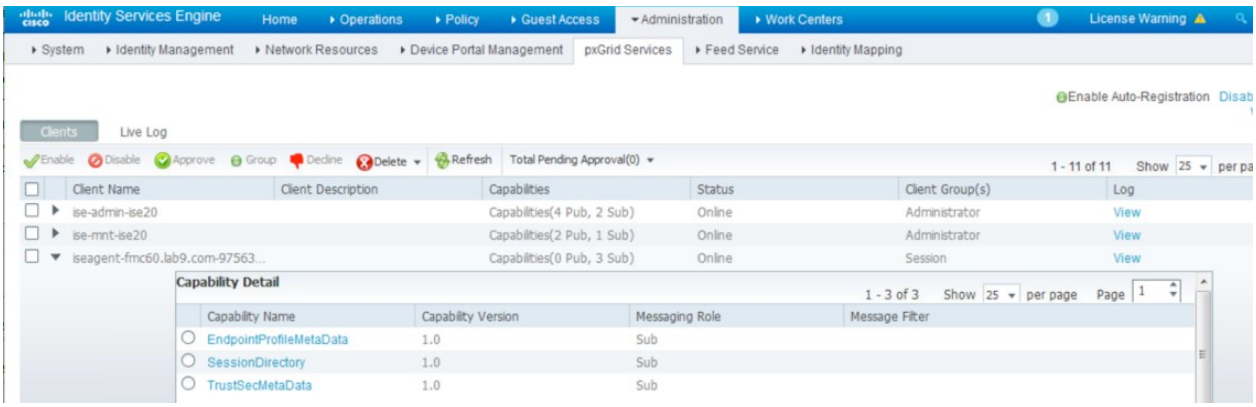
**CA 署名付き環境*



手順 2. [テスト(Test)] を選択します。
次のメッセージが表示されます。



手順 3. [保存(Save)] を選択します。
手順 4. ISE pxGrid ノードに次のように表示されます。
[管理(Administration)] > [pxGrid サービス(pxGrid Services)] を選択します。



FMC が ISE pxGrid ノードに正常に登録され、EndPointProfileMetada、SessionDirectory、TrustsecMetaData 機能にサブスクライブされました。

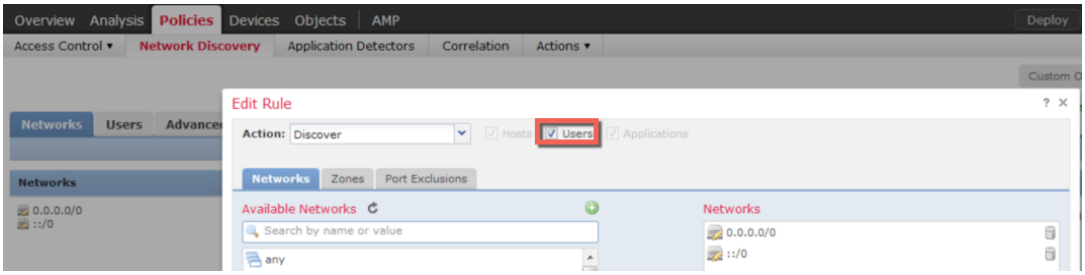
Firepower Management Center

ネットワーク検出の有効化

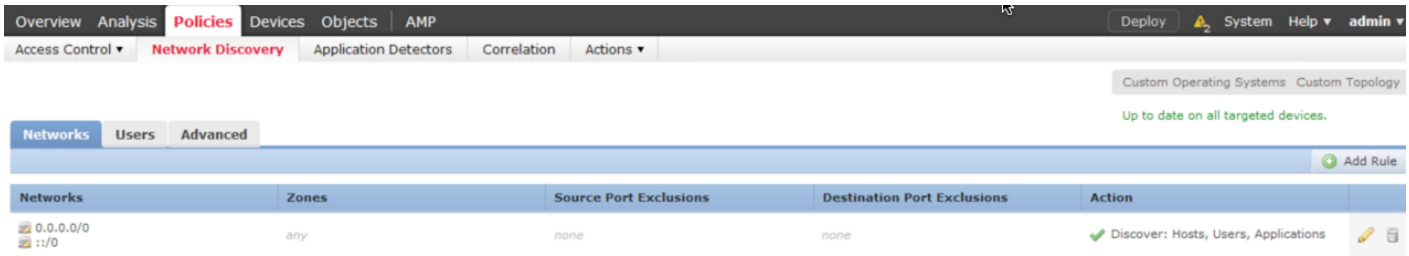
ネットワーク検出を有効にすると、ユーザ ID 情報が提供されます。

手順 1. [ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] を選択し、 をクリックして [ルールの編集(Edit Rule)] を開きます。

手順 2. [ユーザ(User)] をオンにします。



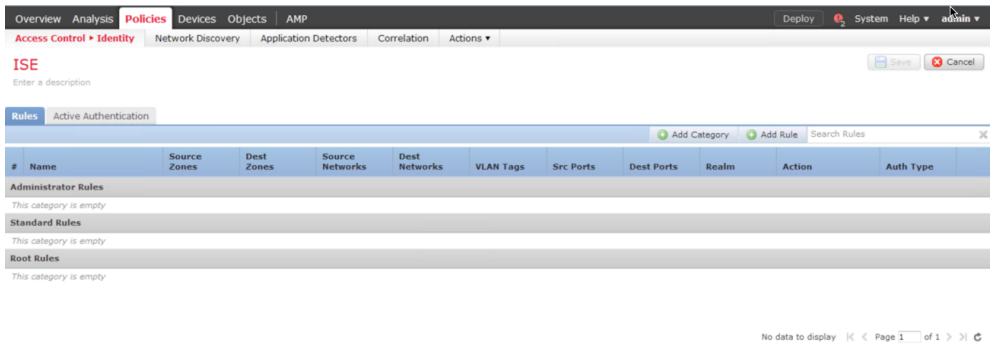
手順 3. [保存(Save)] を選択します。
次が表示されます。



ISE ID ポリシー

ISE ID ポリシーは、Firepower Management Center のデフォルトのアクセス制御ポリシーで、パッシブ ISE 認証を許可するために使用されます。

手順 1. [ポリシー(Policies)] > [アクセス制御(Access Control)] > [ID(Identity)] > [新規ポリシー(New Policy)] > [新規 ID ポリシー(New Identity Policy)] の順に選択し、名前を入力した後、[保存(Save)] を選択します。
次が表示されます。

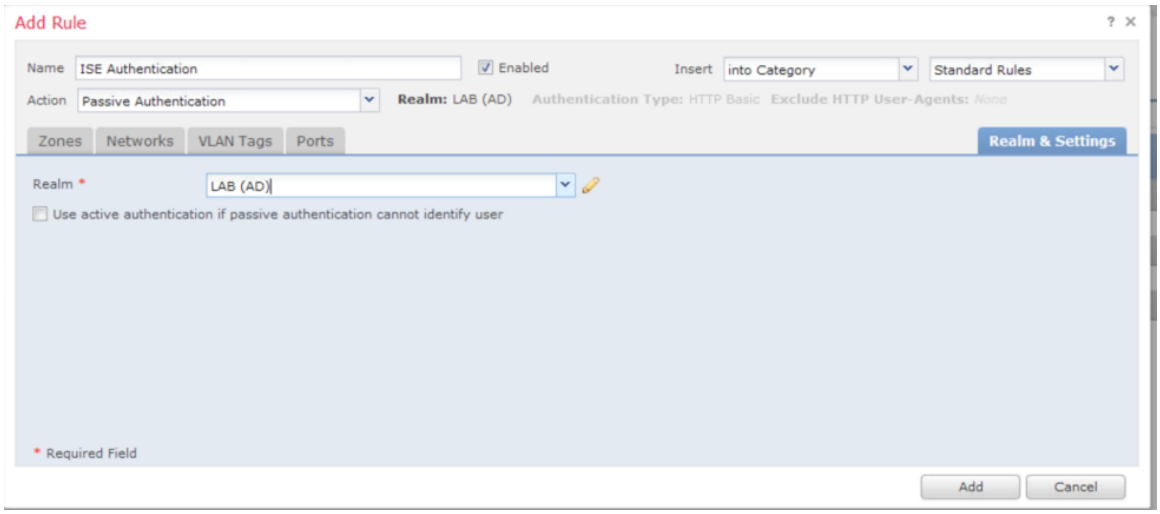


手順 2. [ルールの追加(Add Rule)] を選択します。

手順 3. [名前(Name)] に **ISE Authentication** と入力します。

手順 4. [アクション(Action)] で [パッシブ認証(Passive Authentication)] を選択します。

手順 5. [レルム(Realm)] を選択後、[追加(Add)] を選択して、先に定義した ISE レルムを選択します。次のように表示されます。



手順 6. 変更を [保存(Save)] します。

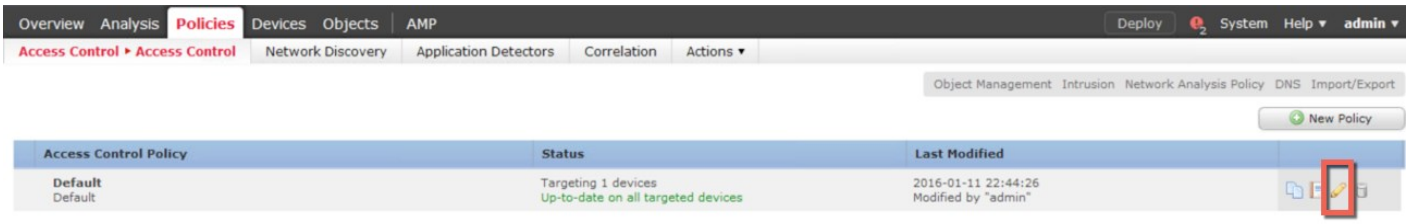
デフォルトのアクセス制御ポリシー

デフォルトのアクセス制御ポリシーには、ISE ID ポリシー、トランザクションをブロックするためのトランスポート層/ネットワーク層のプリプロセッサ設定、アクセス制御ルール、Firepower Management Center の侵入ポリシーが含まれます。

ISE ID ポリシーの追加

ISE ID ポリシーをデフォルトのアクセス ポリシーに追加します。

手順 1. [ポリシー(Policies)] > [アクセス制御(Access Control)] を選択し、デフォルトのアクセス ポリシーを編集します。



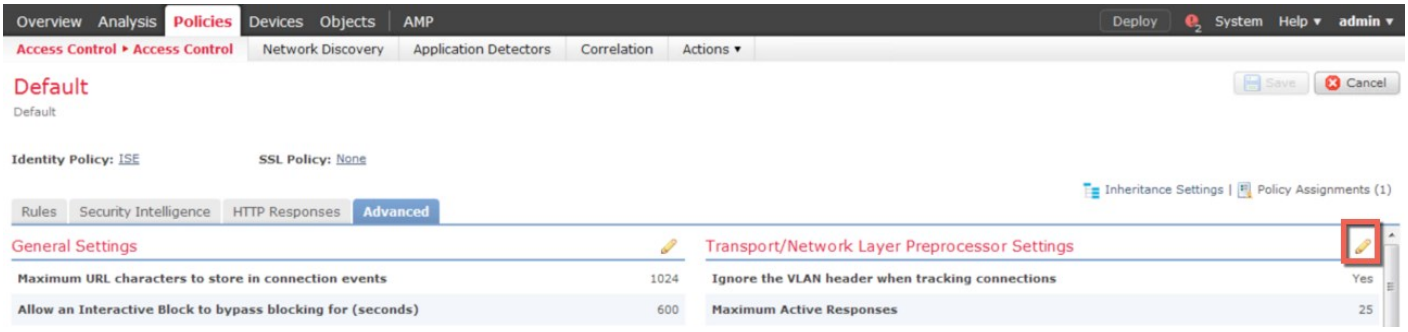
手順 2. [なし(None)] > [ID ポリシー(Identity Policy)] の順にクリックし、ドロップダウン メニューから ISE を選択します。

手順 3. [保存(Save)] を選択します。

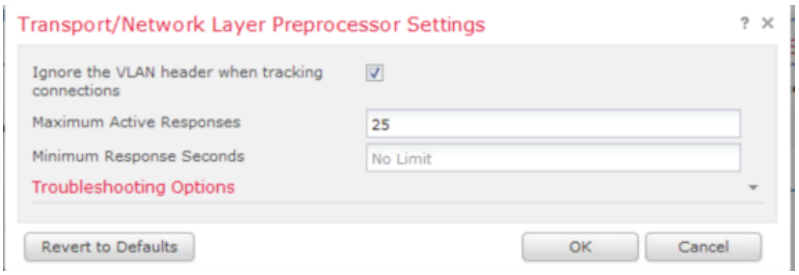
トランスポート層とネットワーク層のプリプロセッサの設定

これらの設定は、Firepower 管理対象侵入ポリシーによってトラフィックがブロックされるように変更されています。

手順 1. トランスポート層/ネットワーク層のプリプロセッサ設定を編集します。



手順 2. 次のように設定します。

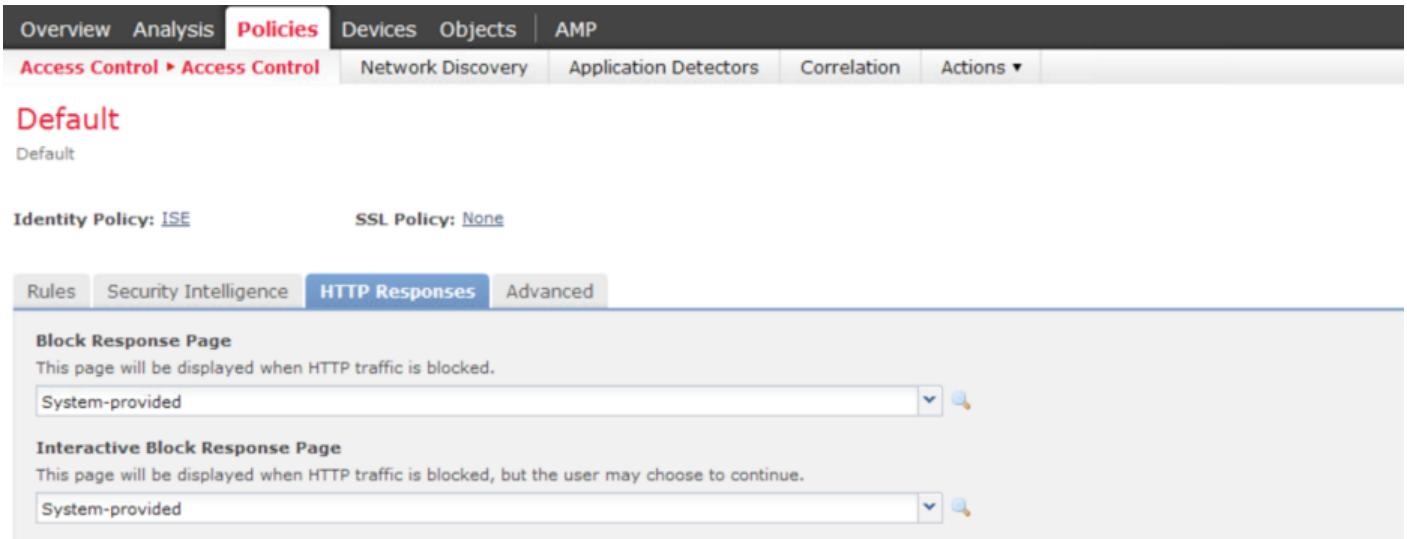


手順 3. [OK] を選択します。

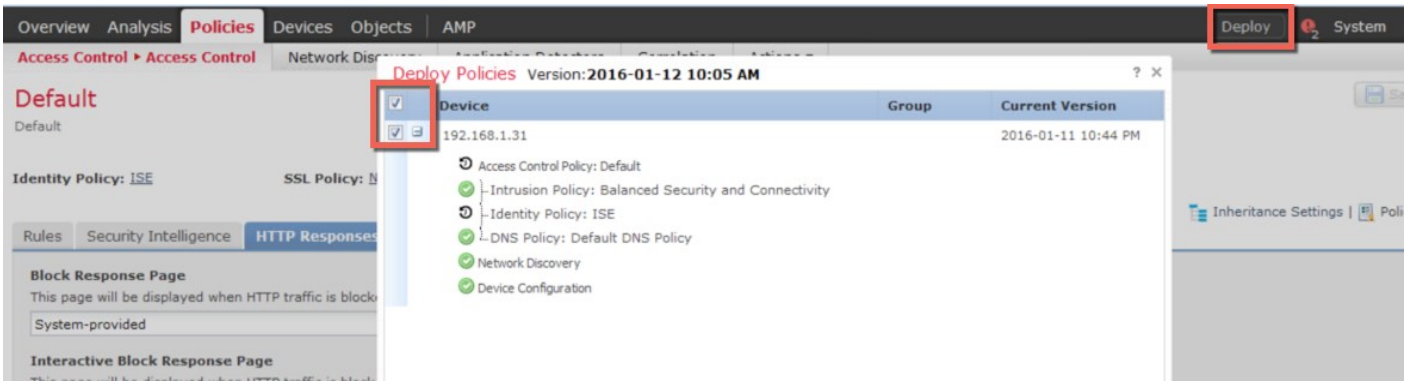
ブロック応答ページの追加

Firepower Management Center のアクセス制御ポリシーに基づいてブロックされた Web カテゴリに、システムで提供されるブロック応答ページを追加します。

手順 1. [HTTP 応答（HTTP Responses）] を選択し、応答ページ設定として次のように入力します。



手順 2. 変更を [保存（Save）] します。
手順 3. [導入（Deploy）] を選択し、変更内容をセンサーに**導入**します。



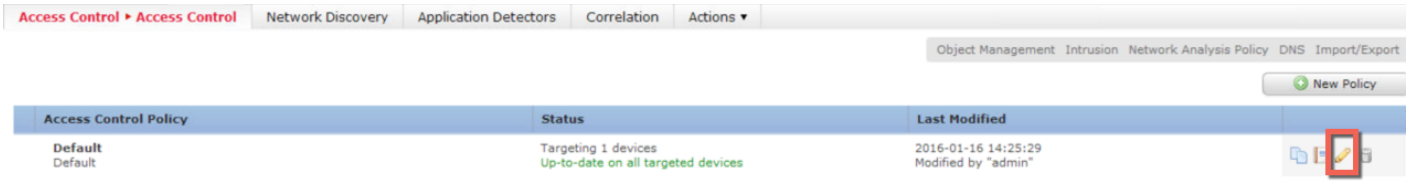
手順 4. 導入ステータス バーを選択して進捗を確認します。

Employee SGT タグ アクセス制御ルールの作成

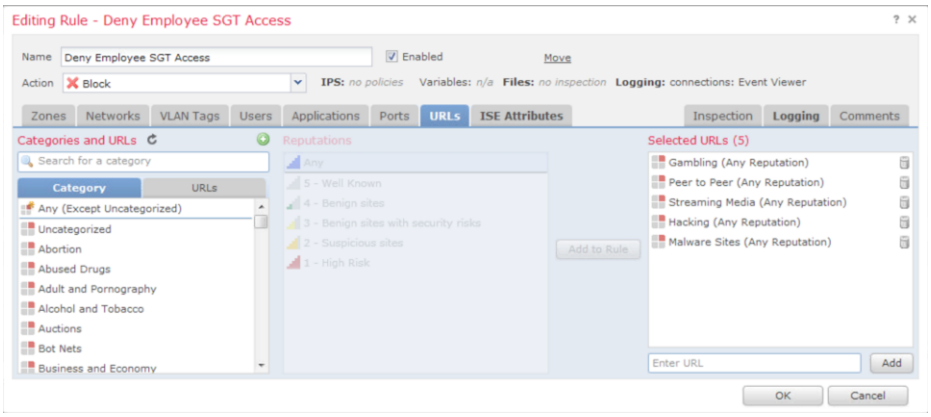
組織のアクセプタブル ユース ポリシーをシミュレートする Employee SGT アクセス制御ポリシーを作成します。

このアクセプタブル ユース ポリシーは、ギャンブル サイト、ハッキング サイト、ストリーミング メディア、ソーシャル メディア、ピアツーピア アプリケーションへのユーザ アクセスを拒否します。

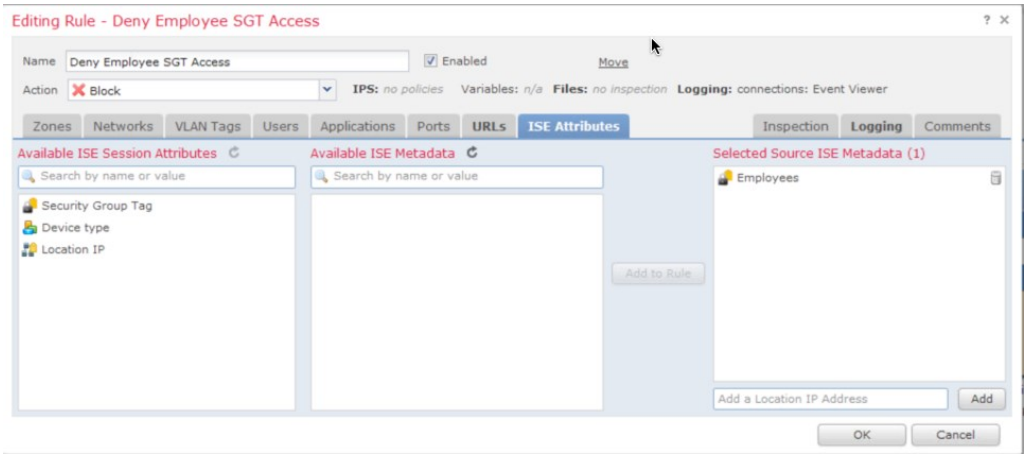
手順 1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] > [ルール（Rules）] を選択し、 をクリックして編集します。



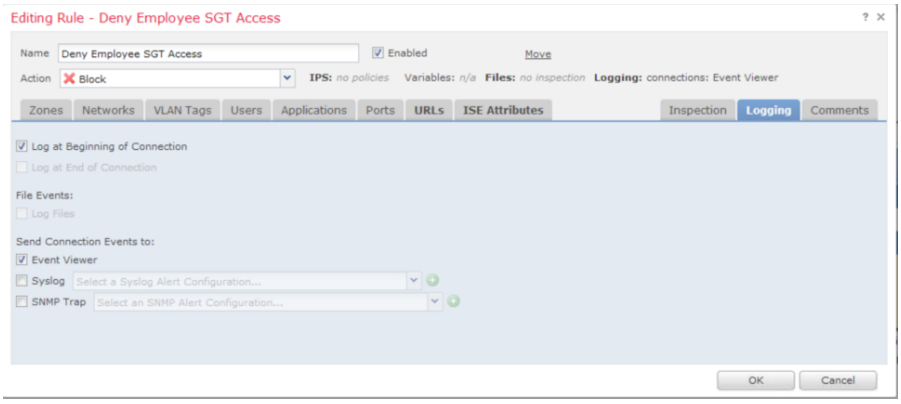
手順 2. [ルールの追加（Add Rule）] を選択し、[名前（Name）]に Deny Employee SGT Access と入力して、[アクション（Action）] で [ブロック（Block）]、[IPS] で [pxGrid 侵入ポリシー（pxGrid intrusion policy）] を選択します。次に [URLs] > [カテゴリ（Category）] を選択して、[ギャンブル（Gambling）、[ピアツーピア（Peer-to-Peer）]、[ストリーミング ビデオ（Streaming Video）]、[ハッキング（Hacking）] を指定し、[ルールに追加（Add to Rule）] を選択します。



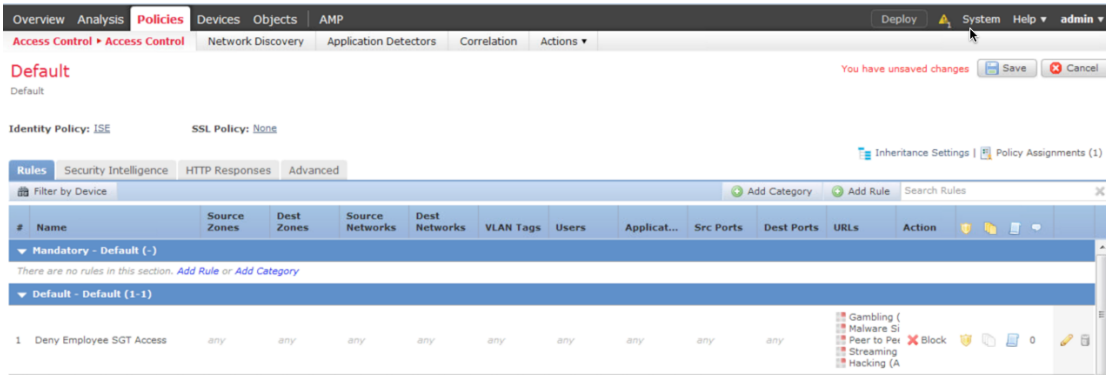
手順 3. [ISE 属性（ISE Attributes）] > [利用可能な ISE セッション属性（Available ISE session attributes）] > [セキュリティ グループ タグ（Security Group Tag）] > [利用可能な ISE メタデータ（Available ISE Metadata）] を選択し、Employees を指定して、[ルールに追加（Add to Rule）] を選択します。



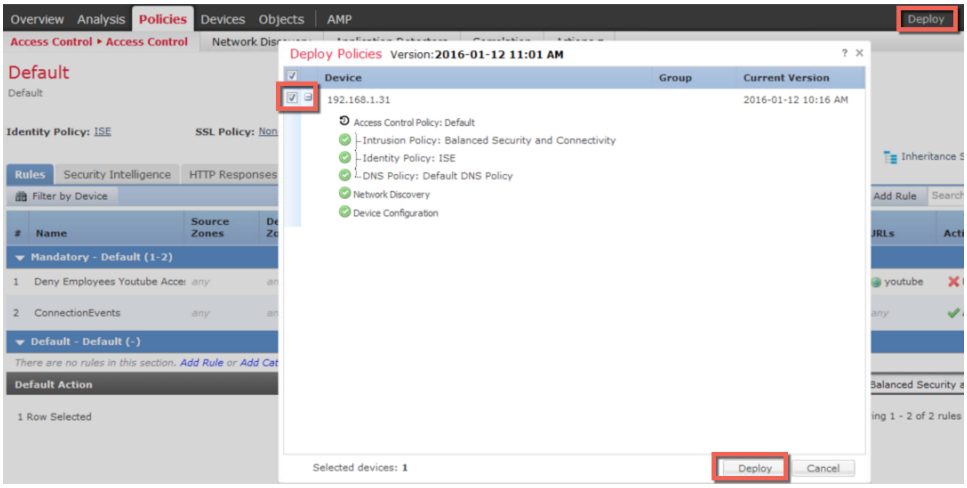
手順 4. [ロギング（Logging）] を選択し、次のように設定します。



手順 5. [OK] を選択します。
次が表示されます。



手順 6. [保存(Save)] を選択します。
手順 7. 変更内容をセンサーに導入します。
[導入(Deploy)] を選択後、センサーを指定して [導入(Deploy)] をクリックします。



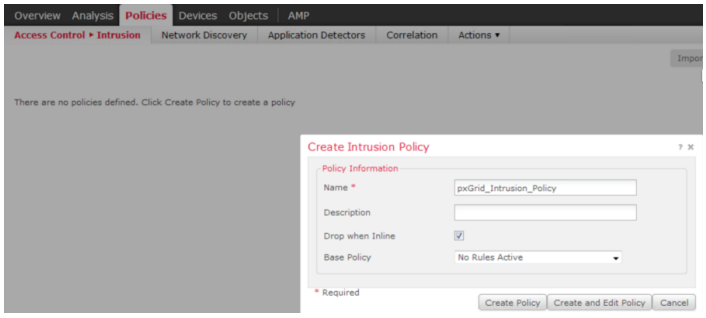
手順 8. をクリックするとタスクのステータスが表示されます。操作が完了したことを確認します。

Firepower pxGrid 侵入ポリシー

pxGrid 侵入ポリシーを作成し、Firepower NGIPS 仮想センサーに導入します。このポリシーには、「SERVER IIS CMD.EXE access」ルールが含まれており、エンドユーザがブラウザに www.yahoo.com/cmd.exe と入力すると、侵入イベントがトリガーされてインライン時にドロップされ、Firepower Management Console の [侵入イベント分析(Analysis Intrusion Events)] にイベントが生成されます。このドキュメントでは、pxGrid 侵入ポリシーにより、ASA with Firepower サービスも集中管理します。

また、このドキュメントでは、ASDM および ASA with Firepower サービスを使用してこのポリシーがオンボックスで作成されます。

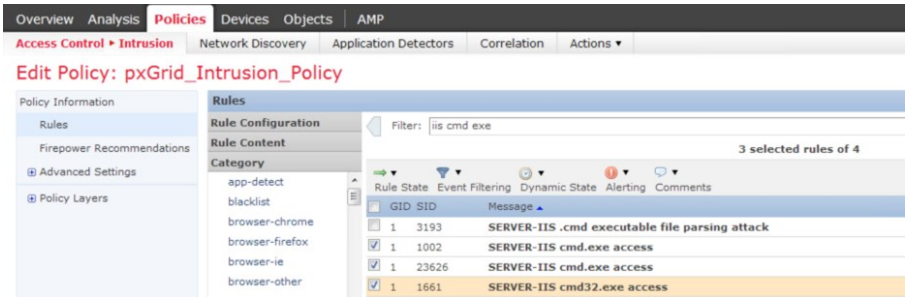
手順 1. [ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] > [ポリシーの作成（Create Policy）] の順に選択し、pxGrid_Intrusion_Policy と入力して、[インライン時にドロップ（Drop when Inline）] をオンにします。



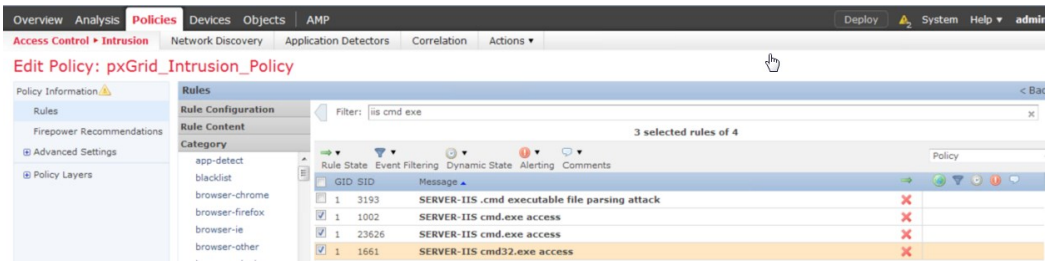
手順 2. [ポリシーの作成（Create Policy）] をクリックします。

手順 3. をクリックして、ポリシーを編集します。

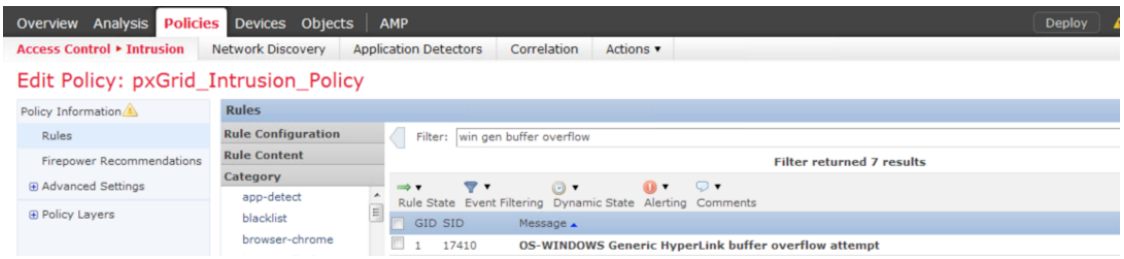
手順 4. [ルール（Rules）] を選択し、[フィルタ（Filter）] に **iis cmd exe** と入力して、次のように選択します。



手順 5. [ルールの状態（Rule State）] > [イベントのドロップと生成（Drop and Generate Events）] > [OK] の順にクリックします。
次が表示されます。

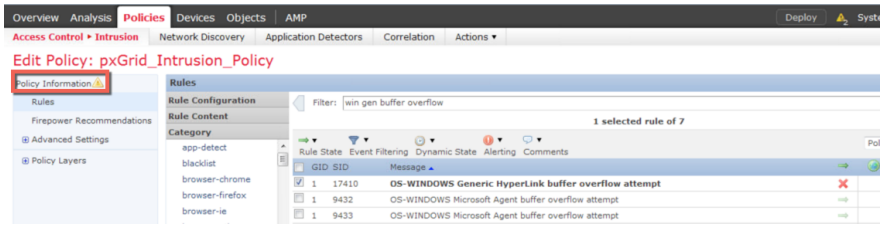


手順 6. 次に [フィルタ（Filter）] に **win gen buffer overflow** と入力して、[OS-Windows Generic Hyperlink BufferOverflow Attempt] を選択します。

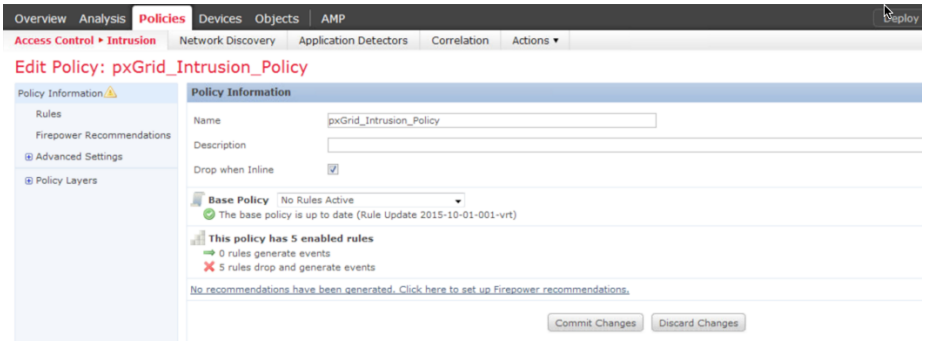


手順 7. [ルールの状態（Rule State）] > [イベントのドロップと生成（Drop and Generate Events）] > [OK] の順にクリックします。

手順 8. [ポリシー情報（Policy Information）] をクリックします。

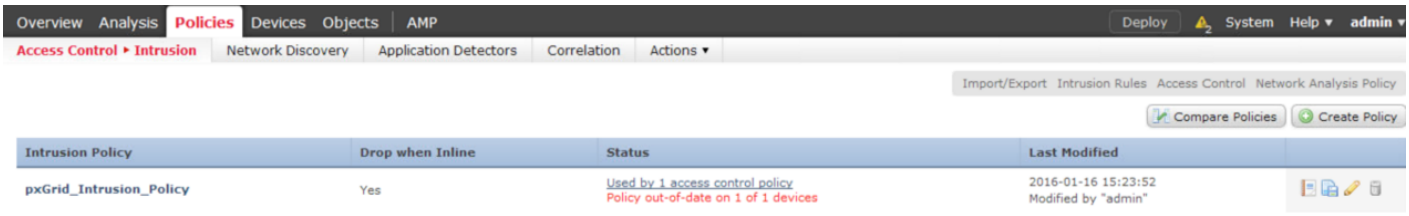


手順 9. 次が表示されます。



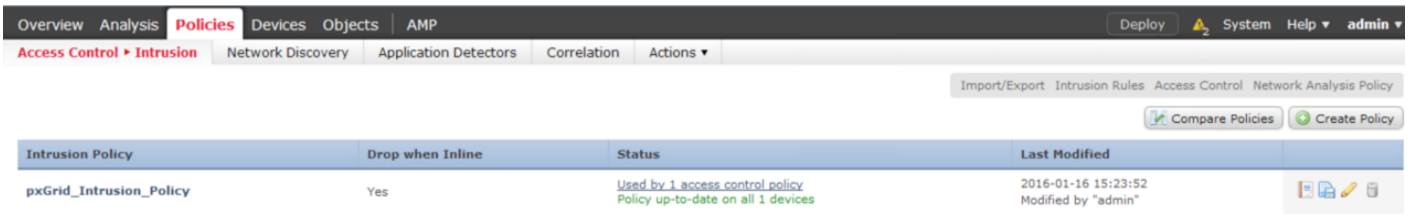
手順 10. [変更を確定（Commit Changes）] を選択します。

手順 11. [OK] をクリックします。
次が表示されます。

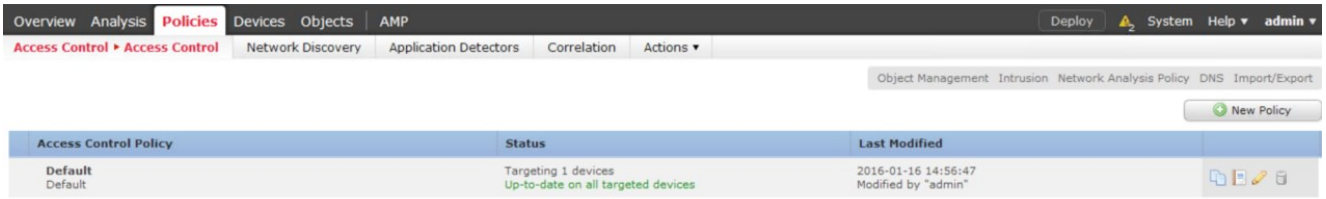


手順 12. [導入（Deploy）] > [センサー（sensor）] > [導入（Deploy）] を再度選択します。

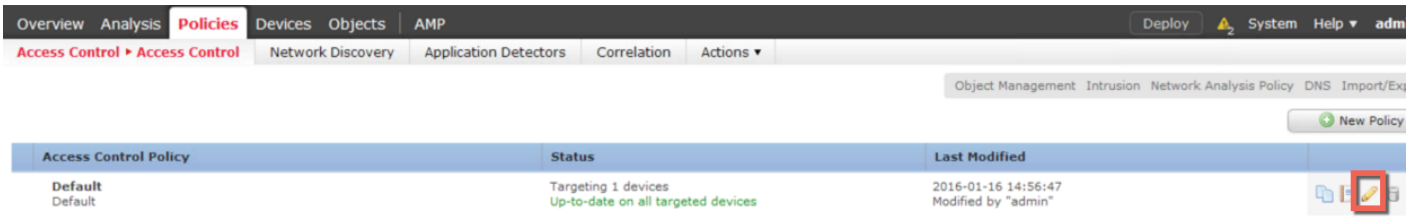
手順 13. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [侵入アクセス制御（Intrusion Access Control）] の順に選択します。次のように表示されます。



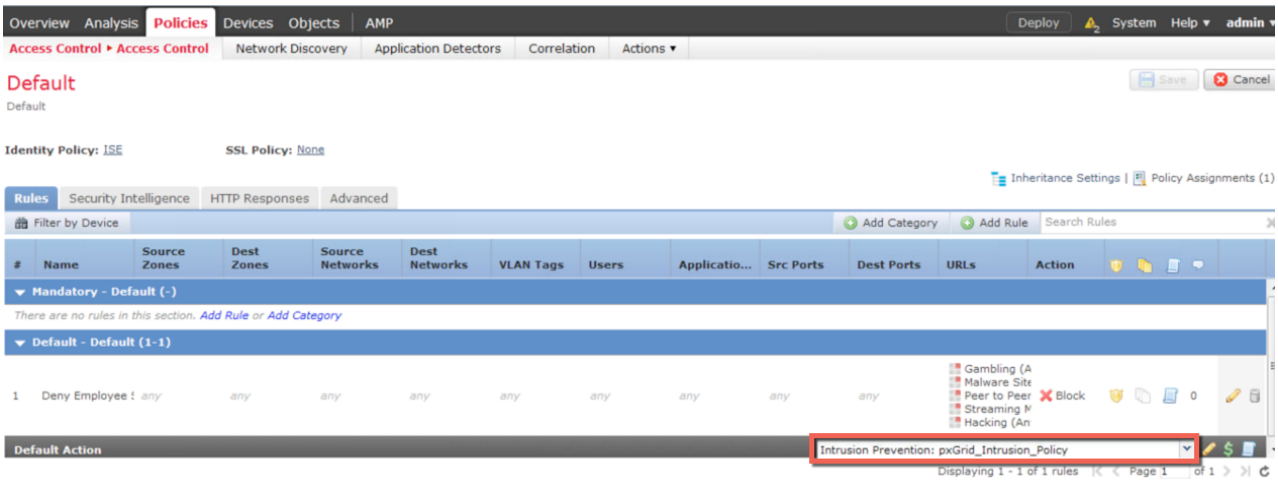
手順 14. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] を選択します。
デフォルトのアクセス ポリシーが表示されます。



手順 15. をクリックして、デフォルトのアクセス ポリシーを編集します。



手順 16. [デフォルトのアクション（Default actions）] で、ドロップダウンから [pxGrid_Intrusion_Policy] を選択します。
次が表示されます。



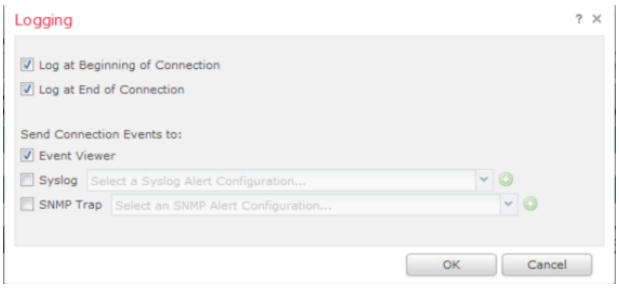
注：アクセス制御ポリシーの追加が求められることがあります。これらは、Employee SGT に基づいて後で追加されます。

手順 17. [保存（Save）] をクリックします。

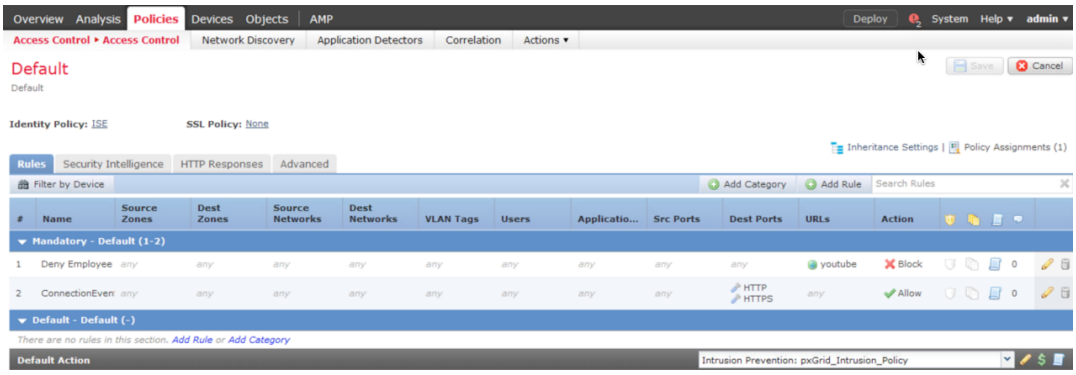
手順 18. SGT アクセス制御ポリシーを編集して、pxGrid 侵入ポリシーを含めます。

手順 19. （[ロギング（Logging）]）をクリックします。

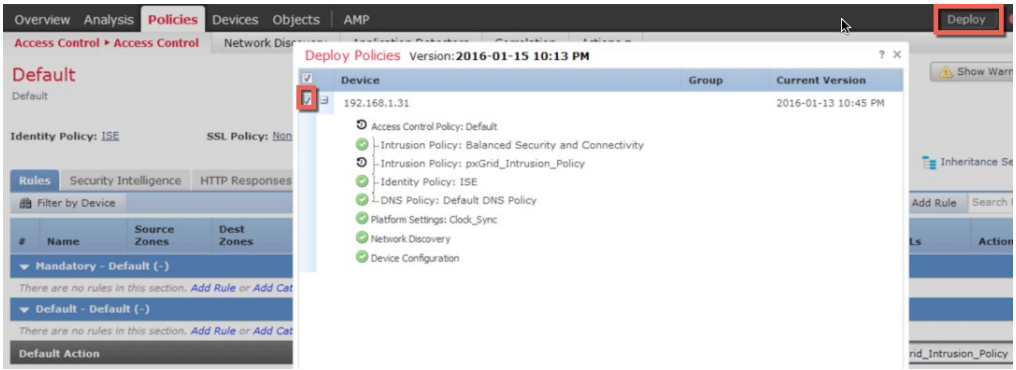
手順 20. 次のように設定し、[OK] をクリックします。



手順 21. [保存（Save）] をクリックします。



手順 22. [導入（Deploy）] をクリックして、デバイスを選択します。

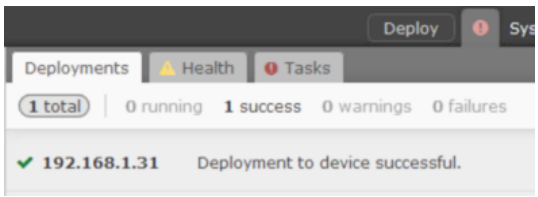


手順 23. [導入（Deploy）] を選択します。

手順 24. をクリックして、タスクのステータスを表示します。

注：タスク ステータスをクリックすると、導入サイクル ステータスが表示されます。

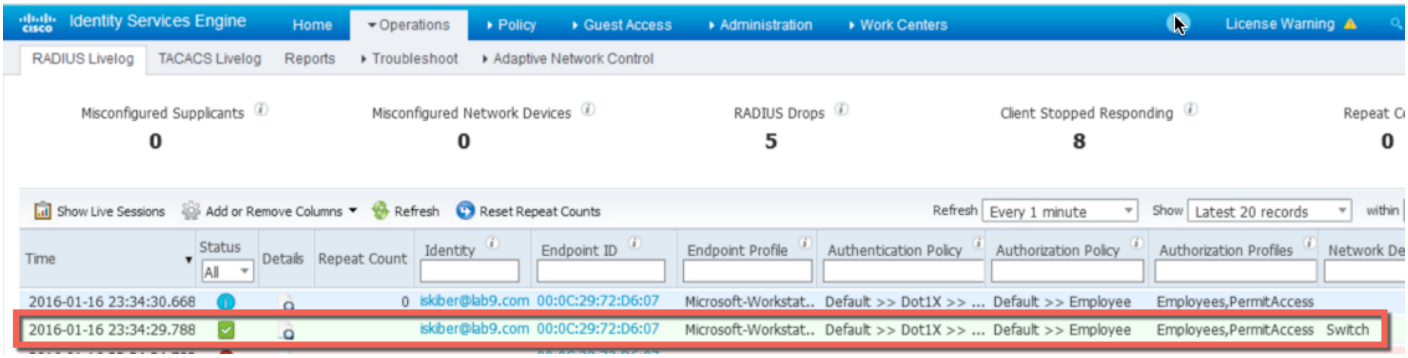
センサーへの導入が成功したことが示されます。



Firepower 仮想センサーによる Employee SGT ユーザのテスト

この使用例では、エンドユーザに Employee SGT が割り当てられ、Firepower Management Center のアクセス制御ポリシーが適用されることにより、ハッキング サイト、ギャンブル サイト、ピアツーピア アプリケーション、ストリーミング メディア アプリケーションへの SGT タグ付き従業員のアクセスが拒否されます。また、侵入ポリシーが実行され、セキュリティ侵害された Web サーバへのアクセスも拒否されます。

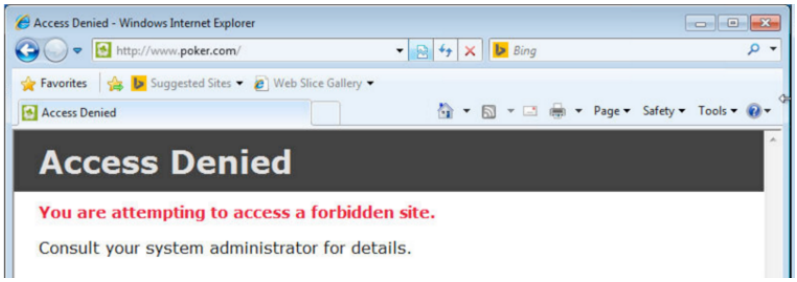
IEEE 802.1x によって正常に認証されたエンドユーザには、次に示すように、Employee SGT が割り当てられます。



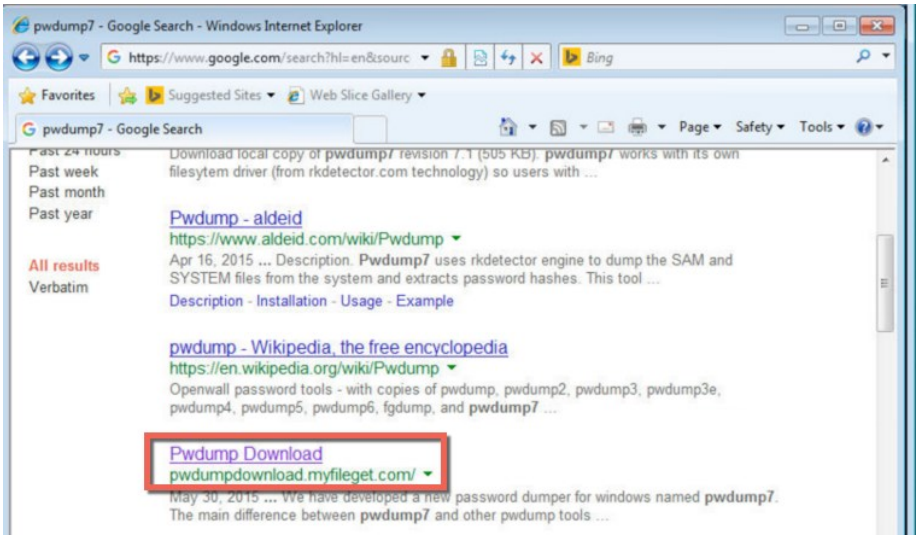
Firepower Management Center 6.0 は、ISE セッション情報を取得し、[ユーザ アクティビティ(User Activity)] 画面に情報を表示します

ISE セッション属性(ユーザ名、セキュリティ グループ タグ、エンドポイント プロファイル、エンドポイント ロケーション)を確認します。セキュリティ グループ タグの属性は、FMC アクセス制御ポリシーの作成に使用されています。

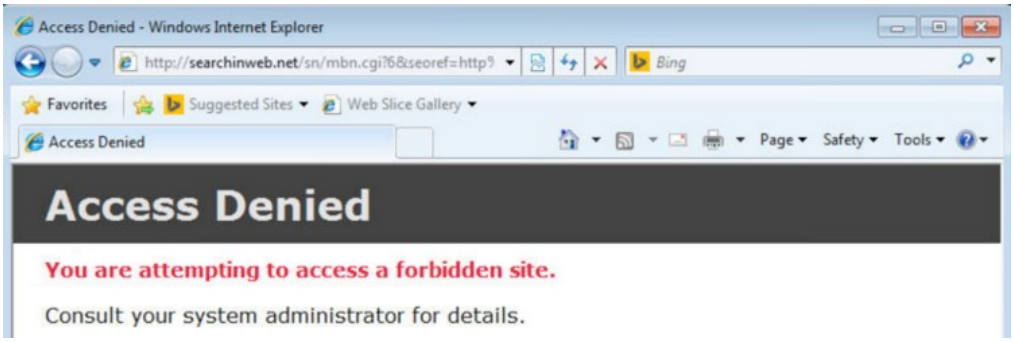
エンドユーザがブラウザを開き、poker.com にアクセスします。ブロックされたトランザクションおよび Firepower Management Center に表示されたページを確認します。



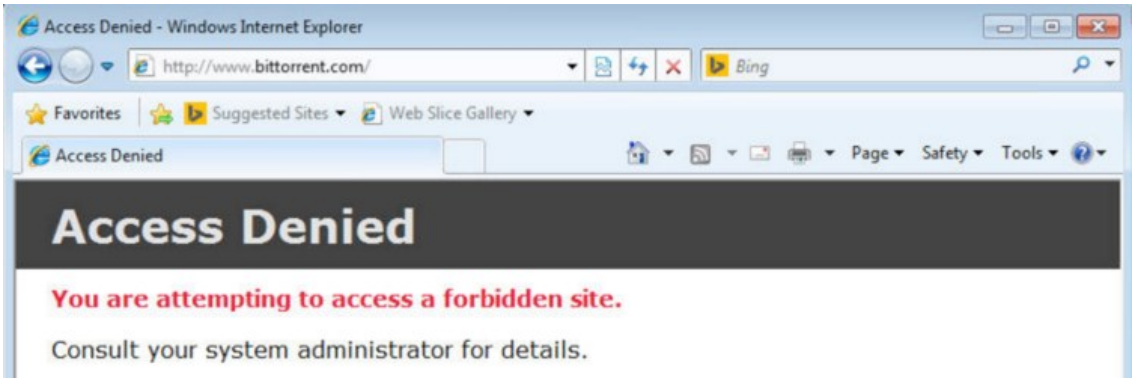
エンドユーザがブラウザを開き、pwdump7 のダウンロードを試みます。



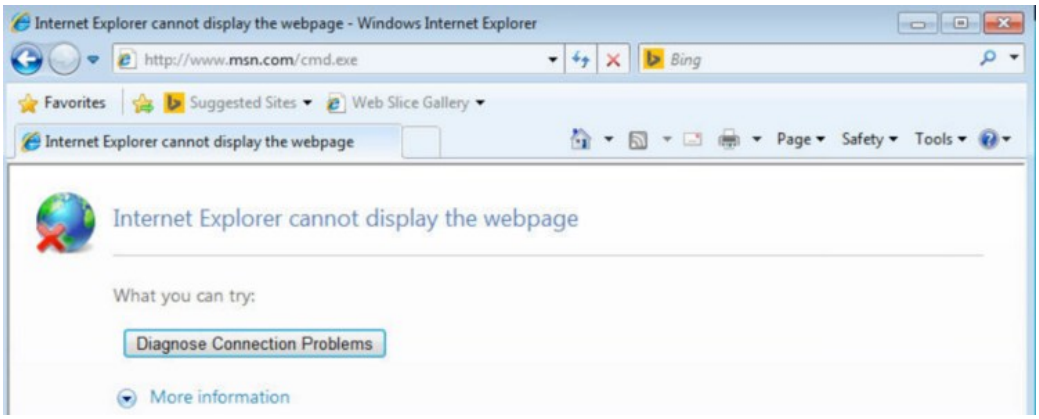
エンドユーザは、Web ページにリダイレクトされ、アクセスが拒否されます。



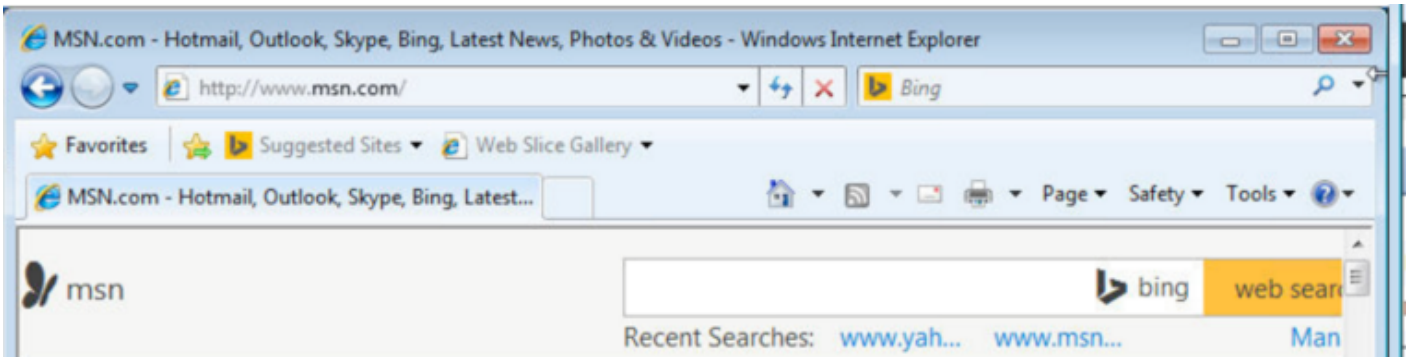
エンドユーザが bittorrent へのアクセスを試み、アクセスが拒否されます。



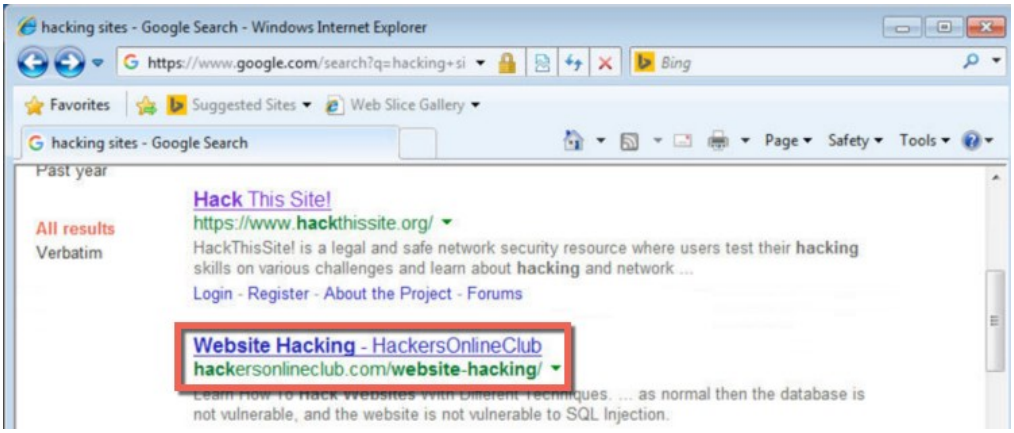
エンドユーザが Web サイトに cmd.exe を挿入してセキュリティ侵害された Web サーバをシミュレートし、アクセスが拒否されます。



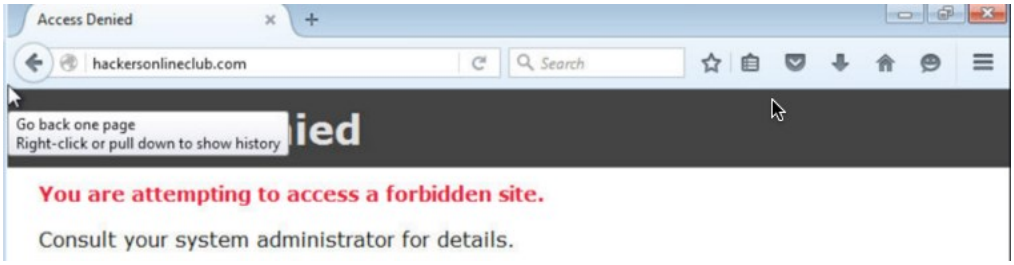
すべてが良好に動作していることがわかります。エンドユーザは有効な Web サイトにはアクセスできます。



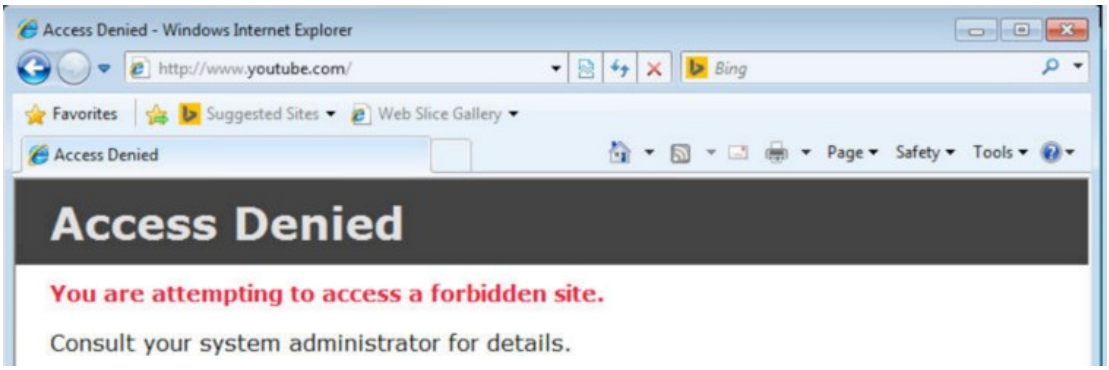
エンドユーザがハッキング クラブに参加を試み、アクセスが拒否されます。



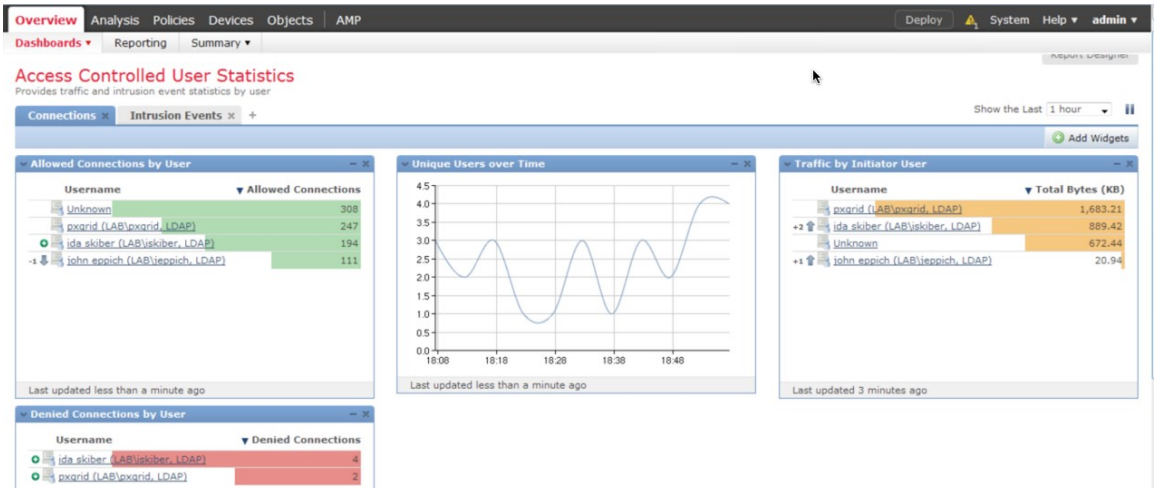
エンドユーザがハッキング クラブへの参加を試みようとすると、そのアクセスが拒否されます。



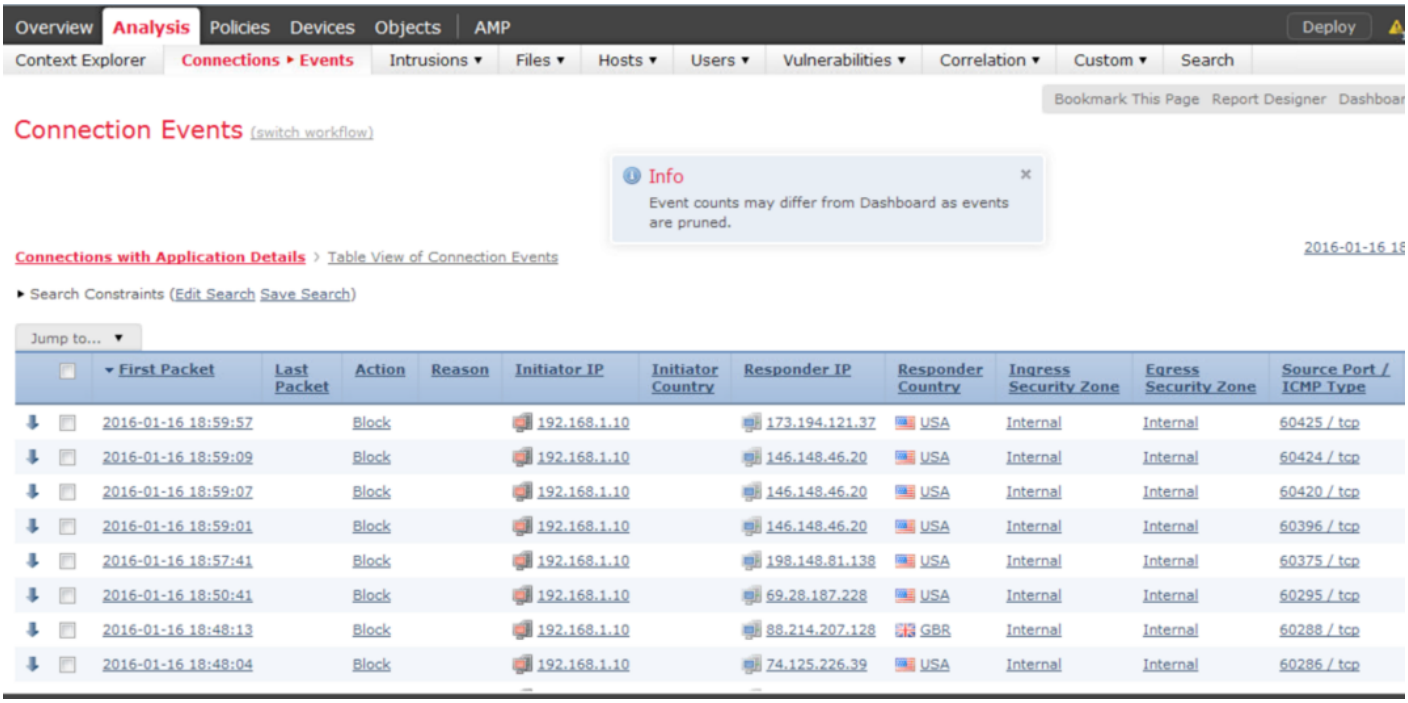
エンドユーザが www.youtube.com へのアクセスを試みようとすると、そのアクセスが拒否されます。



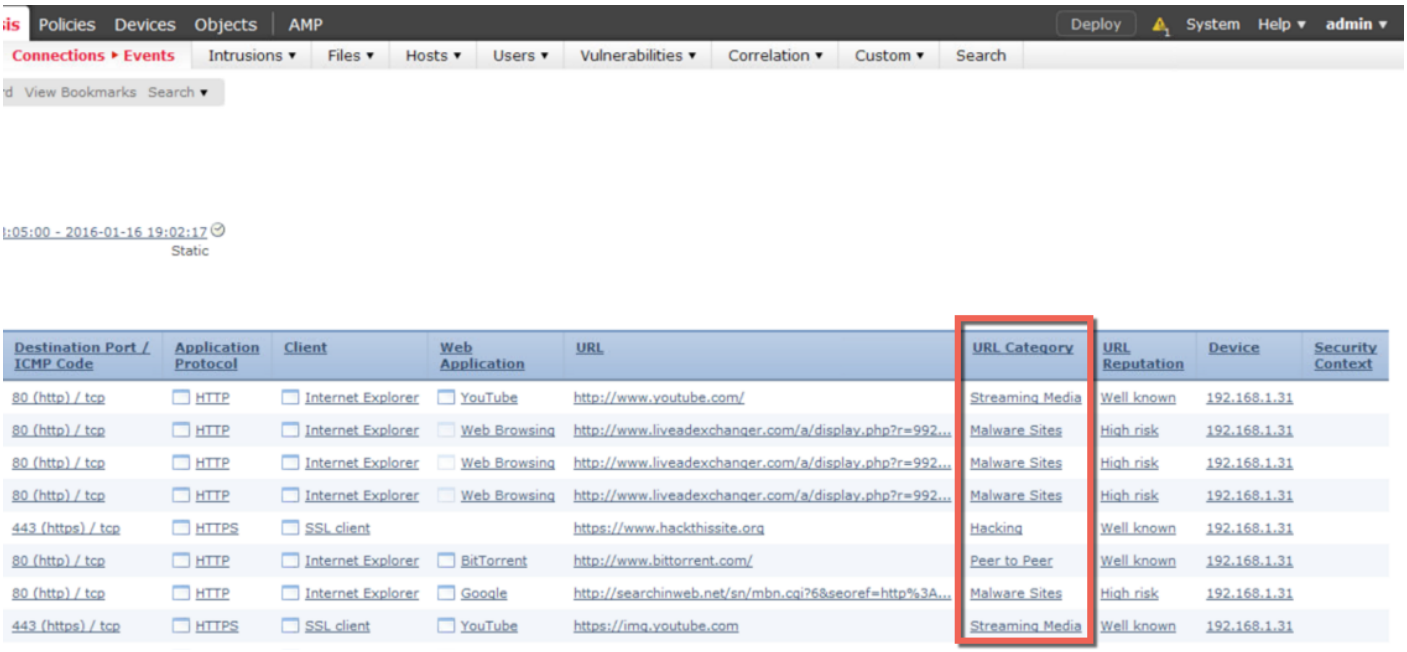
Firepower Management Center アクセス制御ユーザ統計情報ダッシュボードでは、ユーザ iskiber からの拒否された接続を確認できます。



iskiber の拒否された接続をクリックすると、拒否された URL カテゴリが表示されます。これらの拒否されたカテゴリは、Firepower Management Center アクセス制御ルール「Deny Employee SGT Access」で定義された URL カテゴリを表します。



以下に、画面の続きを示します。



Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device	Security Context
80 (http) / tcp	HTTP	Internet Explorer	YouTube	http://www.youtube.com/	Streaming Media	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
443 (https) / tcp	HTTPS	SSL client		https://www.hackthissite.org	Hacking	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	BitTorrent	http://www.bittorrent.com/	Peer to Peer	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Google	http://searchinweb.net/sn/mbn.cgi?6&seoref=http%3A...	Malware Sites	High risk	192.168.1.31	
443 (https) / tcp	HTTPS	SSL client	YouTube	https://img.youtube.com	Streaming Media	Well known	192.168.1.31	

ASA with Firepower サービス

このドキュメントでは、ASA 5506W をテストに使用しています。ASA Firepower（sfr）モジュールをインストールし、以下に関してテストしました。

- 管理対象 Firepower pxGrid 侵入ポリシーと Employee SGT アクセス制御ルール
- オンボックス管理対象 Firepower pxGrid 侵入ポリシーと Employee SGT アクセス制御ルール

集中型 Firepower Management Center ポリシーの使用

ここでは、ASA Firepower（sfr）モジュールをインストールします。設定が完了したら、Firepower Management Console に ASA を登録します。そこで、管理対象の Cisco Firepower ポリシーを ASA が実行します。

注: 管理対象 ASA with Firepower サービスのスマート ライセンスまたはクラシック ライセンスを必ずインストールしてください。

ASA Firepower（sfr）のインストールと Firepower Management Center への登録

手順 1. ASDM 7.5.2 および ASA 9.5.2 をダウンロードし、それらを ASA アップロードします。
手順 2. ASA Firepower モジュールをインストールします。

```
ciscoasa# sw-module module sfr recover configure image disk0:/asasfr-5500x-6.0.0.img
```

手順 3. デバッグをオンにします。エラー メッセージが発生した場合のデバッグが容易になります。

```
ciscoasa# sh debug
ciscoasa# debug module
```

手順 4. ASA Firepower ブート イメージをロードします。

```
ciscoasa# sw-module module module sfr recover boot
```

手順 5. ASA Firepower モジュールが起動するまで約 5 ～ 15 分待ってから、現在実行中の ASA Firepower ブート イメージへのコンソール セッションを開きます。Enter キーを数回押して、以下のように入力します。

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr.Escape character sequence is ‘CTRL_^X’.

Cisco ASA SFR Boot Image 5.3.1
asasfr login:admin
Password: Admin123
```

手順 6. システム インストール コマンドを使用してソフトウェア システム イメージをインストールします。次の例では ftp が使用されています。

```
asa-boot>system install http://jeppich:password@192.168.1.8/asasfr-5500x-6.0.0.img
```

終了したら、システムのシャットダウンと再起動が実行されます。sfr が起動するまでしばらく時間がかかります。ASA 5506 の場合と同様に 30 分以上かかることもあります。次のように入力して確認します。

```
sh module sfr
```

モジュールが起動中と表示されます。モジュールがまだ回復状態の場合、モジュールは引き続きインストール中です。

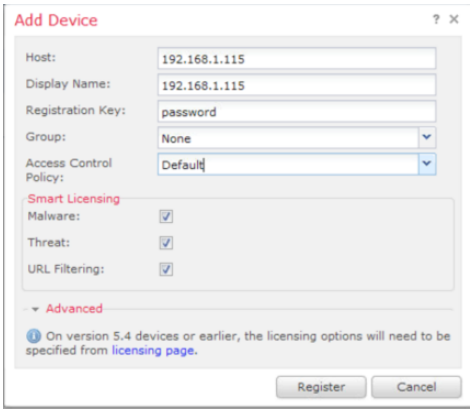
手順 7. ASA Firepower モジュールへのセッションを開きます。

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL- ^X'.

Sourcefire3D login: admin
Password: Admin123
```

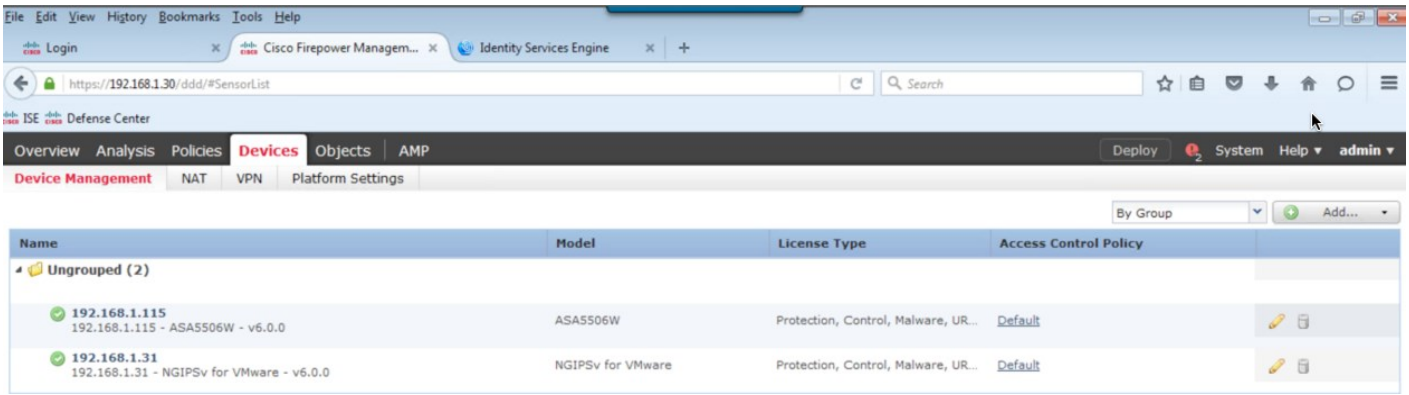
手順 8. EULA を確認して同意し、システム設定を完了します。
手順 9. ASA Firepower サービスを Firepower Management 6.0 に追加します。

```
> configure manager add (ip address of Cisco Firepower Management Console) password
```

手順 10. ASA の適切なライセンスがインストールされていることを確認します。
手順 11. ASA Firepower デバイスを Firepower Management Center 6.0 に追加し、デバイス情報を入力した後、ライセンスを有効化します。
[デバイス(Devices)] > [デバイス管理(Device Management)] > [追加(Add)] > [デバイスの追加(Add Device)] を選択します。

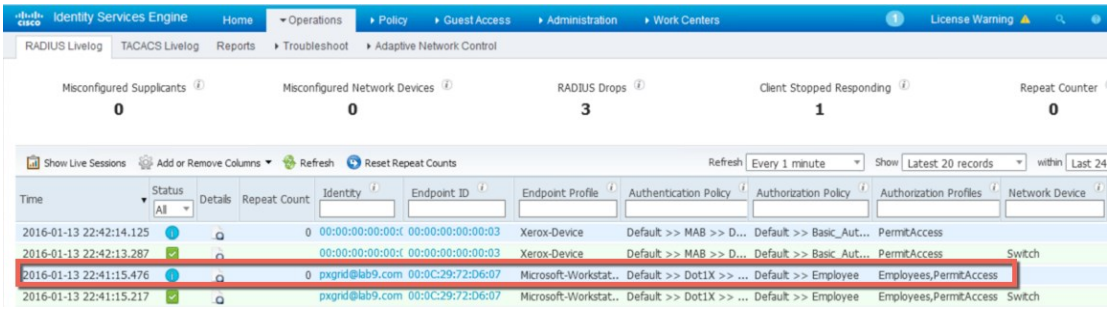


手順 12. [登録(Register)] を選択します。
手順 13. ASA Firepower の登録が完了すると次のようになります。

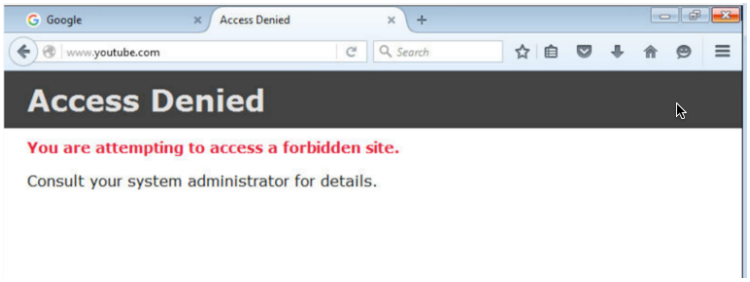


管理対象 Firepower Management ポリシーからの Employee SGT ユーザのテスト

ここでは、従業員としてタグ付けされたエンドユーザ用に作成した FMC 6.0 ポリシーをテストします。エンドユーザは、ISE 認可ポリシーに基づいて 802.1x 認証された後、Employee SGT がタグ付けされます。

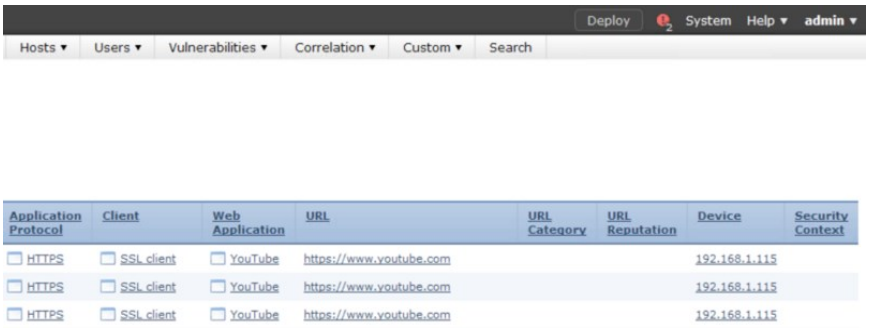


エンドユーザがブラウザを開き、www.youtube.com にアクセスすると、アクセスが拒否されます。

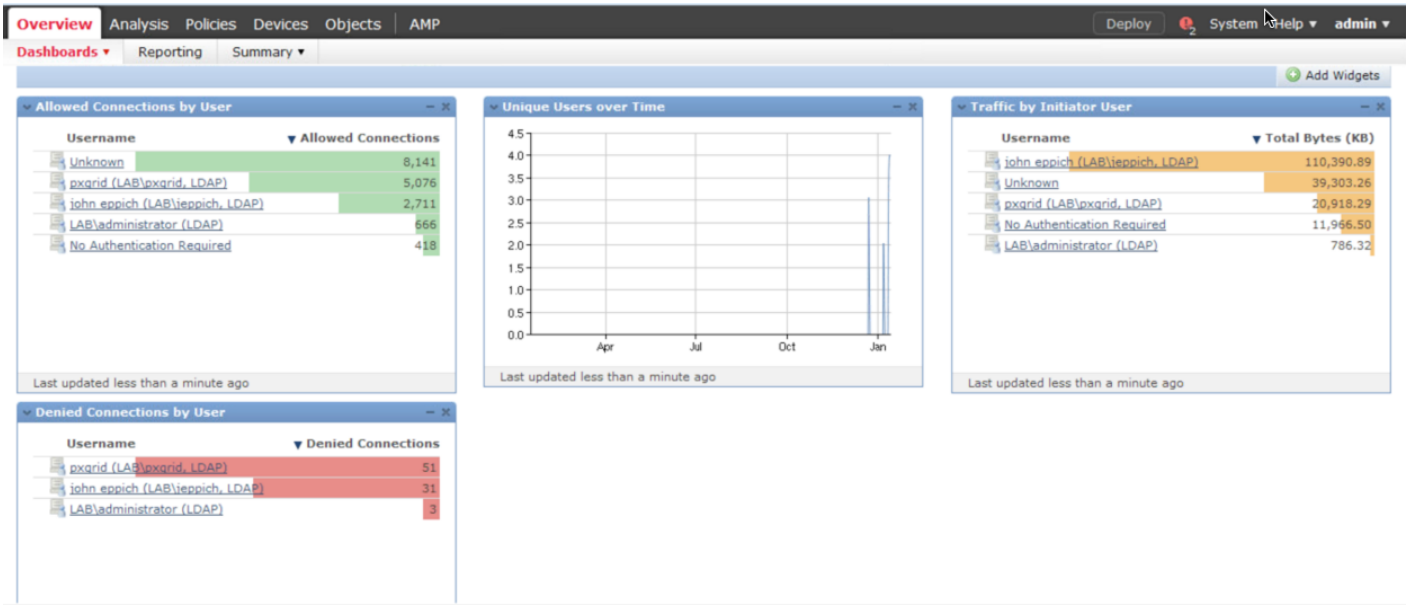


Firepower Management Center で [分析(Analysis)] > [接続(Connection)] > [イベント(Events)] を選択し、ブロックされたトランザクションの詳細を確認します。

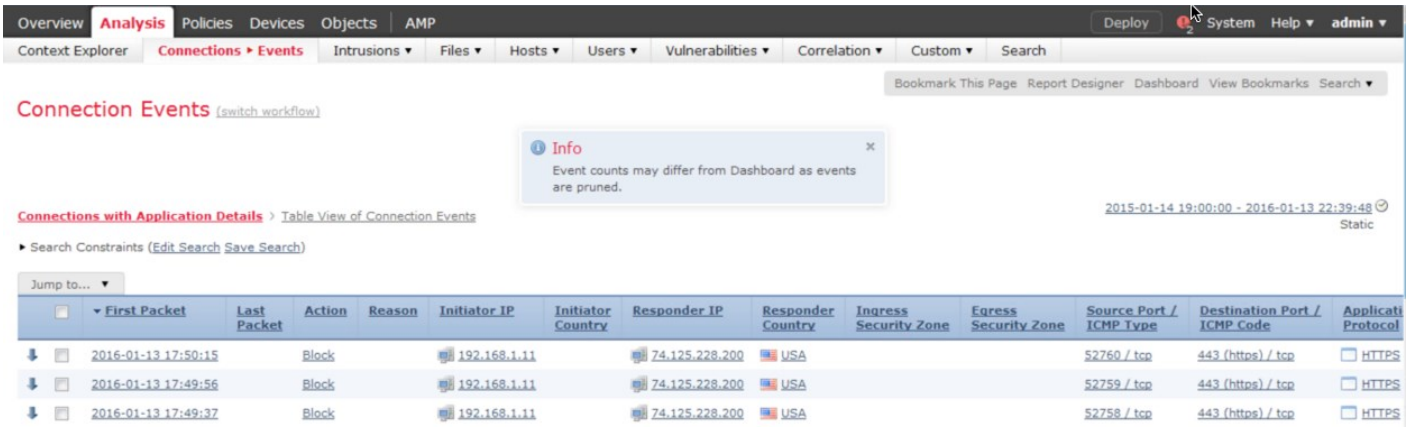
以下の画面の続きに www.youtube.com が表示されているのがわかります。



Firepower Management Center で [概要（Overview）] > [ダッシュボード（Dashboards）] > [アクセス制御されたユーザ統計情報（Access Controlled User Statistics）] を選択し、pxGrid に対する [ユーザ別の拒否された接続（Denied Connections by User）] をクリックします。



www.youtube.com に対してブロックされた接続イベントが表示されます。



オンボックス Firepower ポリシー管理

この項では、ASDM 経由の ASA with Firepower サービスのオンボックス管理に関する詳細について説明します。ただし、ASDM 経由で Firepower ポリシーを使用するオンボックス ASA のライセンスが別に必要になる点に注意してください。また、ASA with Firepower サービスは CA 署名付き環境用に設定されています。

Firepower Management Center 6.0 から ASA を削除

手順 1. ASA5500 デバイスを Firepower Management Center 6.0 から削除します。

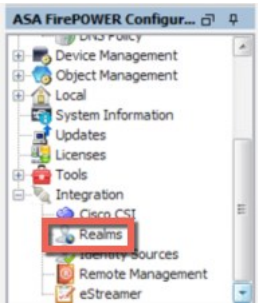
[デバイス(Devices)] > [デバイス管理(Devices Management)] を選択し、 をクリックして ASA 5500 センサーを削除します。

注:ASA デバイスが FMC 6.0 から削除されていない場合、ASDM は ASA Firepower 設定の詳細を確認することができません。これには、オンボックス登録に関する別のライセンス セットが必要です。

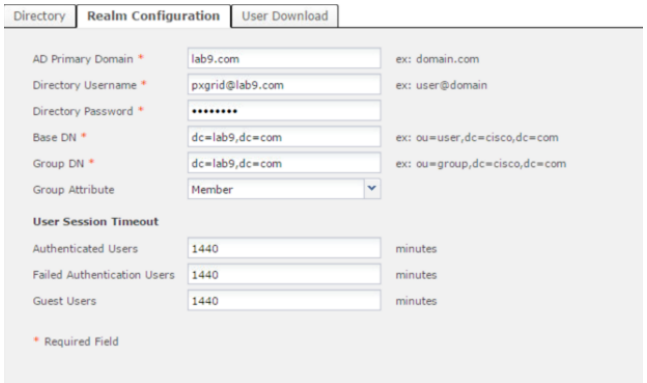
ISE レルム設定

ここでは、ISE 上で ISE レルムを設定します。

手順 1. [ASA Firepower 設定(ASA Firepower Configuration)] > [レルム(Realms)] を選択します。

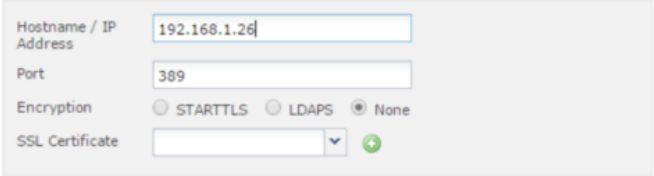


手順 2. [新規レルム(New Realm)] を選択し、レルム設定の詳細を入力します。



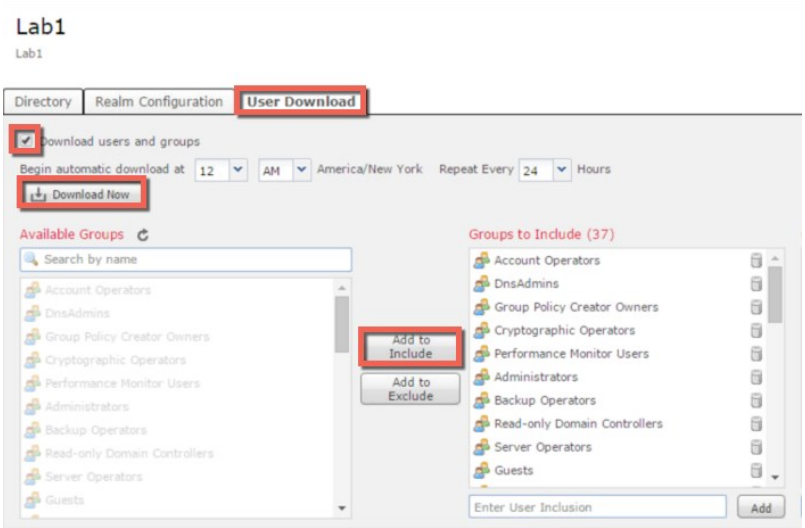
手順 3. [OK] を選択し、[状態(State)] をクリックしてレルムを有効化します。

手順 4. [ディレクトリの追加(Add Directory)] を選択し、以下の情報を入力します。



手順 5. [テスト(Test)] を選択し、操作が成功したことを確認します。

手順 6. [ユーザのダウンロード(User Download)] をクリックし、[ユーザおよびグループのダウンロード(Download users and groups)] をオンにした後、[今すぐダウンロードする(Download Now)] > [一覧に含める(Add to Include)] を選択します。

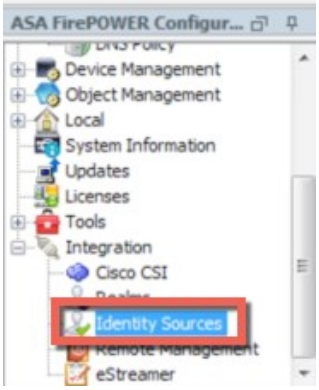


手順 7. [ASA Firepower の変更の保存(Store ASA Firepower Changes)] をクリックします。

ISE ID ソースの設定

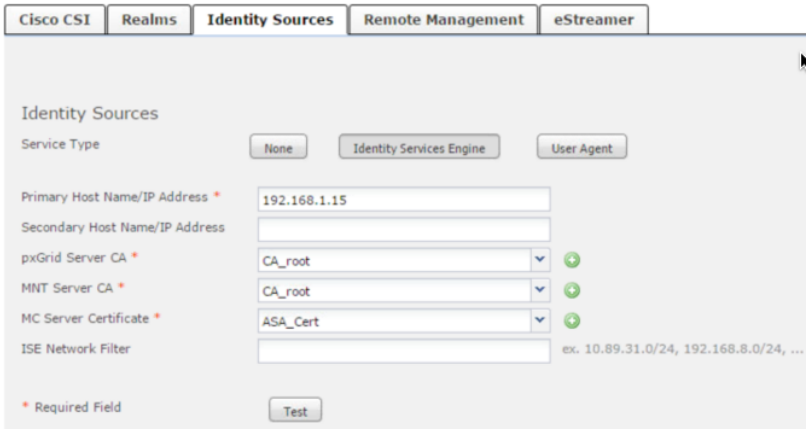
ID ソースの設定には、ASA with Firepower サービスと ISE pxGrid ノードの間の接続パラメータが含まれます。ASA に CA 署名付き証明書があることを確認してください。証明書のインストールに精通していない場合は、CA 署名の操作を参照してください。

手順 1. [ASA Firepower 設定の変更（ASA Firepower Configuration Changes）] > [ID ソース（Identity Sources）] の順に選択します。

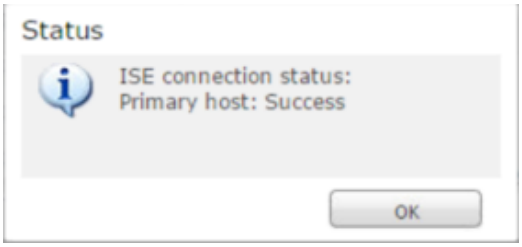


手順 2. [Identity Services Engine] を選択し、以下のように ISE pxGrid 設定を入力します。

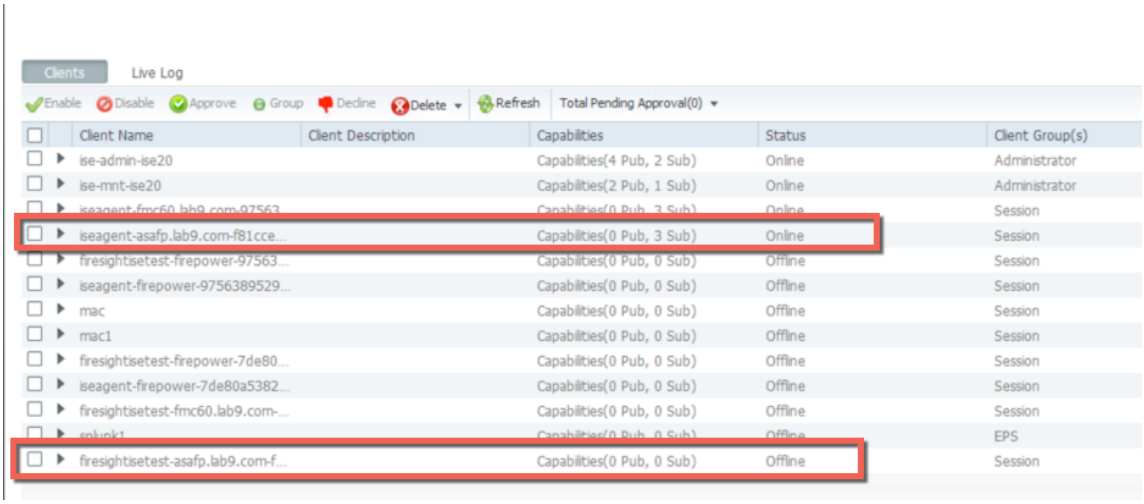
注：自己署名証明書または CA 署名付き証明書に関する適切な証明書情報を入力してください。



手順 3. [テスト（Test）] を選択し、ISE pxGrid ノードへの接続を確認します。次にように表示されます。



手順 4. ASA Firepower が pxGrid クライアントとして正常に登録されたことを確認します。[管理（Administration）] > [pxGrid サービス（pxGrid Services）] を選択します。



手順 5. 試行に失敗した場合は、

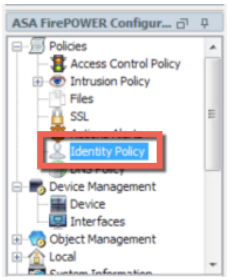
手順 6. [モニタリング（Monitoring）] > [ASA Firepower のモニタリング（ASA Firepower Monitoring）] を選択します。これにより詳細を確認できます。

注: 障害の大半は証明書の問題です。

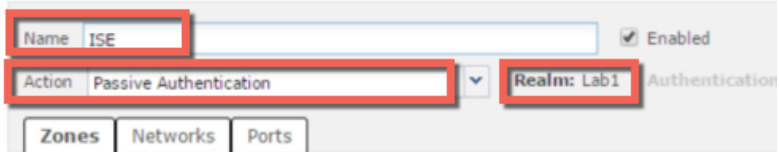
ISE ID ポリシー

ISE ID ポリシーは、パッシブ認証用に設定され、Firepower Management Center の ISE 認証に関するデフォルト アクセス制御ルールで使用されます。

手順 1. [ASA FirePOWER 設定（ASA Firepower Configuration）] > [ポリシー（Policies）] > [ID ポリシー（Identity Policy）] の順に選択します。

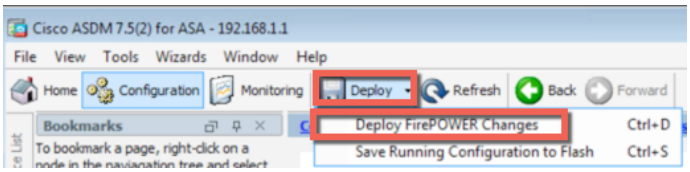


手順 2. [ルールの追加（Add Rule）] を選択し、名前を入力して、[パッシブ認証（Passive Authentication）] > [レルム（Realm）] の順に選択します。



手順 3. [ASA Firepower の変更の保存（Store ASA Firepower Changes）] を選択します。

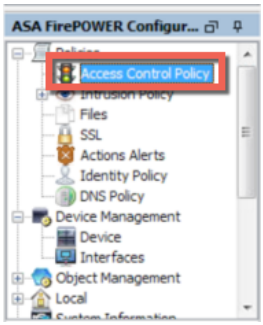
手順 4. [導入（Deploy）] > [Firepower の変更の導入（Deploy Firepower Changes）] > [導入（Deploy）] の順に選択後、[OK] を選択します。



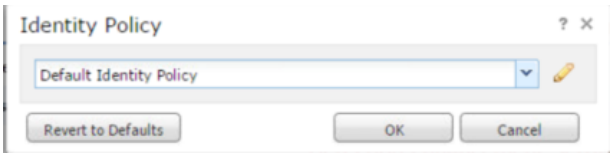
ISE ID ポリシーの追加

ISE の ID ポリシーを Firepower Management Center のデフォルト アクセス ポリシーに追加します。

手順 1. [ASA Firepower 設定（ASA Firepower Configuration）] > [ポリシー（Policies）] > [アクセス制御ポリシー（Access Control Policy）] の順に選択します。



手順 2. [ASA Firepower] > [ルールの追加（Add Rule）] > [ID ポリシー（Identity Policy）] > [なし（None）] の順に選択し、ドロップダウンから、[デフォルト ID ポリシー（Default Identity Policy）] を選択します。



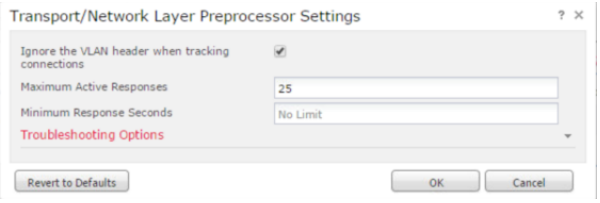
手順 3. [OK] を選択します。

手順 4. [ASA Firepower の変更の保存（Store ASA Firepower Changes）] をクリックします。

トランスポート層とネットワーク層のプリプロセッサの設定

これらの設定は、Firepower 侵入ポリシーに基づいてネットワーク アクセスをブロックするように変更されています。

手順 1. [詳細（Advanced）] > [トランスポート層/ネットワーク層プリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] をクリックし、次のように設定します。



手順 2. [OK] を選択します。

ブロック応答ページの追加

システムで提供されるブロック応答ページが、ブロックされた応答として Firepower アクセス制御ファイルに追加されています。

手順 1. [HTTP 応答（HTTP Responses）] をクリックし、次のように入力します。

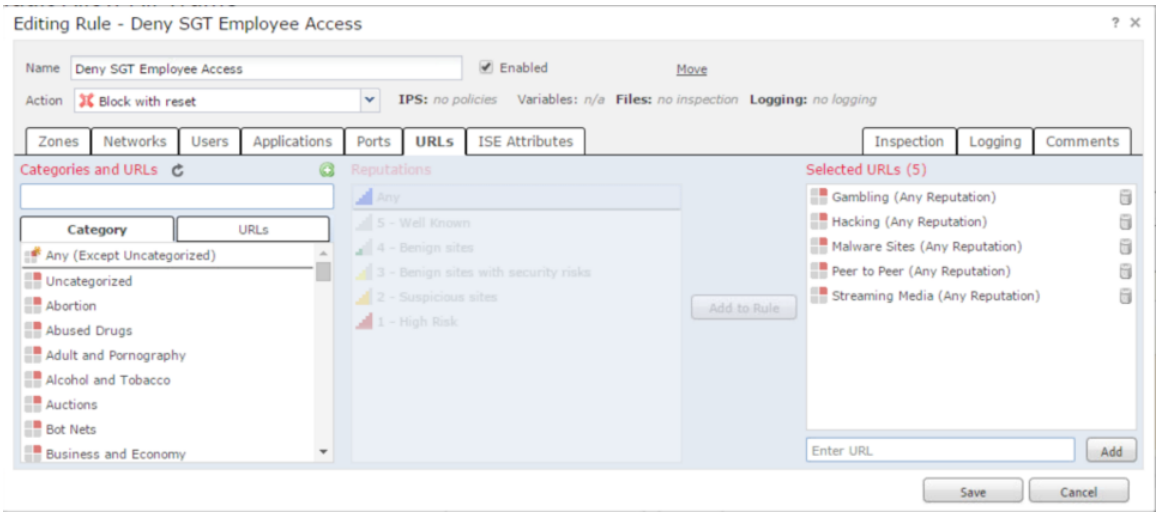
手順 2. [ASA Firepower の変更の保存（Store ASA Firepower Changes）] をクリックします。

ASA 作成の Employee SGT タグのアクセス制御ルール

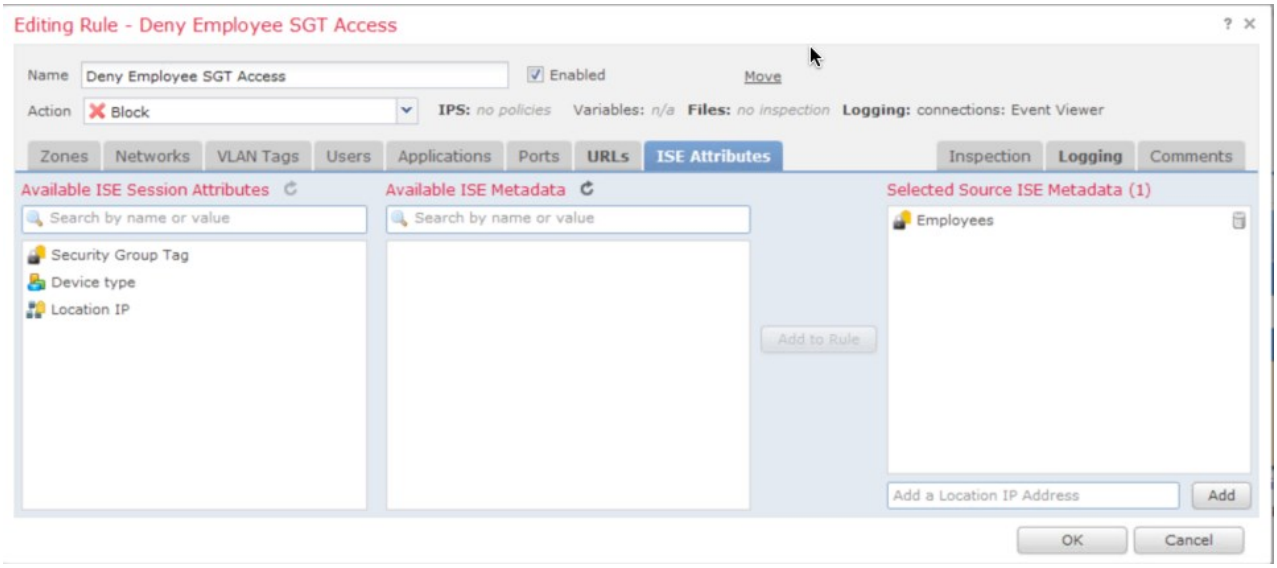
これらの Employee SGT タグ アクセス制御ルールは、会社のアクセプタブル ユース ポリシーを設定し、ハッキング サイト、ストリーミング メディア、ピアツーピア アプリケーション、マルウェア サイト、ギャンブル サイトへのアクセスを拒否します。

手順 1. [ASA Firepower 設定（ASA Firepower Configuration）] > [アクセス制御ポリシー（Access Control Policy）] > [ASA Firepower] の順に選択し、ルールを追加します。

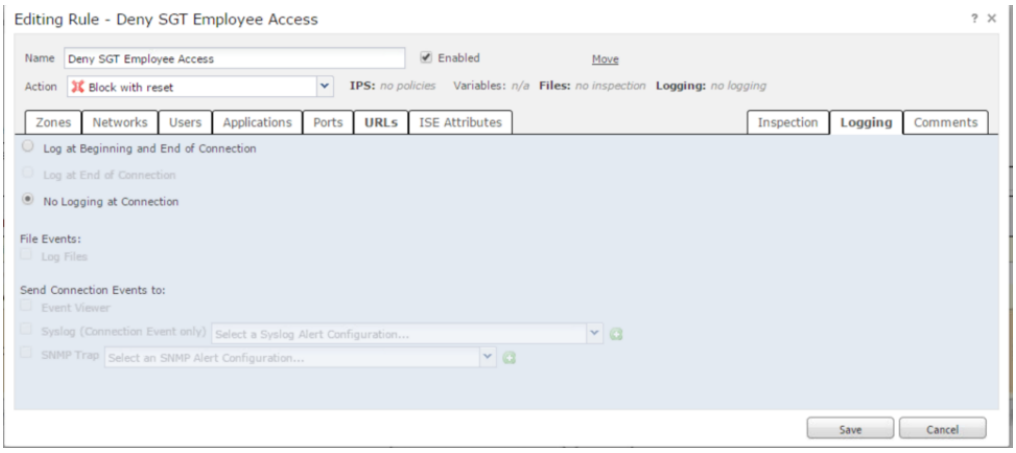
手順 2. [ルールの追加(Add Rule)] を選択し、[名前(Name)]に Deny Employee SGT Access と入力して、[アクション(Action)] で [ブロックしてリセット(Block with reset)]、[IPS] で [pxGrid 侵入ポリシー(pxGrid intrusion policy)] を選択します。次に [URLs] > [カテゴリ(Category)] を選択して、[ギャンブル(Gambling)、[ピアツーピア(Peer-to-Peer)]、[ストリーミング ビデオ(Streaming Video)]、[ハッキング(Hacking)] を指定し、[保存(Save)] を選択します。



手順 3. [ISE 属性(ISE Attributes)] > [利用可能な ISE セッション属性(Available ISE session attributes)] > [セキュリティ グループ タグ(Security Group Tag)] > [利用可能な ISE メタデータ(Available ISE Metadata)] を選択し、Employees を指定して、[ルールに追加(Add to Rule)] を選択します。

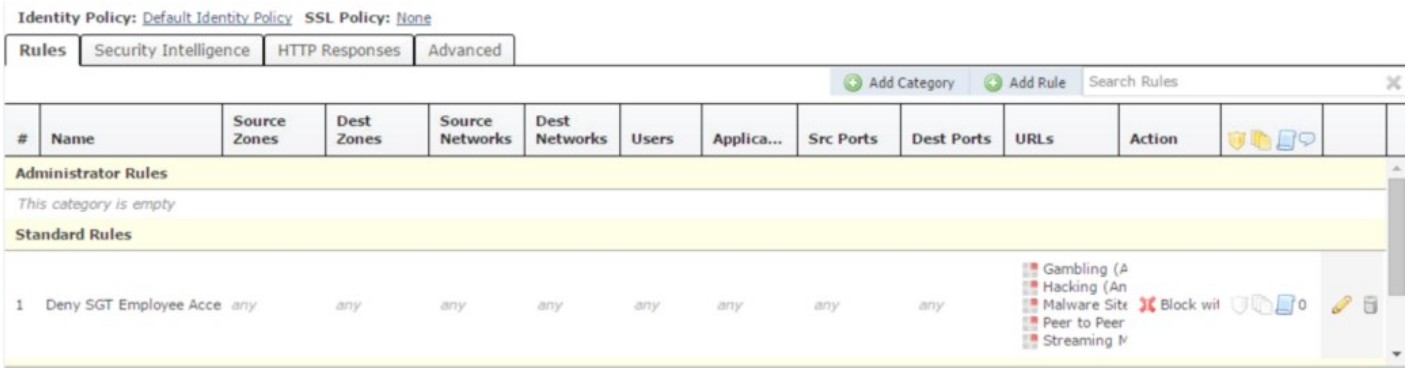


手順 4. [ロギング(Logging)] を選択し、次のように設定します。



手順 5. [保存(Save)] を選択します。

次が表示されます。



手順 6. [保存(Save)] を選択します。

手順 7. [ASA Firepower の変更の保存(Store ASA Firepower Changes)] を選択します。

手順 8. [導入(Deploy)] > [Firepower の変更の導入(Deploy Firepower Changes)] > [導入(Deploy)] の順に選択後、[OK] を選択します。

手順 9. [モニタリング(Monitoring)] > [ASA Firepower のモニタリング(ASA Firepower Monitoring)] > [タスクのステータス(Task Status)] を選択すると、導入ステータスが表示されます。

ASA Firepower pxGrid 侵入ポリシー

この項では、pxGrid 侵入ポリシーを作成し、Firepower センサーに導入します。このポリシーには、「SERVER IIS CMD.EXE access」ルールが含まれており、エンドユーザがブラウザに www.yahoo.com/cmd.exe と入力すると、侵入イベントがトリガーされてインライン時にドロップされ、Firepower Management Console の [侵入イベント分析（Analysis Intrusion Events）] にイベントが生成されます。

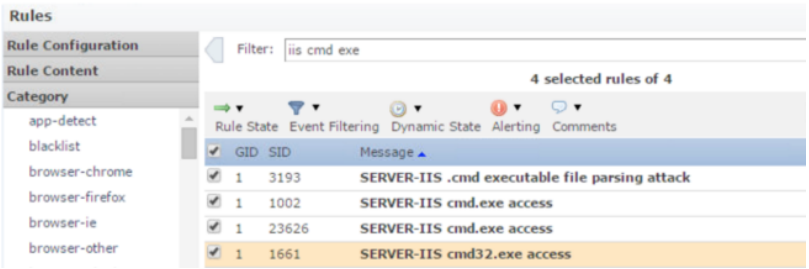
手順 1. [ASA Firepower の設定（ASA Firepower Configuration）] > [侵入ポリシー（Intrusion Policy）] > [ポリシーの作成（Create Policy）] の順に選択し、次のように設定します。

手順 2. [ポリシーの作成（Create Policy）] をクリックします。

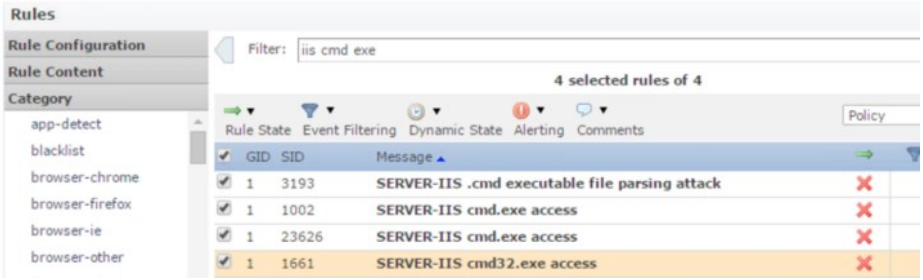
手順 3. 次が表示されます。

手順 4. をクリックして、ポリシーを編集します。

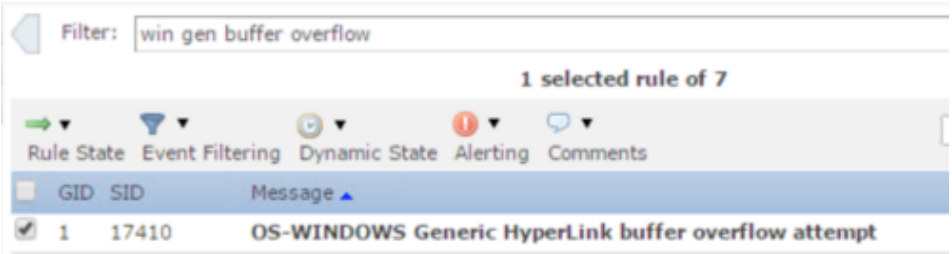
手順 5. [ルール（Rules）] を選択し、[フィルタ（Filter）] に **iis cmd exe** と入力して、次のように選択します。



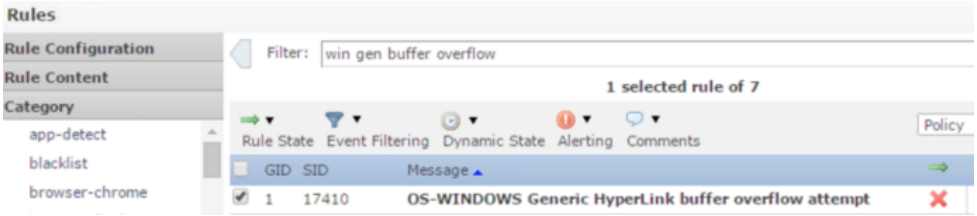
手順 6. [ルールの状態（Rule State）] > [イベントのドロップと生成（Drop and Generate Events）] > [OK] の順にクリックします。
次が表示されます。



手順 7. 次に [フィルタ（Filter）] に **win gen buffer overflow** と入力して、[OS-Windows Generic Hyperlink BufferOverflow Attempt] を選択します。

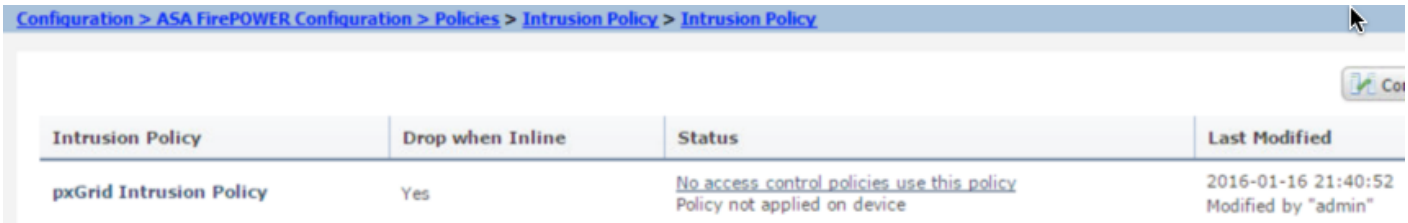


手順 8. [ルールの状態（Rule State）] > [イベントのドロップと生成（Drop and Generate Events）] > [OK] の順にクリックします。



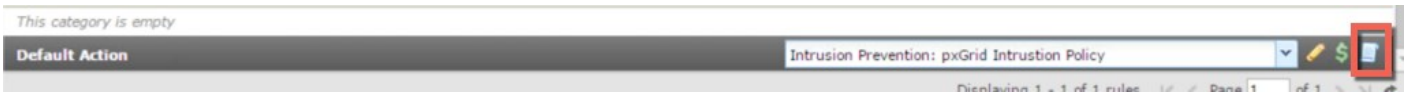
手順 9. [ポリシー情報（Policy Information）] をクリックして変更を確定します。

手順 10. [変更を確定（Commit Changes）] > [OK] をクリックします。
手順 11. 次が表示されます。

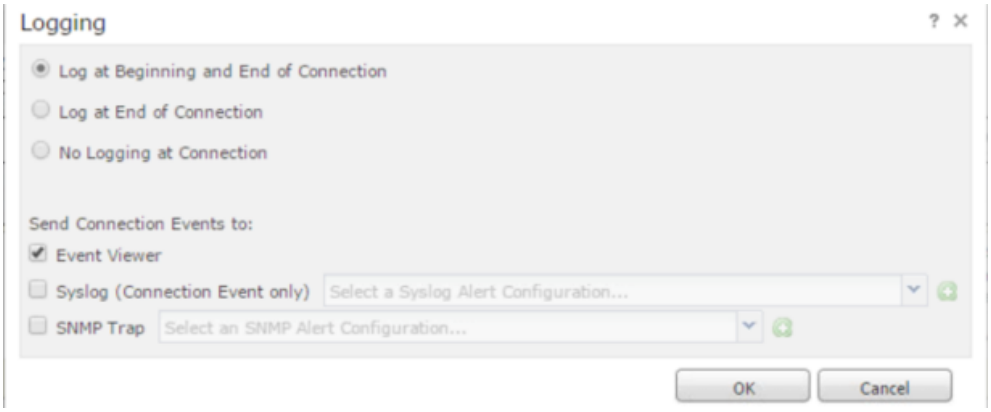


手順 12. pxGrid 侵入ポリシーをデフォルトのアクセス制御ポリシーに追加します。
[ASA Firepower の設定（ASA Firepower Configuration）] > [ポリシー（Policy）] > [アクセス制御ポリシー（Access Control Policy）] の順に選択し、ドロップダウンから [侵入防御：pxGrid 侵入ポリシー（Intrusion Prevention: pxGrid Intrusion Policy）] を選択します。

手順 13. を選択して、ロギングを設定します。



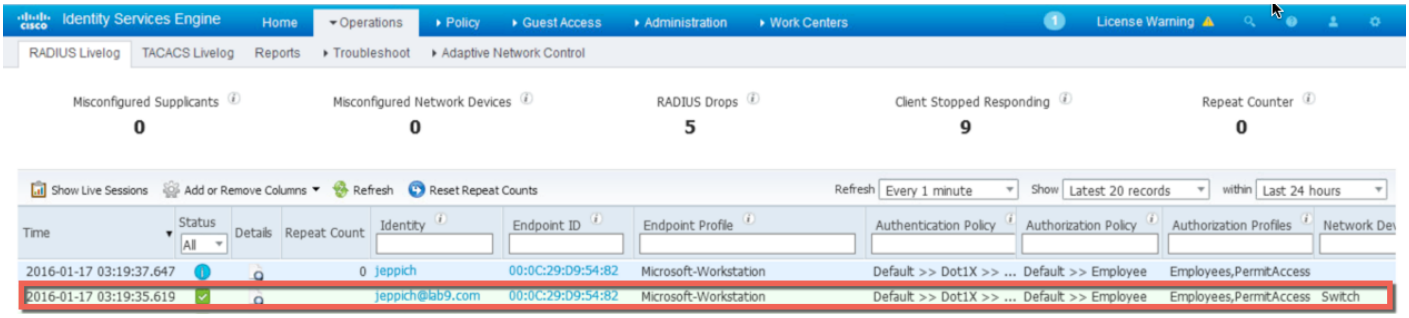
手順 14. 次のようにロギングを設定します。



手順 15. [OK] をクリックします。
手順 16. [ASA Firepower の変更の保存（Store ASA Firepower Changes）] をクリックします。
手順 17. [導入（Deploy）] > [Firepower の変更の導入（Deploy Firepower Changes）] > [導入（Deploy）] の順に選択後、[OK] を選択します。
手順 18. [モニタリング（Monitoring）] > [ASA Firepower のモニタリング（ASA Firepower Monitoring）] > [タスク（Task）] を選択すると、導入ステータスが表示されます。

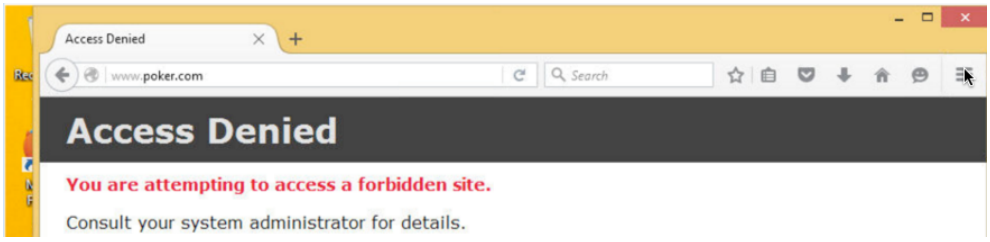
オンボックス Firepower Management ポリシーを使用した Employee SGT ユーザのテスト

従業員は ISE に認証されると、Employee SGT が割り当てられます。

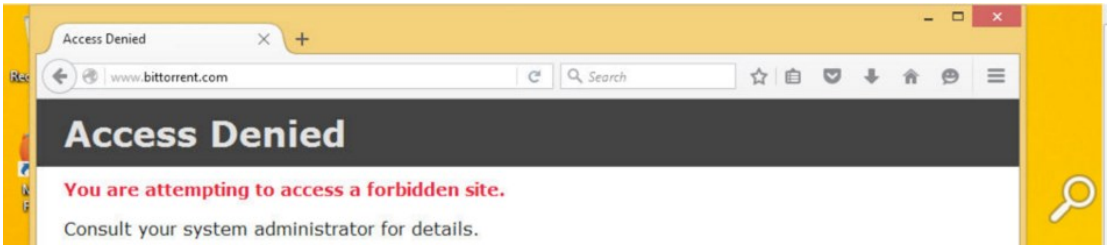


Firepower Management Center がユーザ セッションを取得したことがわかります。

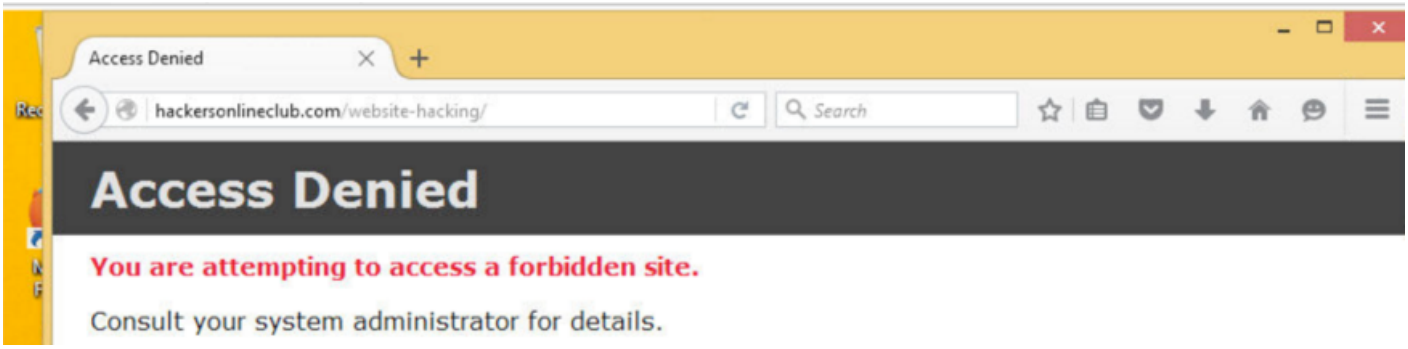
従業員が www.poker.com にアクセスすると、そのアクセスは拒否されます。



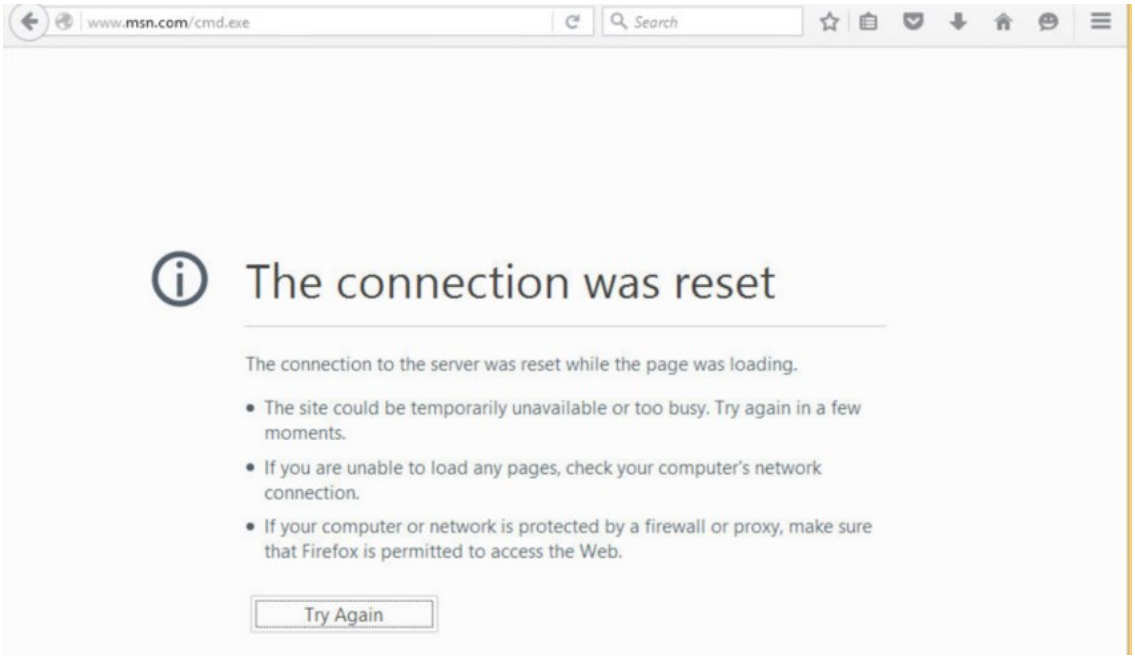
従業員が www.bittorent.com にアクセスすると、そのアクセスは拒否されます。



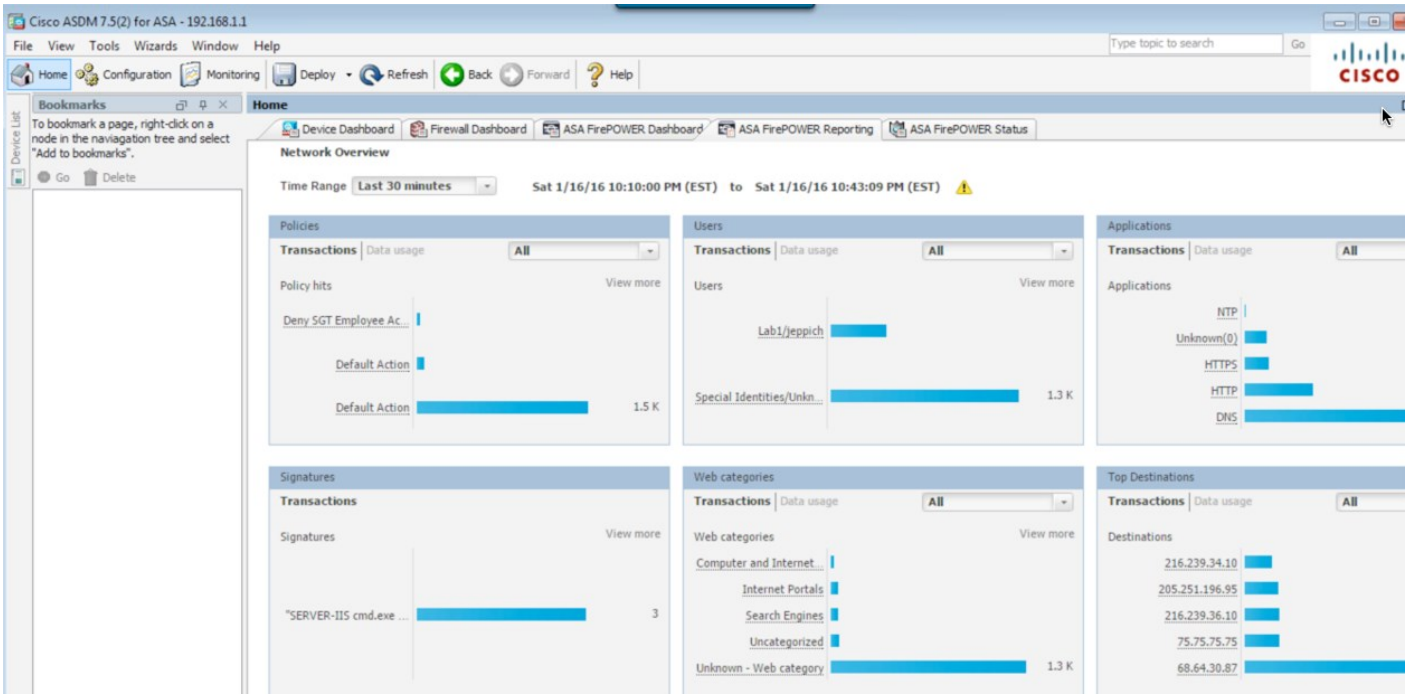
従業員がハッキング クラブ www. hackersonlineclub.com に参加しようとすると、そのアクセスは拒否されます。



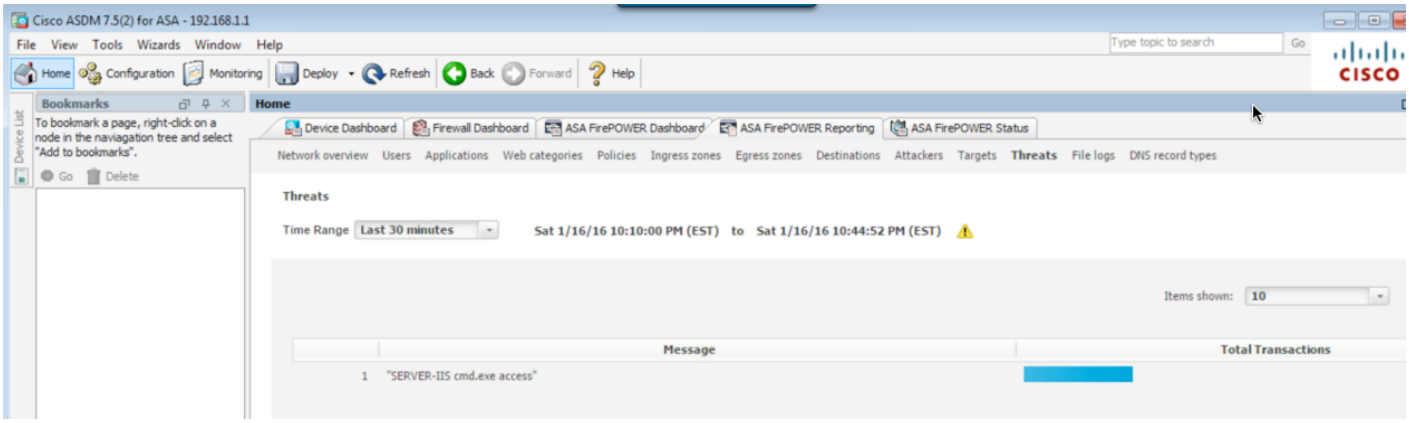
また、その従業員がブラウザに www.msn.com/cmd.exe を挿入しようとすると、そのアクセスは拒否されます。



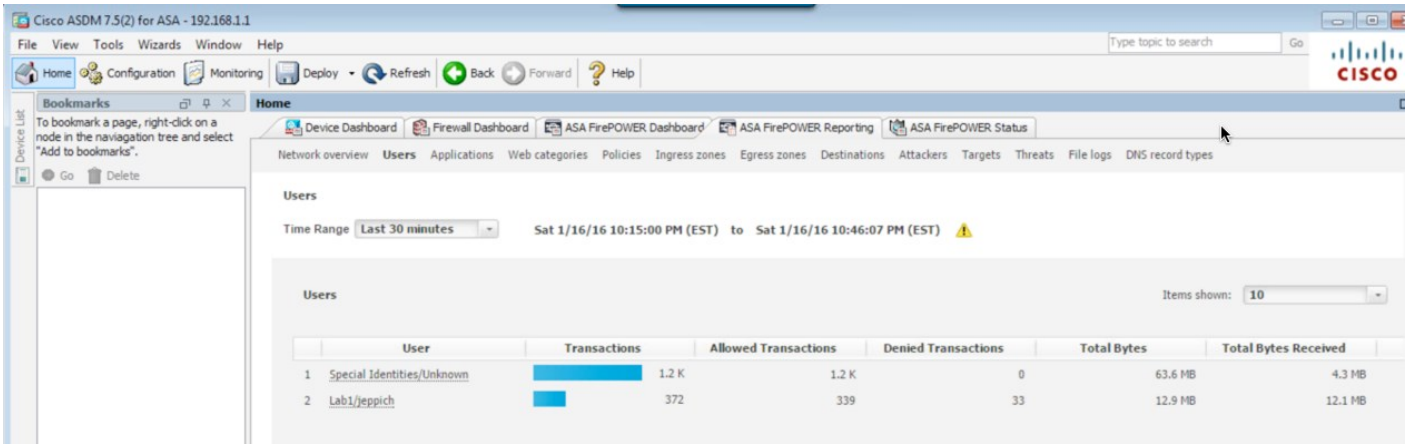
[ASA Firepower レポーティング（ASA Firepower Reporting）] でレポートを見ることができます。拒否された Web カテゴリトランザクションと起動されたサーバ IIS-Web シグネチャを確認します。



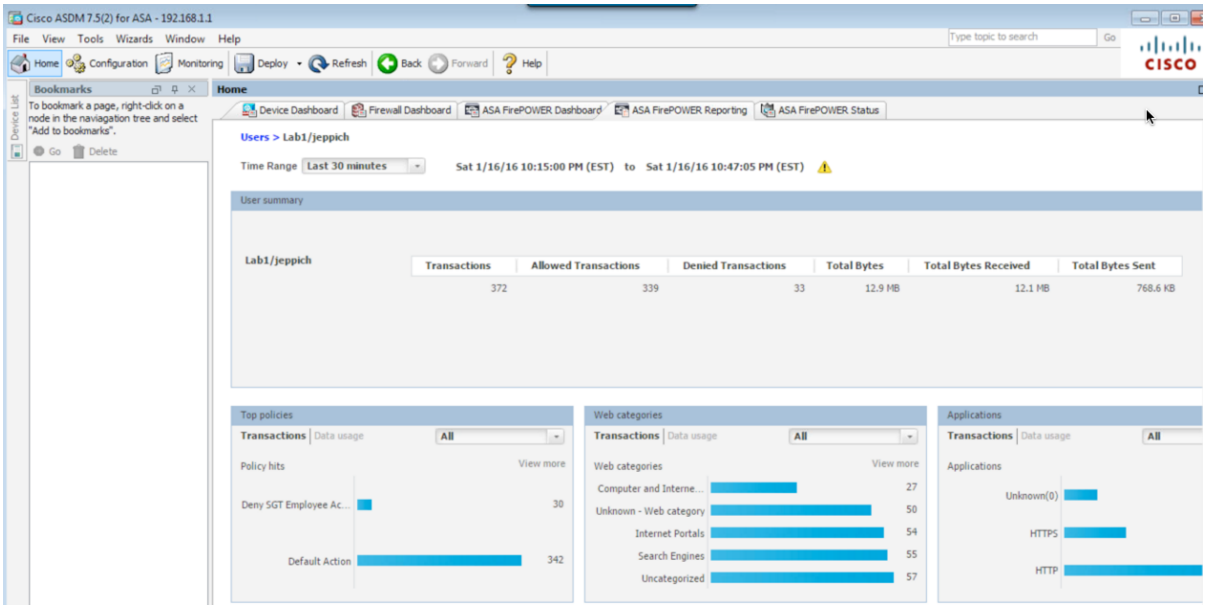
[脅威（Threat）] レポートの下をクリックすると、SERVER-IIS のシグネチャが表示されます。



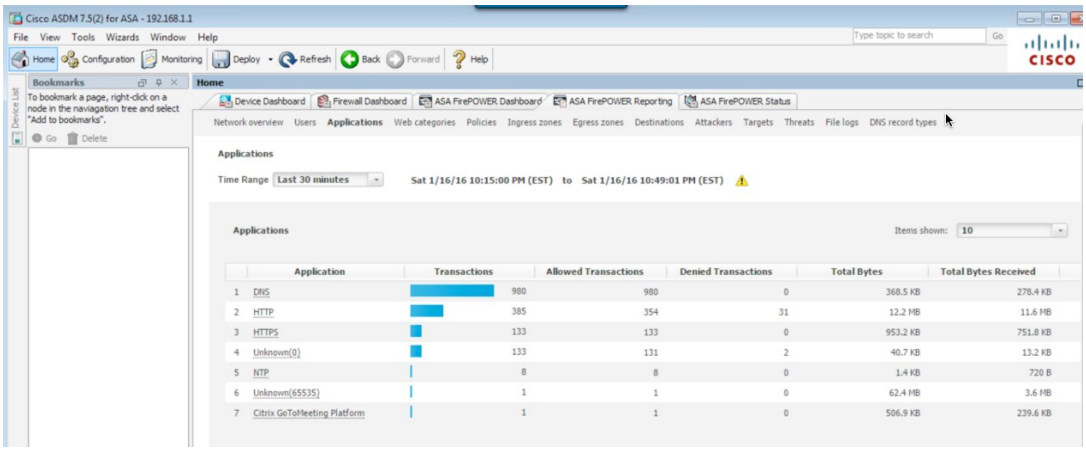
ユーザ別にレポートを選択する場合は、[jeppich] をクリックします。



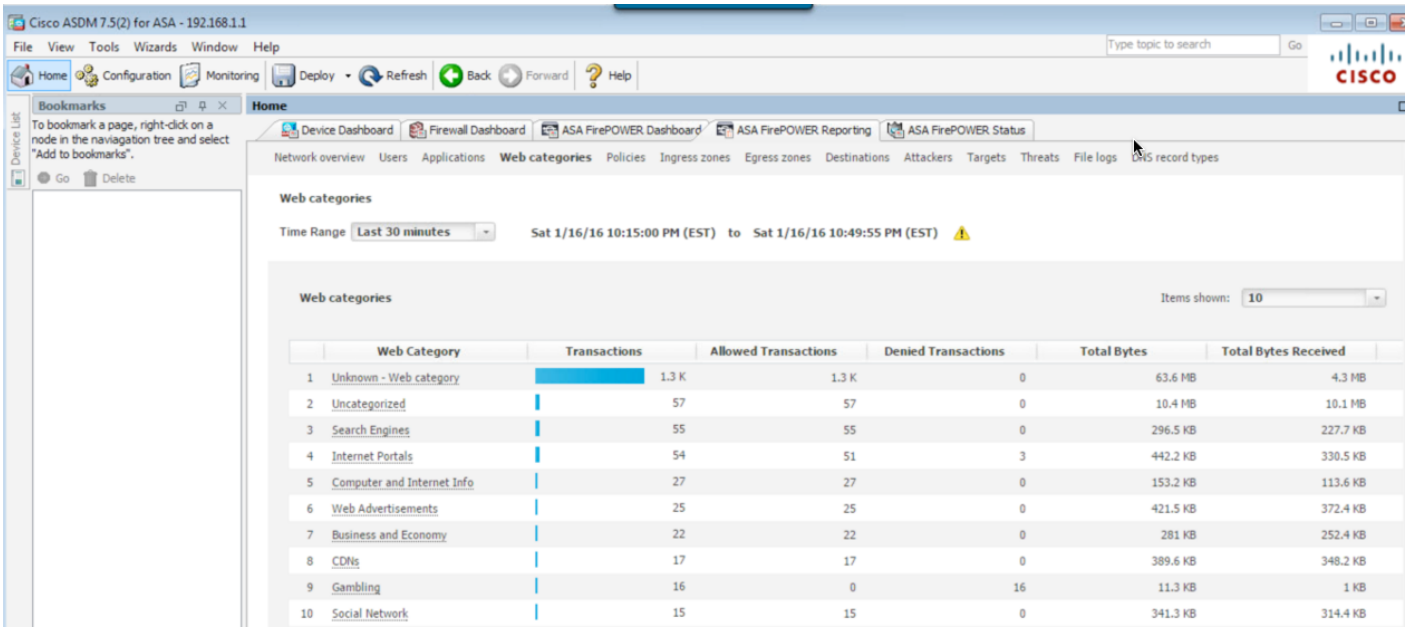
上位のトランザクション、Web カテゴリ、アプリケーションが表示されます。



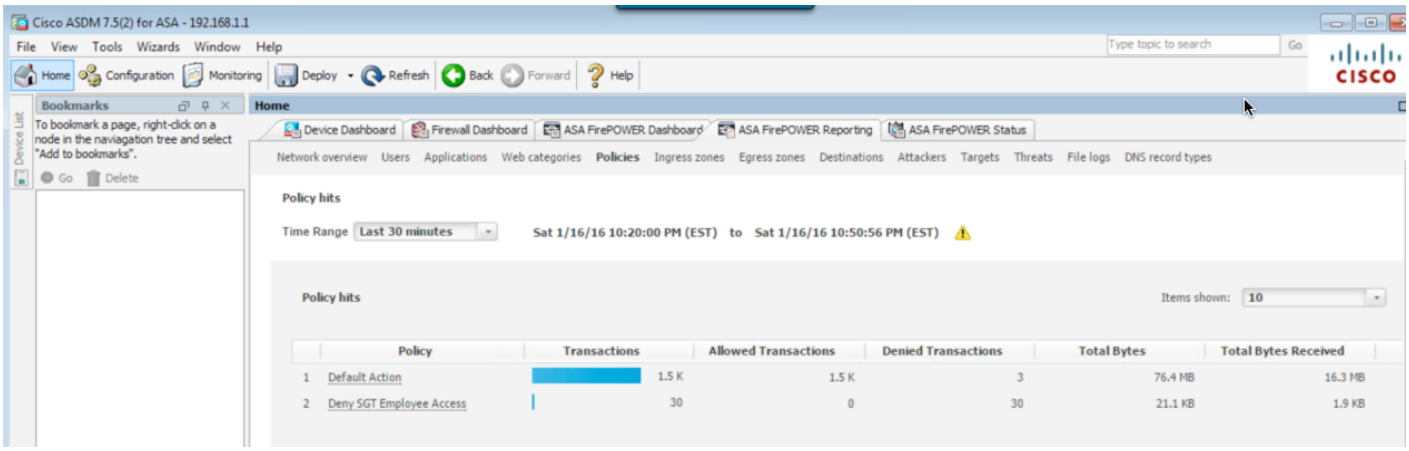
アプリケーションを表示するレポートもあります。



また、ポリシーに基づいてレポートを表示できます。



さらに、[ポリシー ヒット情報（Policy hits）] もあります。


Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Deploy Refresh Back Forward Help
Bookmarks
To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".
Go Delete
Device List
Home
Device Dashboard Firewall Dashboard ASA FirePOWER Dashboard ASA FirePOWER Reporting ASA FirePOWER Status
Network overview Users Applications Web categories Policies Ingress zones Egress zones Destinations Attackers Targets Threats File logs DNS record types
Policy hits
Time Range Last 30 minutes
Sat 1/16/16 10:20:00 PM (EST) to Sat 1/16/16 10:50:56 PM (EST)
Policy hits
Items shown: 10
Policy Transactions Allowed Transactions Denied Transactions Total Bytes Total Bytes Received
1 Default Action 1.5 K 1.5 K 3 76.4 MB 16.3 MB
2 Deny SGT Employee Access 30 0 30 21.1 KB 1.9 KB

トラブルシューティング

ISE pxGrid ノード

pxGrid 公開ノードが表示されず、pxGrid 接続がない

- ISE 1.3/1.4 の自己署名証明書を使用している場合は、pxGrid を有効化する前に、ISE 自己署名アイデンティティ証明書を ISE システム信頼ストアにエクスポート済みであることを確認してください。
- CA 署名付き証明書を使用する場合は、pxGrid を有効化する前に、カスタマイズした pxGrid テンプレートがサーバ認証とクライアント認証の両方の EKU を持っていることを確認してください。
- pxGrid を実稼働環境に導入する場合は、専用 ISE pxGrid ノードがその公開キー/秘密キー ペアを PPAN ノードと PMNT ノードにインポート済みであることを確認してください。pxGrid アクティブ/スタンバイが導入されている場合は、セカンダリ pxGrid ノードが公開キー/秘密キーをセカンダリ SPAN ノードとセカンダリ SMNT ノードにインポート済みであることが必要です。
  アクティブ化可能な pxGrid ノード上でのみ、application status ise を実行して、ISE pxGrid ノードがアクティブノードであることを確認してください。
- ISE の電源をオフにしてから再度オンにします。**application stop ise/application start ise** を実行します。
  また、ISE が pxGrid のバックアップとして対応可能である場合は、ISE サービスを停止する前に、ISE ノードから pxGrid を無効化することもできます。
- ダウンロードした証明書は Base 64 エンコード形式であることが必要です。

Firepower Management Center 6.0

システム統合 ISE 証明書テストが失敗する

- 自己署名証明書を使用するスタンドアロン POC 環境で ISE 1.3/1.4 を使用し、プライマリとして設定してしない場合は、一括ダウンロード セッションに関する既知のバグがあります。このバクで FQDN 問題の説明ができます。プライマリに設定することで解消されます。ISE 2.0 ではこの問題は発生しません。
- CA 署名付き証明書の操作用のスタンドアロン環境で ISE を使用する場合は、CSR 要求の目的が管理であり、pxGrid ではないことを確認してください。これは、アクティブな一括ダウンロード レコード セッションで必須です。
- CA 署名付き操作の場合:
- 自己署名操作の場合:
- FMC 6.0、ISE pxGrid ノード、デバイスがすべて DNS 解決可能であることが必要です。

ISE から相関イベントが見えない

- FMC と ISE の間で時刻が同期されていることを確認してください。時刻は、FMC とすべての登録済みデバイスの間でも同期されていることが必要です。

ASA with Firepower サービス

Firepower Management Center に登録済みの ASA デバイスパラメータを変更できない

- Firepower Management Center 上の適切な ASA モデルに対する適切なデバイス ライセンスがあることを確認してください。

SFR が回復状態のまま変わらない

- SFR インストールを再実行してください。これにはしばらく時間がかかります。既存の ASA 5506 では 30 分以上かかりました。sh module sfr を実行して、起動していることを確認してください。

```
Password:
Type help or '?' for a list of available commands.
ciscoasa> en
Password: *********
ciscoasa# sh module sfr

Mod  Card Type                                    Model              Serial No.
---- ---------------------------------------------- ------------------ -----------
 sfr FirePOWER Services Software Module            ASA5506W           JAD192300TD

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
 sfr d8b1.90ab.ab09 to d8b1.90ab.ab09  N/A          N/A          6.0.0-1005

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 sfr ASA FirePOWER                  Up               6.0.0-1005

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
 sfr Up                 Up

ciscoasa#
```

ASA Firepower レポートにトラフィックが表示されない

- ASA Firepower サービスにすべてのトラフィックを設定してください。
- 設定例を以下に示します。

```
ciscoasa# conf t
ciscoasa(config)# sh run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
```

```
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)# sh service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 5531, lock fail 0, drop 0, reset-drop 0, 5-min-

pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,

5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5

-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-

min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 15, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
```

```
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options _default_ip_options_map, packet 0, lock fail 0, drop 0, reset-

drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default

      Default Queueing      SFR: card status Up, mode fail-open
        packet input 250, packet output 250, drop 0, reset-drop 0
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)

ciscoasa(config-pmap-c)# sh service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: class-default
      SFR: card status Up, mode fail-open
        packet input 264, packet output 264, drop 0, reset-drop 0
ciscoasa(config-pmap-c)# sh service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: class-default
      SFR: card status Up, mode fail-open
        packet input 290, packet output 290, drop 0, reset-drop 0
ciscoasa(config-pmap-c)#
```

不具合の解決

pxGrid & Identity マッピング サービスが再起動する

説明：証明書が ISE 展開の信頼ストアからインポートまたは削除された場合、ISE pxGrid ノードで pxGrid & Identity マッピング サービスが再起動します。

提起された障害：CSCuv43145

回避策：サービスは自動的に再起動するために回避策は必要ありませんが、サービスが再起動中は新しい検疫イベントは処理されません。

解決の計画：ISE Carlsbad リリース 2016 年春

アクティブな pxGrid ノードが GUI に反映されない。CLI には反映される

説明：pxGrid HA 展開で 2 つの pxGrid ノードが利用可能な場合、1 つはアクティブで、もう 1 つはスタンバイです。どちらがアクティブかを識別する際、管理者は CLI で pxGrid のステータスを確認する必要があります。ステータスは UI の [展開（Deployment）] ページに表示されません。この追加は Carlsbad で行われます。

回避策：CLI を使用してアクティブ/パッシブの状態を判別します。

解決の計画：ISE Carlsbad リリース 2016 年春

参考資料

分散 ISE 環境での pxGrid の設定：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

Cisco pxGrid による証明書の展開方法。CA 署名 ISE pxGrid ノードおよび CA 署名 pxGrid クライアントの設定：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-CA_signed_pxGridISEnode_CAsigned_pxGridclient.pdf

Cisco pxGrid による証明書の展開方法。ISE pxGrid ノードと pxGrid クライアントを使用する自己署名証明書：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf

Cisco Firepower Management Center 6.0 設定ガイド

http://www.cisco.com/c/en/us/td/docs/security/Firepower/60/configuration/guide/fpmc-config-guide-v60.html