

Cisco Firepower 次世代ファイアウォール 6.4 機能ラボ v1.3

最終更新日：2019 年 3 月 19 日

このガイドについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

- [要件](#)
- [6.4 リリースとこのラボについて](#)
- [シナリオの依存関係](#)
- [トポロジ](#)
- [はじめに](#)
- [シナリオ 1：オブジェクト使用状況とヒット カウント](#)
- [シナリオ 2：NGFW に SSH でアクセスするための RBAC](#)
- [シナリオ 3：ファイル イベントを含むユニファイド ログイング](#)
- [シナリオ 4：FMC におけるリモート アクセス VPN の強化](#)
- [シナリオ 5：FDM におけるリモート アクセス VPN の強化](#)
- [シナリオ 6：証明書ベースの認証を使用して、FMC と FDM の管理対象デバイスでサイト間 VPN 接続を行う](#)
- [シナリオ 7：NGFW のデバイス API](#)

要件

次の表に、このデモンストレーションの要件の概要を示します。

表 1. 要件

必須	オプション
<ul style="list-style-type: none"> • ラップトップ 	<ul style="list-style-type: none"> • Cisco AnyConnect®

6.4 リリースとこのラボについて

6.4 リリースでは、いくつかの機能が強化されています。このラボでは、そうした機能の多くに重点を置きます。

シナリオ 1 では、6.4 の 2 つの新しい機能である、オブジェクトの使用状況、およびヒット カウントの演習を行います。オブジェクトの使用状況は、限られた一連のオブジェクト タイプで使用できます。たとえば、ポリシー内のネットワーク オブジェクトの使用状況を特定できます。ヒット カウントは、プレフィルタとアクセス コントロール ポリシーのルールで利用可能です。

IMPORTANT! This content includes pre-release software, and you may experience issues with some features. This documentation was not created or verified by dCloud. Check Cisco dCloud regularly for new releases!

シナリオ 2 では、ユニファイド ログイングとコンテキスト クロス起動を設定してテストします。これらは 6.3 の機能です。6.4 では、ファイルとマルウェアのイベントがユニファイド ログイングに追加されました。

シナリオ 3 では、NGFW への SSH アクセスに RBAC を設定してテストします。この機能は 6.4 で追加されていて、FMC と FDM の両方の管理対象デバイスで使用できます。

シナリオ 4 と 5 の両方で、FTD 向けの新しい 6.4 RA VPN 機能 (2 要素認証と二重認証を含む) を取り上げます。シナリオ 4 では FMC に、シナリオ 5 では FDM に注目します。

シナリオ 6 では、6.4 で強化されたサイト間 VPN に重点を置きます。

シナリオ 7 では、さまざまな API ツールを紹介します。これは、厳密には 6.4 の教材ではありませんが、6.4 では、API が強化されています。

シナリオの依存関係

シナリオ間に依存関係はありません。シナリオは、任意の順序で実施することも、省略することもできます。

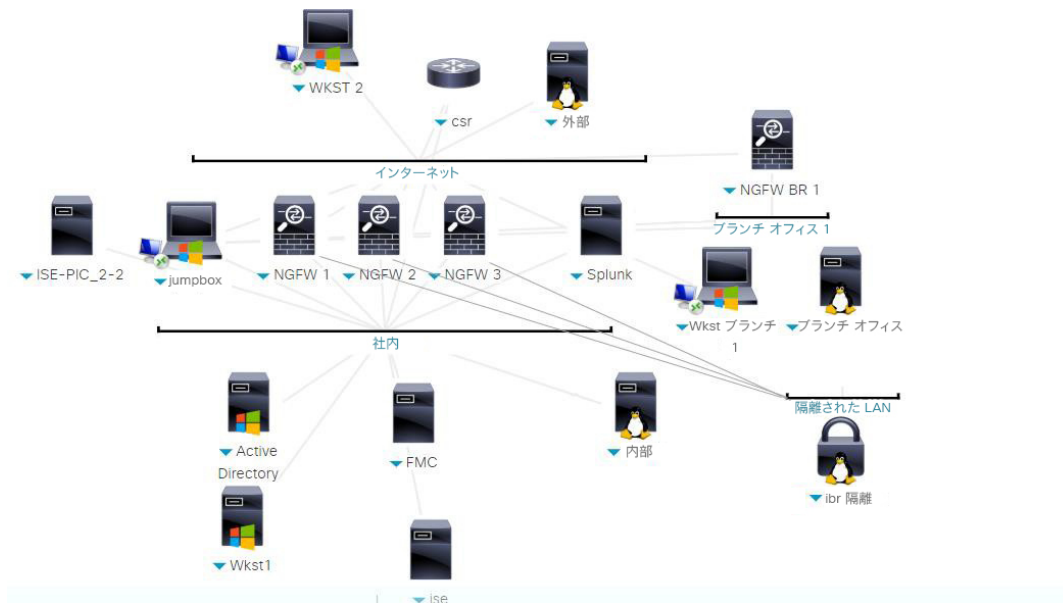
シナリオ 4 とシナリオ 5 には多くの重複項目があります。受講者は、これらのシナリオのいずれかを実施します。両方の実施は想定されていません。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント クレデンシャルは、アクティブな dCloud セッションの [トポロジ (Topology)] メニューのコンポーネント アイコンをクリックして確認でき、それらを使用する必要があるシナリオ内の手順でも確認できます。

注：わかりやすさを考慮して、この図にはすべての IP アドレスと VLAN を含めていません。

図 1. dCloud のトポロジ



クレデンシャル

ログイン クレデンシャルは、必要なときにガイド内の手順で提示されます。ただし利便性を考慮して、以下の表にこれらのシナリオで使用されるクレデンシャルを示します。

表 2. デバイスのログイン クレデンシャル

VM	ログイン	パスワード
FMC	admin	C1sco12345
すべての NGFW	admin	C1sco12345
すべての Windows ワークステーション	Administrator	C1sco12345
Splunk	admin	C1sco12345
ISE および ISE PIC	admin	C1sco12345
内部 Linux サーバ	root	C1sco12345
外部 Linux サーバ	root	C1sco12345
CSR	admin	C1sco12345

また、パッシブ認証と RBAC のために複数のユーザがすでに作成されています。

表 3. ユーザ クレデンシャル

ログイン	パスワード	詳細
dilbert	C1sco12345	Engineering グループ内の Active Directory ユーザ
harry	C1sco12345	HR グループ内の Active Directory ユーザ
ira	C1sco12345	Finance および Investment グループ内の Active Directory ユーザ
rita	C1sco12345	IT グループ内の Active Directory ユーザ
alicia	C1sco12345	ISE のローカル ユーザ、FDM 管理者ユーザ
oliver	C1sco12345	ISE のローカル ユーザ、FDM 読み取り専用ユーザ

ログイン	パスワード	詳細
victoria	C1sco12345	ISE のローカル ユーザ、VPN ユーザ
william	C1sco12345	ISE のローカル ユーザ、FDM 読み取り/書き込みユーザ

はじめに

ログイン クレデンシャルは、必要なときにガイド内の手順で提示されます。ただし利便性を考慮して、以下の表にこれらのシナリオで使用されるクレデンシャルを示します。

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[\[手順を見る\]](#) [英語]

注：セッションがアクティブになるまで、最長で 10 分かかります。

2. このガイドでは、提示された詳細情報を使用して Jumpbox RDP セッションからすべてのデバイスに接続することを前提としています。

注： Cisco AnyConnect VPN [\[手順を見る\]](#) [英語] またはラップトップのローカル RDP クライアント [\[手順を見る\]](#) [英語] を使用して、ワークステーションに接続することもできます。

Jumper : 198.18.133.50、ユーザ名 : administrator、パスワード : C1sco12345

シナリオ 1： オブジェクト使用状況とヒット カウント

6.4 より前では、FMC でカスタム ワークフローを作成することで、アクセス コントロール ポリシー ルールのヒット カウントのみ生成することができました。6.4 では、アクセス コントロール ポリシー ルールとプレフィルタ ポリシー ルールの両方の標準機能として、ヒット カウントが追加されています。また 6.4 では、制限付きオブジェクトの使用状況に関する情報が、一部のオブジェクト タイプで追加されています。

注：ヒット カウントは、6.4 の FDM でも使用できます。デバイス API のラボ演習で、それを確認できます。

このシナリオの目的：

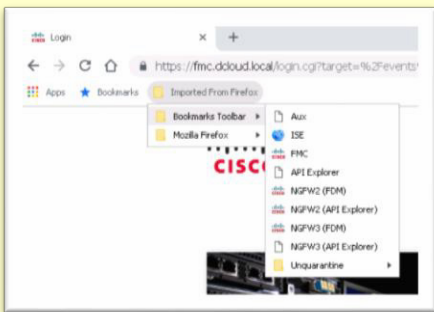
- オブジェクト使用状況の機能を利用する。
- ヒット カウント機能を使用する。

イベントの生成

1. Jumpbox で、[内部Linuxサーバ (Inside Linux Server)] への PuTTY セッションを開きます。root でログインします。パスワードは **C1sco12345** を使用します。

注：Chrome は Firefox よりも速くページを読み込みます (特に FMC の場合)。ただし、Chrome では、セキュリティ警告がより頻繁に表示され、NGFW2 と NGFW3 のクレデンシャルがキャッシュされません。ブラウザはどちらでも使用できます。また、両方のブラウザを使用することもできます。

Chrome では、ブックマークは Firefox からインポートされたもので、次に示すようにブックマーク バーのサブフォルダ内にあります。

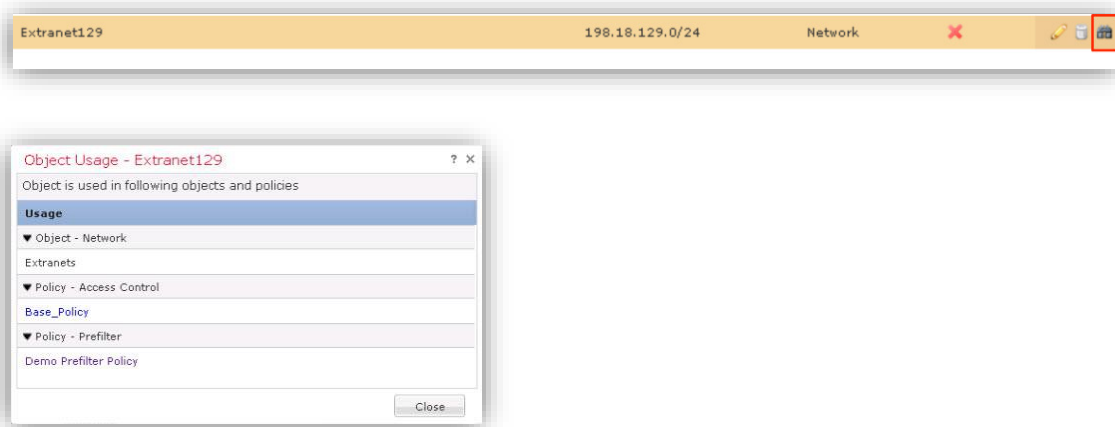


必要に応じて、Chrome と Firefox のいずれかを選択します。

2. 内部 Linux サーバで、「**makeevents**」と入力します。これにより、さまざまなイベントが生成されます。
3. 外部 Linux サーバへの PuTTY セッションを開きます。root でログインします。パスワードは **C1sco12345** を使用します。
4. 内部 Linux サーバと外部 Linux サーバの両方で、「**ifup tun0**」と入力します。これにより、NGFW1 を介して、これらのサーバ間で GRE トンネルが確立します
5. 内部 Linux サーバと外部 Linux サーバの両方で、「**makehits**」と入力します。これにより、これらのサーバ間で ICMP および GRE トラフィックが生成されます。

オブジェクト使用状況の利用

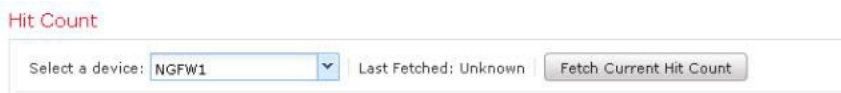
1. FMC で、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] に移動します。ネットワーク オブジェクトのページが表示されます。
2. オブジェクト Extranet129 の右側にある双眼鏡アイコンをクリックします。オブジェクトがプレフィルタとアクセス コントロール ポリシーの両方で使用されていることを確認します。



3. ポリシー参照はリンクになっています。アクセス コントロール ポリシーのリンクをクリックします。オブジェクトが、[リセットしてブロック (Block with reset)] のルールで宛先として使用されていることを確認します。
4. Web ブラウザで前に戻ります。Extranet129 のオブジェクト使用状況ページを再度開きます。今回はプレフィルタ ポリシーへのリンクをクリックします。ここで、矛盾があることに注意します。アクセス コントロール ポリシーは Extranet129 へのトラフィックをブロックするように設定されていますが、プレフィルタ ポリシーは Extranet129 へのトラフィックを fastpath するように設定されています。これは、修正しないでください。

ヒット カウントの活用

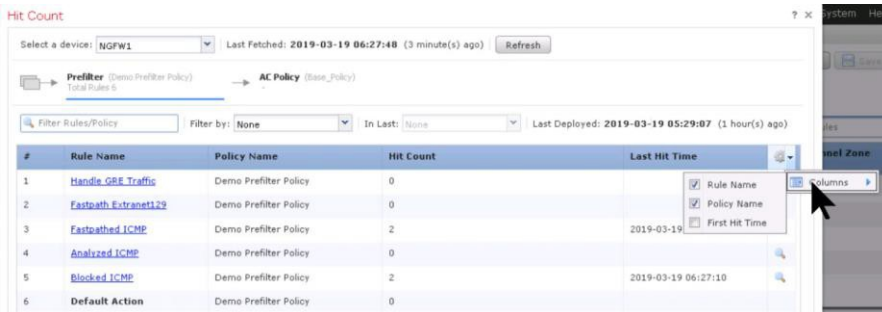
1. 引き続き、プレフィルタ ポリシーのページを使用します。ページの右上隅にある [ヒットカウントの分析 (Analyze Hit Counts)] をクリックします。
2. NGFW1 デバイスを選択し、[現在のヒットカウントの取得 (Fetch Current Hit Count)] をクリックします。



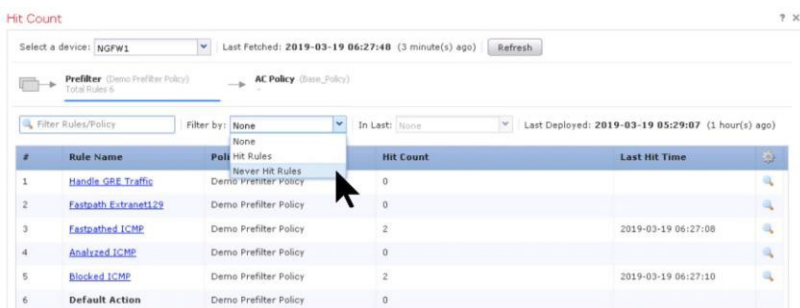
注：プレフィルタ ルールでは、ヒット カウントは fastpath アクションまたはブロック アクションのルールに対してのみ維持されます。分析アクションを設定したルールでは、ヒット カウントは常に 0 になります。

3. 次の機能を検証します。

- a. 歯車アイコンをクリックすると、列を追加または削除できます。[最初のヒット時刻 (First Hit Time)] 列は、デフォルトで非表示に設定されています。



- b. ヒットしたルールのみ、またはヒットしたことがないルールのみを表示できます。

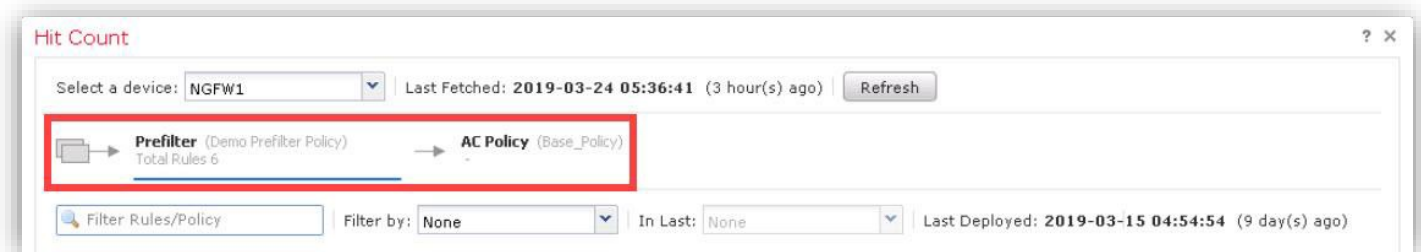


- c. 虫眼鏡のアイコンをクリックしてフィルタリングすることで、ルールを精査できます。

- d. ルール名を右クリックすると、そのルールのルール カウントをクリアできます。

- e. ルール名はリンクになっています。ルール名をクリックすると、プレフィルタ ポリシー内のルールを確認することができます。

4. ヒット カウント ポップアップの [アクセスポリシー (Access Policy)] にピボットします。Base_Policy アクセス コントロール ポリシーに対して、手順 1 ~ 3 を繰り返します。



シナリオ 2： NGFW に SSH でアクセスするための RBAC

6.4 では、NGFW への SSH アクセスに RBAC を導入しています。これには、RADIUS のサービスタイプ属性を使用します。

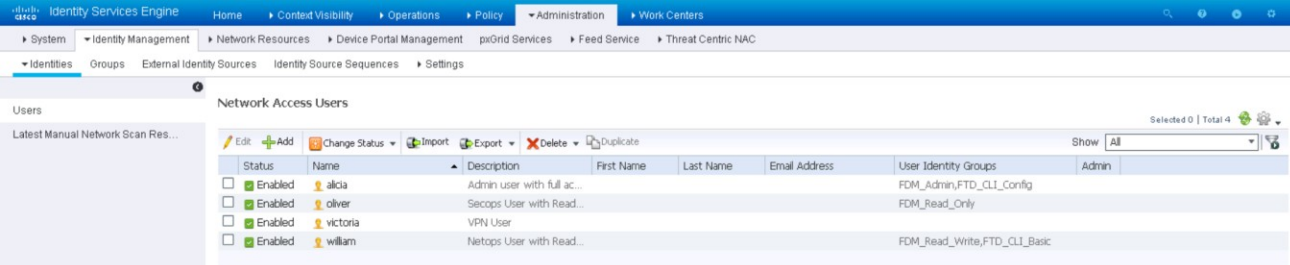
注：6.4 では、NGFW に SSH でアクセスするための RBAC を、FMC と FDM 両方の管理対象デバイスに利用できます。ただし、このラボでは、FMC の管理対象デバイスのみを考慮します。

このシナリオの目的は、3 種類の SSH 認証の動作を対比することです。

- 設定ユーザ：エキスパート モードを含む完全なアクセス権があります。これらのユーザには、6 のサービスタイプ属性が設定されています。Alicia は設定ユーザです。
- 基本ユーザ：アクセスが制限されていて、設定 CLI とエキスパート モードを使用できません。これらのユーザには、6 以外のサービスタイプ属性が設定されています。William は基本ユーザです。
- アクセス権のないユーザ：これらのユーザには、サービスタイプ属性が定義されていません。

ISE 設定の検査 (オプション)

1. 新しいブラウザタブを開いて、ブックマーク バーの [ISE] ブックマークをクリックします。admin として ISE にログインします。パスワードは **C1sco12345** を使用します (これらのクレデンシャルは事前に入力されています)。
2. [管理 (Administration)] > [IDの管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] に移動します。**Alicia、Oliver、William** の [ユーザIDグループ (User Identity Groups)] を確認します。これらは、FDM RBAC と NGFW SSH RBAC の両方をテストするように設定されています。



Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups
Enabled	alicia	Admin user with full ac...				FDM_Admin_FTD_CLI_Config
Enabled	oliver	Secops User with Read...				FDM_Read_Only
Enabled	victoria	VPN User				
Enabled	william	Netops User with Read...				FDM_Read_Write_FTD_CLI_Basic

3. [ポリシー (Policy)] > [ポリシーセット (Policy Sets)] に移動します。[ロールベースアクセスコントロール (Role Based Access Control)] ポリシーセットの右側にある [>] 記号をクリックします。

4. [許可ポリシー (Authorization Policy)] を展開し、以下を確認します。

FDM_Read_Only グループに属している Oliver には **Secops** 認証プロファイルが割り当てられます。

FTD_CLI_Basic グループに属している William には **Netops** 認証プロファイルが割り当てられます。

FTD_CLI_Config グループに属している Alicia には **Firewall_admin** 認証プロファイルが割り当てられます。

▼ Authorization Policy (4)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Secops	InternalUser:IdentityGroup EQUALS User Identity Groups:FDM_Read_Only	× Secops	Select from list	0	⚙️
✓	Netops	InternalUser:IdentityGroup EQUALS User Identity Groups:FDM_Read_Write OR InternalUser:IdentityGroup EQUALS User Identity Groups:FTD_CLI_Basic	× Netops	Select from list	0	⚙️
✓	Admin	InternalUser:IdentityGroup EQUALS User Identity Groups:FDM_Admin OR InternalUser:IdentityGroup EQUALS User Identity Groups:FTD_CLI_Config	× Firewall_Admin	Select from list	0	⚙️
✓	Default		× DenyAccess	Select from list	0	⚙️

5. [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認可 (Authorization)] > [認可プロファイル (Authorization Profiles)] に移動します。3つのプロファイル、**Firewall_Admin**、**Netops**、**Secops** が追加されていることを確認します。

6. 各プロファイル名をクリックし、ページの一番下までスクロールします。サービスタイプ属性値が次のように設定されていることを確認します。**Firewall_Admin** は **6**、**Netops** は **1**、**Secops** は未定義。以下に、Firewall_Admin 認証プロファイルの情報を示します。

▼ Advanced Attributes Settings

Radius:Service-Type	=	Administrative
Cisco:cisco-av-pair	=	fdm.userrole.authority.admin

▼ Attributes Details

```

Access_Type = ACCESS_ACCEPT
Service-Type = 6
cisco-av-pair = fdm.userrole.authority.admin

```

FMC で、NGFW に SSH でアクセスするための RBAC を設定する

1. FMC で、[システム (System)] > [ユーザ (User)] > [外部認証 (External Authentication)] に移動します。[外部認証オブジェクトの追加 (Add External Authentication Object)] をクリックします。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Users User Roles External Authentication

Save Cancel Save and Apply

Default User Role: None Shell Authentication Disabled

Add External Authentication Object

Name	Method	Enabled
------	--------	---------

2. [認証方法 (Authentication Method)] で [RADIUS] を選択します。[外部認証オブジェクト (External Authentication Object)] の [名前 (Name)] を入力します。[ホスト名/IPアドレス (Host Name/IP Address)] に「ise.dcloud.local」と入力します。ポートの設定は **1812** のままにします。[RADIUS秘密キー (RADIUS Secret Key)] に **C1sco12345** を入力します。ページの一番下までスクロールし、[保存 (Save)] をクリックします。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Users User Roles External Authentication

External Authentication Object

Authentication Method: RADIUS

Name: ISEAuth

Description:

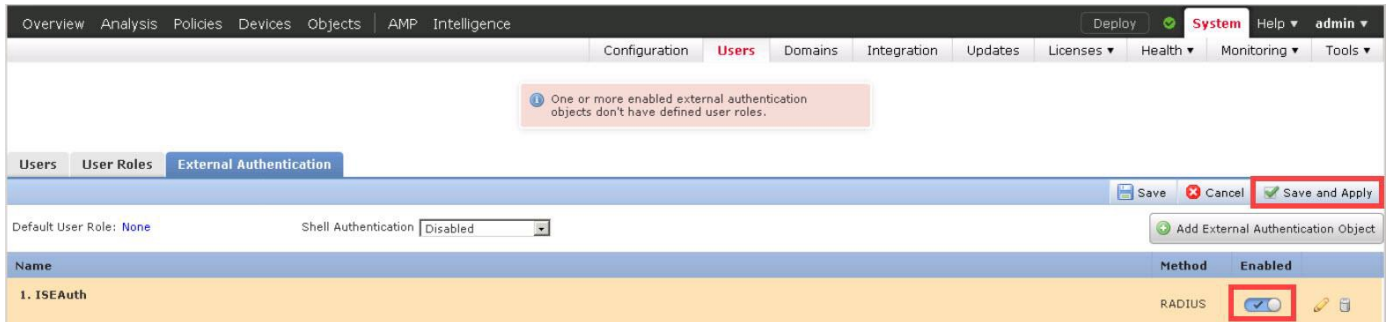
Primary Server

Host Name/IP Address: ise.dcloud.local

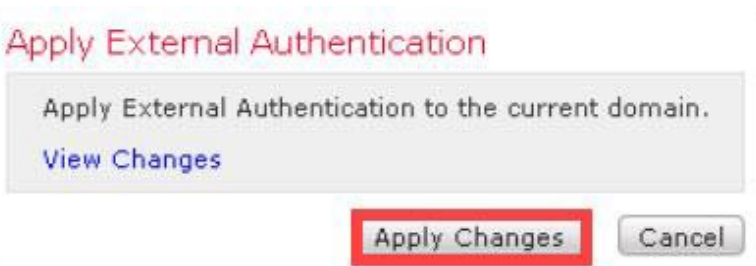
Port: 1812

RADIUS Secret Key: C1sco12345

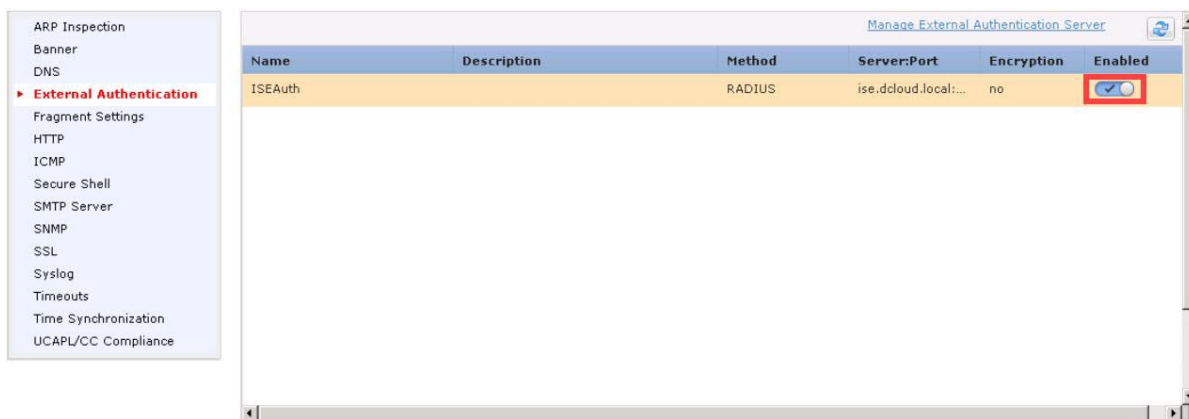
- 外部認証オブジェクトを有効にします。デフォルトのユーザ ロールに関する警告は無視します。[保存して適用 (Save and Apply)]をクリックします。



- 確認画面が表示されたら、[変更の適用 (Apply Changes)]をクリックします。



- [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] に移動して、**NGFW1_Platform_Settings** プラットフォーム設定を編集します。
- 左側のナビゲーション フレームから [外部認証 (External Authentication)] を選択します。外部認証オブジェクトが、すでに存在していることに注意してください。このオブジェクトを有効にします。



- プラットフォーム設定の変更を保存して、NGFW1 に導入します。

NGFW に SSH アクセスするための RBAC をテストする

1. NGFW1 への PuTTY セッションを開きます。
2. **oliver** としてログインを試みます。パスワードは **C1sco12345** を使用します。SSH アクセスが拒否されます。

```

PuTTY (inactive)
login as: oliver
Using keyboard-interactive authentication.
Password:
!!! Your username is not defined with a service type that is valid for this system. You are not authorized to access the system. !!!
Last login: Tue Mar 19 07:34:51 UTC 2019 from jump.dcloud.local on pts/0

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.4.0 (build 1106)
Cisco Firepower Threat Defense for VMWare v6.4.0 (build 49)

```

Oliver が、再度ログインを試みると、FTD は無効なパスワードが入力されたかのようにクレデンシャルを拒否します。

3. PuTTY セッションのタイトル バーを右クリックし、[セッションの再開 (Restart Session)] を選択します。
4. **william** としてログインを試みます。パスワードは **C1sco12345** を使用します。SSH アクセスは拒否されますが、メッセージが異なることに注目します。

```

login as: william
Using keyboard-interactive authentication.
Password:
!!! New external username identified. Please log in again to start a session. !!!

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.4.0 (build 1106)
Cisco Firepower Threat Defense for VMWare v6.4.0 (build 49)

```

5. **william** として再度ログインを試みます。正常にログインできます。「**configure?**」と入力します。William に許可される設定コマンドが、**configure password** のみであることを確認します。また、「**expert**」と入力し、William がエキスパートモードに変更できないことを確認してください。NGFW1 からログアウトします。
6. **alicia** としてログインを試みます。パスワードは **C1sco12345** を使用します。SSH アクセスが拒否されます。William と同じメッセージが表示されます。
7. **alicia** として再度ログインを試みます。正常にログインできます。「**configure?**」と入力します。さまざまな設定コマンドを使用できることを確認します。「**expert**」と入力し、Alicia がエキスパートモードを利用できることを確認します。

シナリオ 3： ファイル イベントを含むユニファイド ロギング

6.3 リリースでは、イベントに関連するアーキテクチャと機能が大幅に変更されました。その主な目的は、NGFW から直接、任意の Syslog サーバに接続イベントを送信できるようにすることです。一部のセキュリティ指向イベント（ポリシー違反イベント）は、引き続き FMC に送信可能です。この機能強化のメリットとしては、FMC のスケーリングや SIEM との統合の強化などが挙げられます。

この拡張機能は、次のようにまとめることができます。

- データ プレーンと Firepower モジュールから送信される Syslog イベントを統合します。FMC での Syslog 設定を簡素化します。
- Syslog イベントにより多くの情報が追加されるため、すべての重要な接続イベントの情報を把握できます。
- 新しい外部ルックアップ機能を利用して SIEM との統合が強化されます。

6.3 では、接続イベントと侵入イベントの両方で、ユニファイド ロギング アーキテクチャを利用できます。6.4 では、ファイル イベントが追加されました。このシナリオの目的：

- Splunk に、接続、侵入、マルウェアの各イベントが送信されるように FMC を設定する
- Splunk への外部ルックアップ クエリを作成してテストする

NGFW1 のプラットフォーム設定を作成する

1. FMC で、[デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] に移動します。
2. **NGFW1_Platform_Settings** プラットフォームの設定を編集します。
3. 左側のナビゲーション ペインで [Syslog] を選択します。[ロギングの設定 (Logging Setup)] タブが選択されます。[ロギングの有効化 (Enable Logging)] チェックボックスをオンにします。

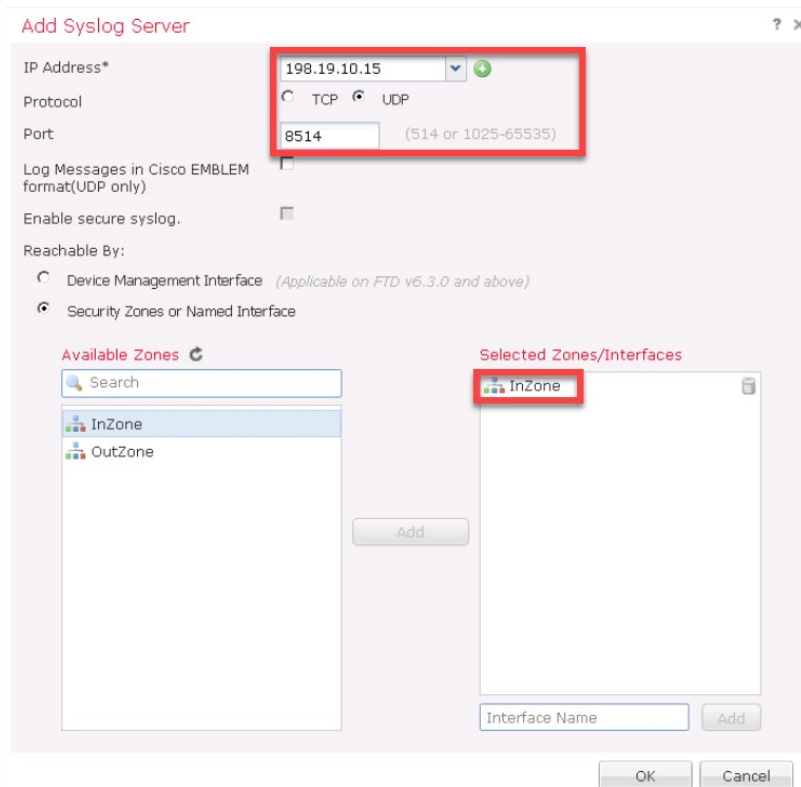
The screenshot shows the 'Logging Setup' configuration page in the FMC interface. The left sidebar contains a navigation menu with 'Syslog' selected. The main content area is divided into several sections:

- Basic Logging Settings:** This section is highlighted with a red box. It includes:
 - Enable Logging
 - Enable Logging on the failover standby unit
 - Send syslogs in EMBLEM format
 - Send debug messages as syslogs
 - Memory Size of the Internal Buffer: 4096 (4096-52428800 Bytes)
- VPN Logging Settings:**
 - Enable Logging to FMC
 - Logging Level: errors (dropdown menu)
- Specify FTP Server Information:**
 - FTP Server Buffer Wrap
 - IP Address: (dropdown menu)
 - Username: (text input field)

4. [Syslogサーバ (Syslog Servers)]タブを選択します。TCP Syslog を使用している場合は、該当のチェックボックスをオフにすることに注意してください。Syslog サーバが使用できない限り、トラフィックは NGFW を通過しません。これにより、ロギングなしではトラフィックが許可されないことが保証されます。このシナリオではこの機能は使用しません。



5. [追加 (Add)] をクリックして、Syslog サーバを追加します。
- [IPアドレス (IP Address)] に「**198.19.10.15**」と入力します。これはポッドの Splunk サーバの IP アドレスです。
 - [UDP] ラジオボタンが選択されていることを確認します。
 - [ポート (Port)] を「**8514**」に変更します。
 - [選択したゾーン/インターフェイス (Selected Zones/Interfaces)] に [InZone] を追加します。



6. [OK] をクリックして Syslog サーバを追加します。[保存 (Save)] をクリックし、プラットフォーム設定への変更を保存します。

NGFW1 の侵入ポリシーを変更する

1. [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [侵入 (Intrusion)] に移動します。
2. [デモ侵入ポリシー (Demo Intrusion Policy)] を編集します。
3. [詳細設定 (Advanced Settings)] をクリックします。[Syslogアラート (Syslog Alerting)] を有効にします。

Edit Policy: Demo Intrusion Policy

The screenshot shows the 'Edit Policy: Demo Intrusion Policy' interface. On the left, a navigation menu has 'Advanced Settings' highlighted with a red box. The main panel is titled 'Advanced Settings' and contains three sections:

- Specific Threat Detection:** Sensitive Data Detection is set to 'Disabled'.
- Intrusion Rule Thresholds:** Global Rule Thresholding is set to 'Enabled'.
- External Responses:** SNMP Alerting is 'Disabled', and Syslog Alerting is 'Enabled' (highlighted with a red box).

4. 鉛筆アイコンをクリックして、[Syslogアラート (Syslog Alerting)] を編集します。[施設 (Facility)] を [LOCAL4] に設定します (接続イベントのログGINGとの整合性を維持するため)。また、[重大度 (Severity)] を [INFO] に設定します。

The screenshot shows the 'Syslog Alerting' configuration page. The left sidebar has 'Syslog Alerting' selected. The main panel is titled 'Syslog Alerting' and contains a 'Settings' section:

- Logging Hosts:** Using default syslog configuration in Access Control Logging. To (Single IP address or comma-separated list)
- Facility:** LOCAL4 (highlighted with a red box)
- Severity:** INFO (highlighted with a red box)

 A 'Revert to Defaults' button is visible at the bottom right.

5. [ポリシー情報 (Policy Information)] をクリックします。[変更を確定 (Commit Changes)] をクリックします。

The screenshot shows the 'Policy Information' page for 'Demo Intrusion Policy'. The left sidebar has 'Policy Information' selected. The main panel shows:

- Name:** Demo Intrusion Policy
- Description:** (empty field)
- Drop when Inline:**
- Base Policy:** Balanced Security and Connectivity
- Status:** The base policy is up to date (Rule Update 2018-10-10-001-vrt)
- Summary:** This policy has 9767 enabled rules (98 rules generate events, 9669 rules drop and generate events)
- Message:** No recommendations have been generated. Click here to set up Firepower recommendations.

 At the bottom, 'Commit Changes' and 'Discard Changes' buttons are visible, with 'Commit Changes' highlighted by a red box.

6. プロンプトが表示されたら [OK] をクリックします。

NGFW1 のアクセス コントロール ポリシーを変更して、その変更を導入する

1. [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [アクセス制御 (Access Control)] の順に選択します。
2. **Base_Policy** を編集します。

3. [ロギング (Logging)] タブを選択します。プラットフォーム設定で設定された Syslog サーバへの [INFO] (以上の) メッセージの送信を有効にします。また、[ファイルとマルウェアの設定 (Files and Malware Settings)] で、ファイル イベントのロギングを有効にします。次の図を見てください。

4. [ルール (Rules)] タブを選択します。デフォルト アクションの前に最後のルールを編集します。このルールの名前は、**Allow Outbound** です。このルールの [ロギング (Logging)] セクションで、[接続開始時にロギング (Log at Beginning of Connection)] と [接続終了時にロギング (Log at End of Connection)] をオンにします。ロギング先を [イベントビューア (Event Viewer)] から [Syslogサーバ (Syslog Server)] に変更します。[保存 (Save)] をクリックして変更を保存します。

5. [保存 (Save)] をクリックして、このルールの変更内容を保存します。
6. [保存 (Save)] をクリックして、アクセスコントロールポリシーの変更を保存します。
7. NGFW1 に変更を導入します。導入が完了するまで待たないでください。

Splunk への外部ルックアップを作成する

注：外部ルックアップは管理対象デバイスに導入されません。FMC でのみ利用可能です。時間を節約するために、設定の導入中にこのタスクを実行します。

1. Jumpbox デスクトップで、**Strings to cut and paste** という名前のファイルを開きます。このファイルの冒頭に 3 つの Splunk クエリがあります。最初のクエリがこのシナリオで使用されます。
2. FMC で、[分析 (Analysis)] > [詳細 (Advanced)] > [状況に応じた相互起動 (Contextual Cross-launch)] に移動します。[新しい相互起動 (New Cross-launch)] をクリックします。
 - a. [名前 (Name)] に「Splunk IP」と入力します。
 - b. [URL テンプレート (URL Template)] に、**Strings to cut and paste** ファイルから以下の文字列を切り取って貼り付けます。**https://splunk.dcloud.local:8000/en-US/app/search/search?q=search "SrcIP%3A {ip}" OR "DstIP%3A {ip}"**。このクエリでは、**{ip}** が唯一の変数です。
 - c. [保存 (Save)] をクリックしてこの相互起動を保存します。

Add Contextual Cross-launch ? ×

Name*
Splunk IP Enabled

URL Template*
https://splunk.dcloud.local:8000/en-US/app/search/search?q=search "SrcIP%3A {ip}" OR "DstIP%3A {ip}"

Click on the variables below to insert them into the URL template. Cross-launches are done by right-clicking an event and these variables will be populated from the event.

ip src_ip dst_ip port src_port dst_port protocol domain sha256

Save

設定をテストする

1. Firefox ブラウザで新しいタブを開きます。ブックマーク ツールバーで [Splunk] ブックマークをクリックします。admin として、パスワード C1sco12345 でログインします（このクレデンシャルは自動的に入力されているはずです）。ログイン後、[FMC] タブに戻ります。
2. NGFW1 の変更内容の導入が完了するまで待ちます。
3. 内部 Linux サーバで **makeevents** コマンドを実行します。これにより、いくつかの、接続、侵入、ファイルのイベントが新しく生成されます。
4. FMC で、[分析 (Analysis)] > [接続 (Connections)] > [イベント (Events)] の順に選択します。
 - a. いずれかの接続イベントで **198.18.133.200** を右クリックします。他の多くのクエリとともに [Splunk IP] クエリが表示されていることに注目します。

Jump to...	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type
↓	2019-03-19 00:32:14	2019-03-19 00:32:14	Allow	Intrusion Monitor	198.19.10.200	USA	18.133.200.108	USA	InZone	OutZone	39730 / tcp
↓	2019-03-19 00:32:14	2019-03-19 00:32:14	Block	Intrusion Block	198.19.10.200	USA	18.133.200.108	USA	InZone	OutZone	39738 / tcp
↓	2019-03-19 00:32:14	2019-03-19 00:32:14	Block	File Block, File Custom Detection	198.19.10.200	USA	18.133.201.108	USA	InZone	OutZone	52285 / tcp
↓	2019-03-19 00:32:14	2019-03-19 00:32:14	Block	Intrusion Block	198.19.10.200	USA	18.133.200.108	USA	InZone	OutZone	51391 / tcp
↓	2019-03-19 00:32:14	2019-03-19 00:32:14	Block	Intrusion Block	198.19.10.200	USA	18.133.200.108	USA	InZone	OutZone	37768 / tcp
↓	2019-03-19 00:32:14	2019-03-19 00:32:14	Block	File Block	198.19.10.200	USA	18.133.200.108	USA	InZone	OutZone	60284 / tcp
↓	2019-03-19 00:32:13	2019-03-19 00:32:13	Block	File Block	198.19.10.200	USA	18.133.202.108	USA	InZone	OutZone	43742 / tcp
↓	2019-03-19 00:32:13	2019-03-19 00:32:13	Block	File Block	198.19.10.200	USA	18.133.200.108	USA	InZone	OutZone	49285 / tcp
↓	2019-03-19 00:32:13	2019-03-19 00:32:13	Block	File Block, File Custom Detection	198.19.10.200	USA	18.133.200.108	USA	InZone	OutZone	48248 / tcp
↓	2019-03-19 00:32:13	2019-03-19 00:32:13	Block	File Block	198.19.10.200	USA	18.133.202.108	USA	InZone	OutZone	43744 / tcp
↓	2019-03-19 00:32:12	2019-03-19 00:32:12	Allow	File Monitor	198.19.10.200	USA	18.133.201.108	USA	InZone	OutZone	57860 / tcp
↓	2019-03-19 00:32:12	2019-03-19 00:32:12	Block	File Block	198.19.10.200	USA	18.133.201.108	USA	InZone	OutZone	57864 / tcp

b. [Splunk IP] を選択してクリックします。これにより新しいタブで Splunk が起動します。

c. FMC のイベント ビューアで表示されなかったイベントが多く存在することを確認します。詳細情報を確認します (ネットワーク プロトコルによって内容は異なります)。

5. 5 つのイベント タイプがあり、イベント タイプ ID がそれぞれ異なります。

430001 - 侵入イベント

430002 - 接続の開始

430003 - 接続の終了

430004 - ファイル イベント

430005 - ファイル マルウェア イベント

これらの各番号をフィルタに追加することで、各イベント タイプと、そのイベント タイプに関連するオブザーバ情報を検索します。たとえば、次のスクリーンショットでは、イベント タイプ ID 430005 を示しています。SHA256 や脅威名など、マルウェアに関連する情報が表示されています。

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query: `"SrcIP: 198.19.10.200" OR "DstIP: 198.19.10.200" 430005`. The search results show 7 events. The first event is expanded, showing details for a file malware event (Event ID 430005) on 3/18/19 at 9:42:09 PM. The event details include: `%FTD-6-430005: SrcIP: 198.19.10.200, DstIP: 198.18.133.200, SrcPort: 60320, DstPort: 80, Protocol: tcp, FileDirection: Download, FileAction: Malware Block, FileSHA256: 76a1f5167239655d91277c79b2c6e8f3746d62924350fc099f7e217b0d58e6622, SHA_Disposition: Malware, SperoDisposition: Spero detection, SperoReason: Spero detected on file, ThreatName: PUA.Win.Adware.Betterinternet.100.sbx.vioc, FileName: Buddy.exe, FileType: MSEXE, FileSize: 155648, ApplicationProtocol: HTTP, Client: wget, User: No Authentication Required, FirstPacketSecond: 2019-03-19T04:42:27Z, FilePolicy: Demo File Policy, URI: http://outside/malware/Buddy.exe`. The event is associated with host 198.19.10.1.

6. (オプション) FMC で、[分析 (Analysis)] > [ファイル (Files)] > [マルウェアイベント (Malware Events)] に移動します。[イベントのテーブルビュー (Table View of Events)] にドリルダウンします。いずれかの IP アドレスを右クリックします。使用可能なアクションを確認します。
7. (オプション) FMC で、[分析 (Analysis)] > [侵入 (Intrusions)] > [イベント (Events)] に移動します。[イベントのテーブルビュー (Table View of Events)] にドリルダウンします。いずれかの IP アドレスを右クリックします。使用可能なアクションを確認します。

シナリオ 4： FMC におけるリモート アクセス VPN の強化

6.4 の FMC では、新しい機能が追加され、有効かつセキュアなリモート アクセス VPN ソリューションをセットアップできるようになりました。多要素認証 (MFA) と ISE ポスチャ評価を、次世代ファイアウォール機能に連携させることで、リモート VPN ユーザの可視性が向上し、きわめて詳細なレベルでのポリシー適用が可能になります。MFA を有効にするには、クライアント証明書、RADIUS クレデンシャル (AD と統合された ISE) 、 Duo OTP を組み合わせるほか、Push 方式を採用します。また、MFA をポスチャ評価とともに使用して、セカンダリ認証サーバまたは二重認証を導入できます。FMC では、LDAPS を介した Duo クラウドへの直接接続、または RADIUS ベースの Duo 認証プロキシを介した接続によって Duo と統合できます。どちらの方法も検証します。

注：このシナリオでは ISE を使用します。時間の節約のためとラボでの ISE の調整を回避するために、ISE は事前に設定されています。このラボには ISE-PIC も含まれていますが、完全には設定されていません。

このシナリオの目的：

- MFA と、認可変更による ISE ポスチャ評価を使用する RA VPN の設定に必要なオブジェクトを作成する。
- RA VPN セットアップ ウィザードを実行する。
- ISE のポスチャ評価を使用して RA VPN MFA をテストする。

Duo アカウントを作成してモバイル デバイスを登録する

注：すでに Duo アカウントがあり、モバイル デバイスをそのアカウントに登録済みの場合は、このセクションをスキップして、「Firepower アプリケーションを追加して VPN ユーザを Duo アカウントに登録する」セクションに進み、モバイル デバイスを Duo アカウントに登録します。

1. RA VPN 認証の要素として Duo を使用するため、最初に自身の Duo アカウントを設定します。Duo では、無料トライアルアカウントを作成して、モバイル デバイスにリンクさせることができます。これは、ラボ演習で十分に使用できる設定です。
2. <https://duo.com/docs/getting-started> [英語] に移動して「Getting Started」セクションの手順 1 ~ 4 に従います。

DUO

Get Your Free Duo Account
Current customers can upgrade now to try more features.


First Name Last Name

Email Address

Company / Account Name

I'm an MSP, Reseller, or Partner

By signing up I agree to the Terms and Services Privacy Notice.

I'm not a robot  hCAPTCHA Privacy - Terms

[Create My Account](#)

- 完了したら、次のセクションに進んで、テスト VPN ユーザと Firepower アプリケーションを自分のアカウントに追加できます。

Firepower アプリケーションを追加して VPN ユーザを Duo アカウントに登録する

- [Duo Admin Panel](#) [英語] にログインし、[Applications] に移動します。
- アプリケーション リストで [Cisco Firepower Threat Defense VPN] を見つけます。

Dashboard > Applications > Protect an Application


Protect an Application

Add an application that you'd like to protect with Duo two-factor authentication.
You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#)

Choose an application below to get started.

firepower

 **Cisco Firepower Threat Defense VPN** [Protect this Application](#) | [Read the documentation](#)

3. [Protect this Application] をクリックして、統合キー、秘密キー、および API のホスト名を取得します。

Dashboard > Applications > Cisco Firepower Threat Defense VPN

Cisco Firepower Threat Defense VPN

Authentication Log | Remove Application

Follow the [Cisco Firepower Threat Defense \(FTD\) Remote Access VPN application instructions](#).

Details Reset Secret Key

Integration key	DIBS6UGGW1KH44Y7LJCH	select
Secret key	Click to view.	select
Don't write down your secret key or share it with anyone.		
API hostname	api-29acc416.duosecurity.com	select

注：秘密キーはパスワードと同じように取り扱う

Duo アプリケーションのセキュリティは、秘密キー (skey) のセキュリティに関連付けられています。機密性の高いクレデンシャルと同じようにそれを保護します。どのような場合にも、それを、許可されていない個人と共有したり、電子メールで他人に送信したりしないでください。

4. このアプリケーションに関連付けられた機能は、「ポリシー」など、その他にも多数ありますが、このラボでは取り上げません。
5. ここで、テストに使用する VPN ユーザ アカウントを追加してみましょう。[Duo Admin Panel] の [Users] に移動し、[Add User] をクリックします。[Username] フィールドに「**vpnuser**」と入力し、[Add User] をクリックします。

Dashboard > Users > Add User

Add User

Adding Users
Most applications allow users to enroll themselves after they complete primary authentication.
[Learn more about adding users](#)

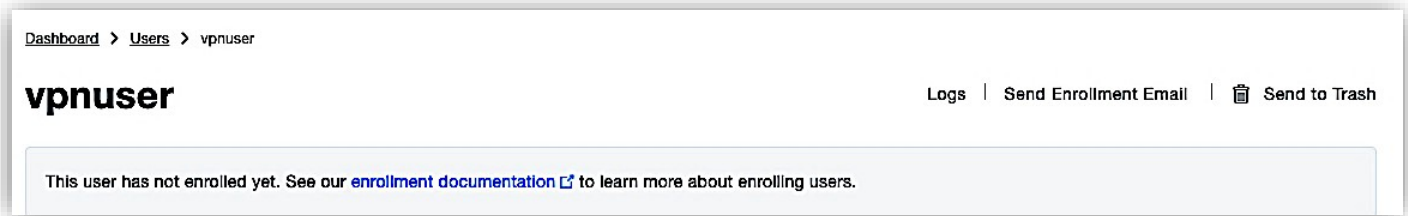
Username

Should match the primary authentication username.

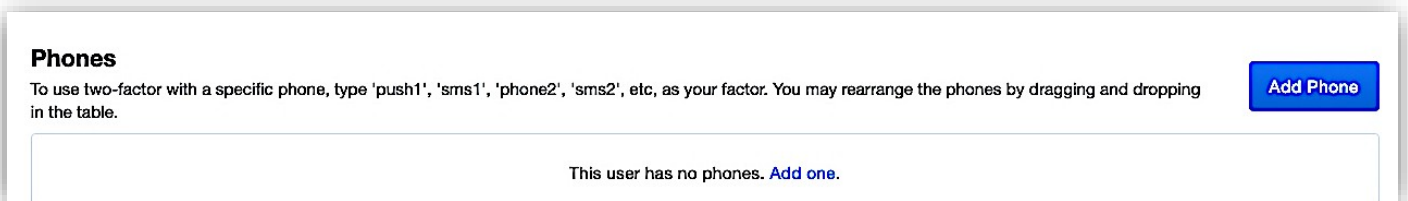
[Add User](#)

注：登録用の SMS メッセージを受信できない場合は、手順 6 に従ってください。それ以外の場合は、手順 7 に進みます。

- [vpnuser] ダッシュボードで、登録に使用できる電子メールアドレスを追加します。[Save Changes] をクリックします。ここで、[Send Enrollment Email] リンクをクリックすると、電話番号やその他の 2FA 認証デバイスを追加できるリンクが含まれたメッセージを受信できます。手順 12 に進みます。



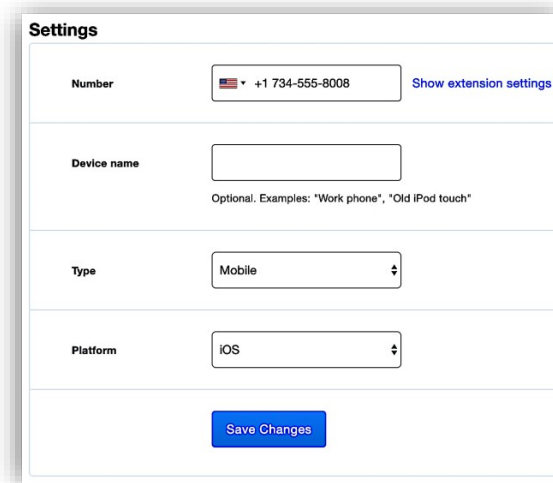
- 登録メッセージが送信されるように、[vpnuser] ダッシュボードで電話番号を追加します。新しいユーザの詳細ページを下にスクロールして [Phones] テーブルに移動し、[Add Phone] をクリックします。



- [Phone] を選択し、電話番号を入力します（タブレットを追加する場合は、このフィールドは空白のままにします）。[Add Phone] ボタンをクリックします。

The screenshot shows the 'Add Phone' form. The breadcrumb navigation is 'Dashboard > Users > avandalay > Add Phone'. The title is 'Add Phone'. There are two radio buttons for 'Type': 'Phone' (selected) and 'Tablet'. Below this, there is a 'Phone number' field with a dropdown menu showing '+1 734-555-8008' and a 'Show extension field' link. At the bottom, there is an 'Add Phone' button.

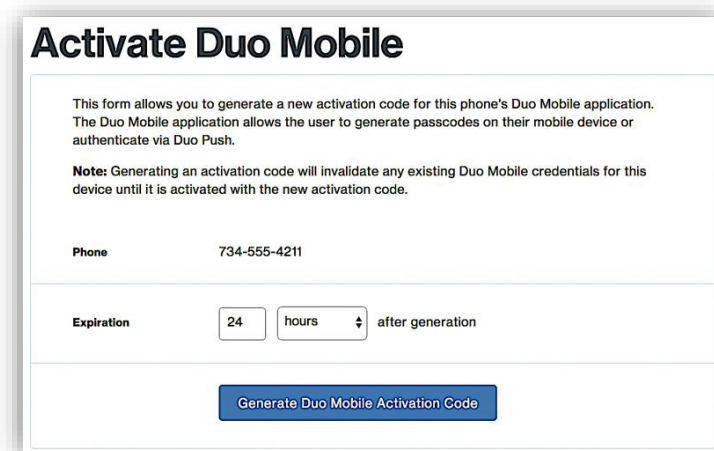
- ドロップダウンメニューから適切な電話の [Type] と [Platform] を選択し、[Device name] を入力します（このフィールドは空白のままでも構いません）。デバイスがスマートフォンであることがわかっていて、プラットフォームが不明の場合は、[Generic Smartphone] を選択します。実際のプラットフォームは、ユーザがアクティベーションを完了したときに設定されます。[Save Changes] ボタンをクリックします。



The screenshot shows a 'Settings' form with the following fields:

- Number:** A text input field containing '+1 734-555-8008' with a country code dropdown set to 'US'. A link 'Show extension settings' is to the right.
- Device name:** An empty text input field. Below it, a note reads: 'Optional. Examples: "Work phone", "Old iPod touch"'. A 'Save Changes' button is at the bottom.
- Type:** A dropdown menu with 'Mobile' selected.
- Platform:** A dropdown menu with 'iOS' selected.

- [Device Info] セクションで [Activate Duo Mobile] リンクをクリックします。このリンクは、電話機のタイプを [Mobile] に設定し、プラットフォームに [Unknown] 以外を選択した場合にのみ使用できます。次のページで [Duo Mobile Activation Code] ボタンをクリックします。



The screenshot shows the 'Activate Duo Mobile' page with the following content:

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: 734-555-4211

Expiration: 24 hours after generation

Generate Duo Mobile Activation Code

11. 次に、送信可能な 2 つのテキスト メッセージが表示されます。最初のメッセージには、ユーザが Duo Mobile をインストールするのに役立つリンクがあります。2 番目のメッセージには、アカウントを、自分の Duo Mobile アプリにすぐに追加できるコードがあります。[Send Instructions by SMS] ボタンをクリックして、ユーザの電話機にテキスト メッセージを送信します。

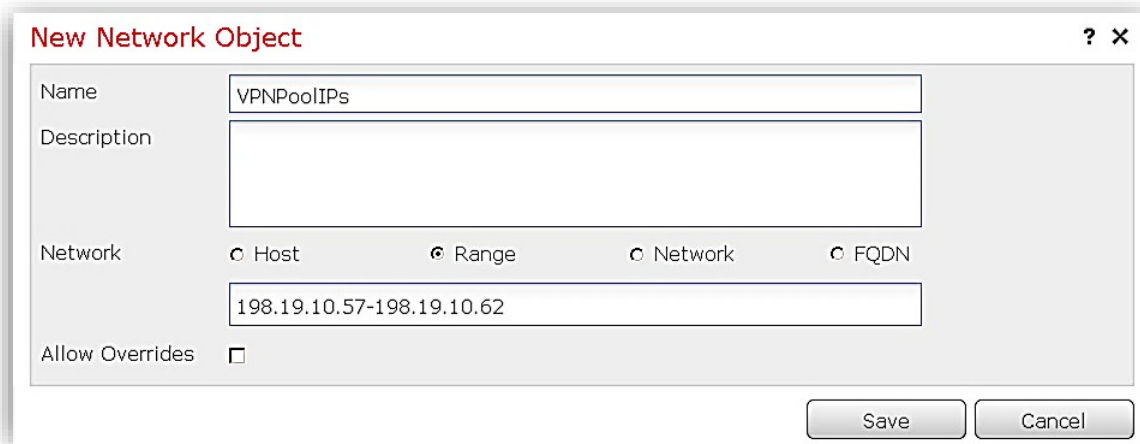
12. 電子メール メッセージまたは SMS メッセージが届きます。それには、アクティベーション リンクと QR コードのほか、すべてのサポート対象プラットフォームの Duo Mobile アプリにアクセス可能なリンクが記載されています。デバイスでリンクを開くか、Duo Mobile アプリで QR コードをスキャンして、Duo アカウントを追加し、vpuser を有効にする必要があります。完了すると、Duo アカウントが追加され、vpuser が完全に有効になります。

このシナリオに必要なオブジェクトを作成する

注：これらのオブジェクトのほとんどは、RA VPN ウィザードを実行しながら作成できます。RA VPN 設定のコンポーネントに慣れていない管理者には、ウィザードの方が効率的なアプローチかもしれませんが、このシナリオでは独立したタスクでオブジェクトを作成します。オブジェクトを作成しておくことで、RA VPN ウィザードを後で容易に実行できます。

1. FMC で、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] に移動します。

- [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順にクリックします。「VPNPoolIPs」という IP 範囲オブジェクトを、IP アドレス範囲を「198.19.10.57-198.19.10.62」に設定して作成します。このオブジェクトは、NAT 免除の作成に使用されます。



New Network Object ? X

Name: VPNPoolIPs

Description:

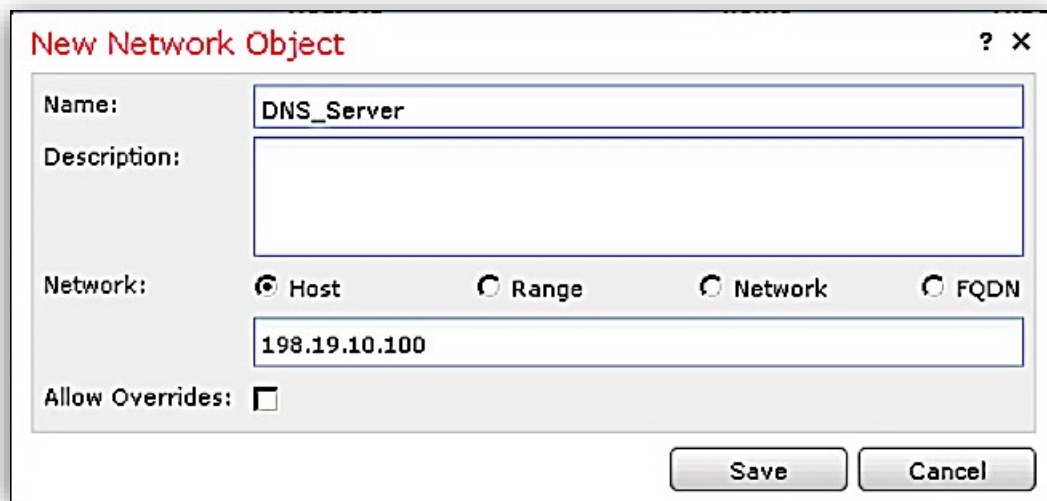
Network: Host Range Network FQDN

198.19.10.57-198.19.10.62

Allow Overrides:

Save Cancel

- [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順にクリックします。「LAN_Network」というホスト オブジェクトを、IP アドレスを「198.19.10.0/24」に設定して作成します。



New Network Object ? X

Name: DNS_Server

Description:

Network: Host Range Network FQDN

198.19.10.100

Allow Overrides:

Save Cancel

4. [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順にクリックします。「ISE_Server」というホストオブジェクトを、IPアドレスを「198.19.10.130」に設定して作成します。

New Network Object ? X

Name: LAN_Network

Description:

Network: Host Range Network FQDN

198.19.10.0/24

Allow Overrides:

Save Cancel

5. [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] の順にクリックします。「DNS_Server」というホストオブジェクトを、IPアドレスを「198.19.10.100」に設定して作成します。

New Network Object ? X

Name: ISE_Server

Description:

Network: Host Range Network FQDN

198.19.10.130

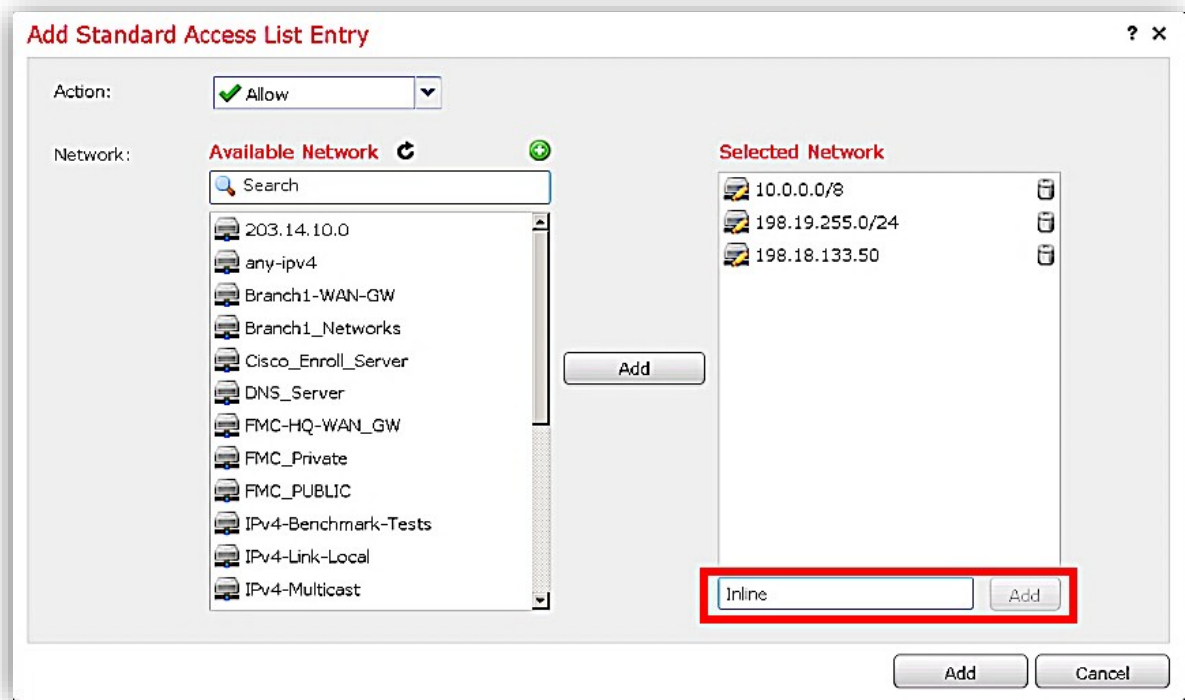
Allow Overrides:

Save Cancel

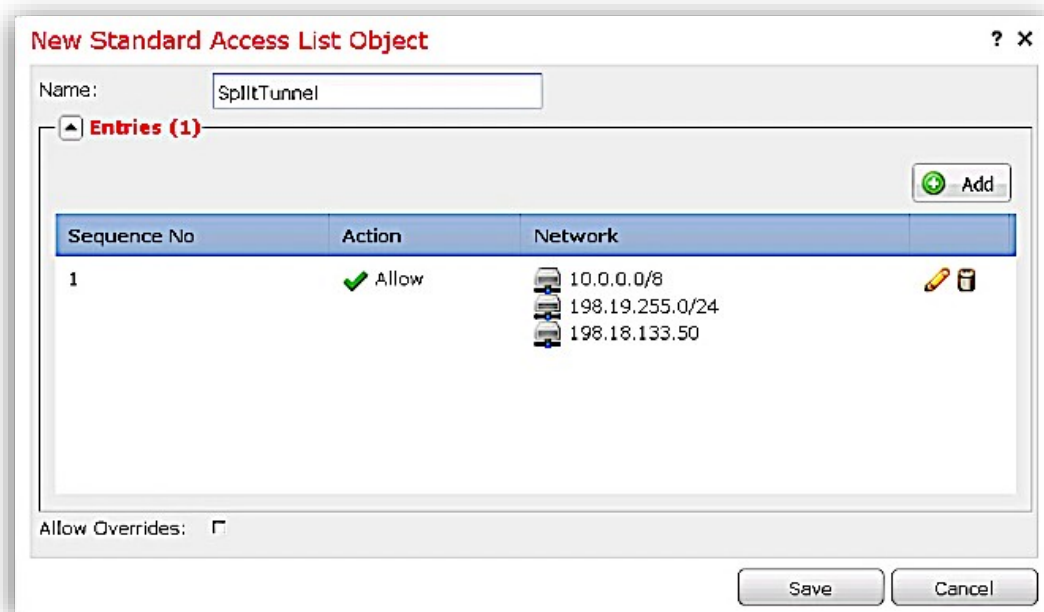
注：最も強力なセキュリティを実現するために、スプリットトンネリングは使用しないことをお勧めします。ただし、AnyConnect を実行するエンドポイントのコンソール アクセスがないため、このシナリオではスプリットトンネリングを使用する必要があります。dCloud でエンドポイントにアクセスするにはさまざまな方法があるため、これらすべての潜在的なアクセスアドレスを回避する標準 ACL を作成する必要があります。これを、ここで行います。

6. 左側のナビゲーション ペインで、[アクセスリスト (Access List)] > [標準 (Standard)] の順に選択します。[標準アクセスリストを追加 (Add Standard Access List)] をクリックします。

7. **10.0.0.0/8**、**198.19.255.0/24**、および **198.18.133.50** を許可する ACE を使用して、「SplitTunnel」という標準アクセスリストを作成します。これを行うには、[選択済みネットワーク (Selected Network)]ボックスの下のテキストボックスにこれらのネットワークを入力し、[追加 (Add)]をクリックします。



8. [保存 (Save)]をクリックしてアクセスリストを保存します。



9. 左側のナビゲーション ペインから、[アクセスリスト (Access List)] > [拡張 (Extended)] の順に選択します。[拡張アクセスリストの追加 (Add Extended Access List)] をクリックします。
10. 以下のような「**redirect**」という拡張アクセス リストを作成します。これは、ポスチャ評価の実行時に ISE にリダイレクトされるトラフィックの決定に使用されます。[アクション (Action)] が [ブロック (Block)] の ACE は、リダイレクトから除外されます。

Edit Extended Access List Object

Name:

Entries (3)

Sequence	Action	Source	Source Port	Destination	Destination Port	
1	Block	Any	Any	ISE_Server	TCP (6):8443	
2	Block	Any	Any	DNS_Server	DNS_over_UDP	
3	Allow	Any	Any	Any	Any	

Allow Overrides:

Save Cancel

11. 左側のナビゲーション ペインから、[アドレスプール (Address Pools)] > [IPv4プール (IPv4 Pools)] の順に選択します。[IPv4プールの追加 (Add IPv4 Pools)] をクリックします。
 - a. [名前 (Name)] に「**VPNPool**」と入力します。
 - b. [IPv4アドレス範囲 (IPv4 Address Range)] に「**198.19.10.57-198.19.10.62**」と入力します。
 - c. [マスク (Mask)] に「**255.255.255.248**」と入力します。

Add IPv4 Pool

Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

! Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

Save Cancel

注：VPNPoolIPs オブジェクトと VPNPool オブジェクトは IP アドレス範囲が同じですが、オブジェクト型は異なります。VPNPool は RA VPN オブジェクトで参照され、VPNPoolIPs は NAT 免除の設定に使用されます。

12. 左側のナビゲーション ペインから、[VPN] > [AnyConnectファイル (AnyConnect Files)] の順に選択します。
13. [AnyConnectファイルの追加 (Add AnyConnect File)] をクリックします。[参照 (Browse)] をクリックし、Jumpbox デスクトップの **RA VPN** フォルダから **AnyConnectProfile.xml** ファイルを選択します。残りのフィールドには自動入力されます。

Add AnyConnect File ? X

Name:* AnyConnectProfile.xml

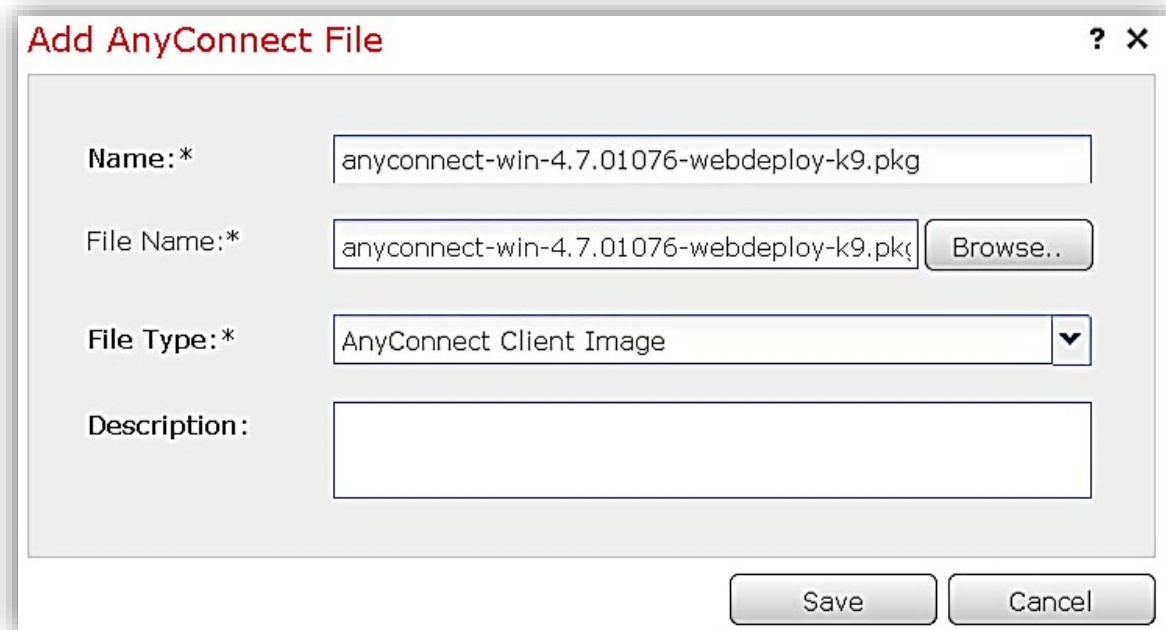
File Name:* AnyConnectProfile.xml Browse..

File Type:* AnyConnect Client Profile ▼

Description:

Save Cancel

14. [AnyConnectファイルの追加 (Add AnyConnect File)] をクリックします。[参照 (Browse)] をクリックし、Jumpbox デスクトップの RA VPN フォルダから **anyconnect-win-4.7.01076-webdeploy-k9.pkg** を選択します。残りのフィールドには自動入力されます。



Add AnyConnect File ? X

Name:* anyconnect-win-4.7.01076-webdeploy-k9.pkg

File Name:* anyconnect-win-4.7.01076-webdeploy-k9.pkg Browse..

File Type:* AnyConnect Client Image ▼

Description:

Save Cancel

15. 左側のナビゲーション ペインから、[PKI] > [証明書の登録 (Cert Enrollment)] の順に選択します。[証明書の登録の追加 (Add Cert Enrollment)] をクリックします。
 - a. [名前 (Name)] に「**NGFW1_Outside**」と入力します。
 - b. [登録タイプ (Enrollment Type)] ドロップダウン メニューから [PKCS12ファイル (PKCS12 File)] を選択します。
 - c. [参照 (Browse)] をクリックし、Jumpbox デスクトップの **Certificates** フォルダから **ngfw-dcloud.pfx** を選択します。
 - d. [パスフレーズ (Passphrase)] に「**C1sco12345**」と入力します。

Add Cert Enrollment ? X

Name* NGFW1_Outside

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: ngfw-dcloud.pfx

Passphrase: ●●●●●●●●

Allow Overrides

ISE の RADIUS サーバグループを作成し設定する

1. 左側のナビゲーション ペインから、[RADIUSサーバグループ (RADIUS Server Group)] を選択します。[RADIUSサーバグループの追加 (Add RADIUS Server Group)] をクリックします。
 - a. グループ名を「**ISE_RADIUS**」にします。
 - b. [動的な許可を有効にする (Enable dynamic authorization)] チェックボックスをオンにします。
 - c. 緑色の [+] 記号をクリックして RADIUS サーバを追加します。
2. 次の情報を入力します (その他の属性はデフォルトのままにしておきます)。
 - a. [IPアドレス/ホスト名 (IP Address/Hostname)] に「**198.19.10.130**」と入力します。
 - b. [キー (Key)] に「**C1sco12345**」と入力します。
 - c. [特定のインターフェイス (Specific interface)] ラジオボタンを選択し、ドロップダウン メニューから [InZone] を選択します。

- d. [リダイレクトACL (Redirect ACL)] に [redirect] を選択します。

Edit RADIUS Server ? X

IP Address/Hostname:* 198.19.10.130
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* 1812 (1-65535)

Key:* ●●●●●●●●

Confirm Key:* ●●●●●●●●

Accounting Port: 1813 (1-65535)

Timeout: 10 (1-300) Seconds

Connect using: Routing Specific Interface ⓘ

InZone

Redirect ACL: redirect

Save Cancel

3. [保存 (Save)] をクリックし、この RADIUS サーバを RADIUS サーバグループに追加します。完了すると、RADIUS サーバグループは以下になるはずですが、[保存 (Save)] をクリックします。

Edit RADIUS Server Group ? X

Name:* ISE_RADIUS

Description:

Group Accounting Mode: Single

Retry Interval:* 10 (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update

Interval:* 24 (1-120) hours

Enable dynamic authorization

Port:* 1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
198.19.10.130

Save Cancel

注：実装する Duo 統合のタイプに応じて、次の 2 つのセクションのいずれかを実行できます。1 つ目は、ファイアウォールと Duo クラウド間の LDAPS 直接接続を使用します。2 つ目は、ラボの目的に合わせて設定済みの認証プロキシサーバを使用します。LDAPS 方式では、Duo Application Dashboard で取得した、統合キー、秘密キー、および API のホスト名を手元に保持する必要があります。

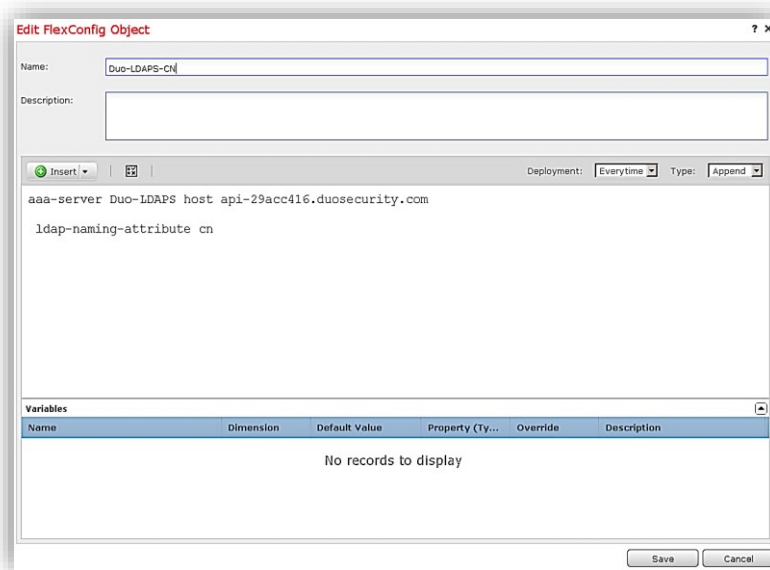
3. [保存 (Save)]をクリックします。レルムの状態を有効にします。

Group Attribute	State
uniqueMember	<input checked="" type="checkbox"/>

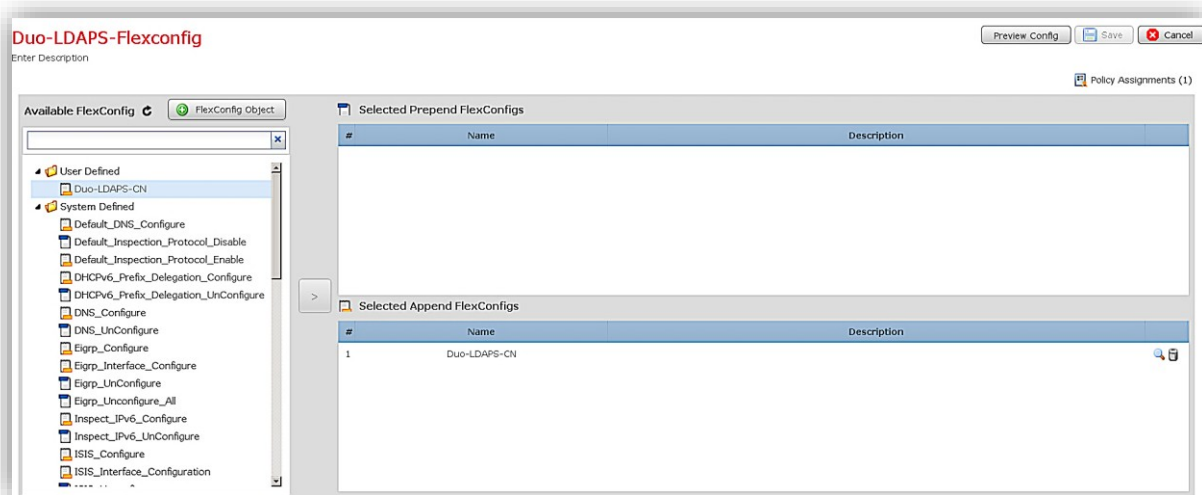
4. もう 1 つ注意すべき点があります。Duo では、**cn** が **LDAP ネーミング属性**である必要があります。これは LDAP サーバの UI では設定できないため、Flexconfig を使用します。[デバイス (Devices)] > [FlexConfig] に移動します。
5. [新しいポリシーの追加 (Add a new Policy)]をクリックします。
 - a. 名前を **Duo-LDAPS-Flexconfig** に設定します。
 - b. デバイスとして **NGFW1** を追加し、[保存 (Save)]をクリックします。

6. [+ FlexConfigオブジェクト (+ FlexConfig Object)] をクリックします。
 - a. [名前 (Name)] に Duo-LDAPS-CN を入力します。
 - b. [導入 (Deployment)] を [毎回 (Everytime)] に変更します。
 - c. 次の設定行を追加します。

```
aaa-server Duo-LDAPS host <API のホスト名>
  ldap-naming-attribute cn
```



- d. [保存 (Save)] をクリックします。
7. 新しく作成したオブジェクトを [使用可能なFlexConfig (Available FlexConfig)] から選択して追加します。 [保存 (Save)] をクリックします。



デバイスには、まだ変更を導入しないでください。

Duo 認証プロキシの RADIUS サーバ オブジェクトを作成して設定する

1. 便宜上、すでに、内部の Active Directory サーバで Duo 認証プロキシ アプリケーションを設定しています。このサーバへの RDP セッションを開始して、認証プロキシの設定ファイルを確認できます。このファイルは、**C:\Program Files (x86)\Duo Security Authentication Proxy\conf** にあります。

```

; Complete documentation about the Duo Auth Proxy can be found
here:
; https://duo.com/docs/authproxy_reference

; MAIN: Include this section to specify global configuration
options.
; Reference: https://duo.com/docs/authproxy_reference#main-
section
; [main]

; CLIENTS: Include one or more of the following configuration
sections.
; To configure more than one client configuration of the same
type, append a
; number to the section name (e.g. [ad_client2])

[duo_only_client]

; SERVERS: Include one or more of the following configuration
sections.
; To configure more than one server configuration of the same
type, append a
; number to the section name (e.g. radius_server_auto1,
radius_server_auto2)

[radius_server_auto]
ikey=DIBS6UGGW1KH44Y7LJCH
skey=aHGHby4M4f8cnmwDuXzQS0M0ADtHxgtRJcmzq7lO
api_host=api-29acc416.duosecurity.com
radius_ip_1=198.19.10.1
radius_secret_1=C1scol2345
radius_ip_2=198.19.10.2
radius_secret_2=C1scol2345
radius_ip_3=198.19.10.3
radius_secret_3=C1scol2345
failmode=safe
client=duo_only_client

```

2. **ikey**、**skey**、および **api_host** を、Duo アカウントの値に変更します。完了後、保存してファイルを閉じます。
3. AD サーバで、**Services.msc** を開き、**Duo 認証プロキシ**のサービスを再起動します。これが成功したことを確認します。
4. **C:\Program Files (x86)\Duo Security Authentication Proxy\bin** に移動して、**authproxy_connectivity_tool** を実行します。

5. 接続テストが成功したかどうかを確認するには、**C:\Program Files (x86)\Duo Security Authentication Proxy\log** に移動し、**connectivity_tool** ファイルを開きます。ファイルの一番下までスクロールし、次のログが出力されていることを確認します。

```

2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] Testing section 'duo_only_client' with
configuration:
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] {}
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] There are no configuration problems 2019-03-
17T23:38:08+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] Testing section 'radius_server_auto' with
configuration:
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] {'api_host': 'api-29acc416.duosecurity.com',
'client': 'duo_only_client',
'failmode': 'safe',
'apikey': 'DIBS6UGGW1KH44Y7LJCH',
'port': '1812',
'radius_ip_1': '198.19.10.1',
'radius_ip_2': '198.19.10.2',
'radius_ip_3': '198.19.10.3',
'radius_secret_1': '*****',
'radius_secret_2': '*****',
'radius_secret_3': '*****',
'skey': '*****[40]'}
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] There are no configuration problems
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] Testing section 'duo_only_client' with
configuration:
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] {}
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] No testing to be done for section.
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] Testing section 'radius_server_auto' with
configuration:
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] {'api_host': 'api-29acc416.duosecurity.com',
'client': 'duo_only_client',
'failmode': 'safe',
'apikey': 'DIBS6UGGW1KH44Y7LJCH',
'port': '1812',
'radius_ip_1': '198.19.10.1',
'radius_ip_2': '198.19.10.2',
'radius_ip_3': '198.19.10.3',
'radius_secret_1': '*****',
'radius_secret_2': '*****',
'radius_secret_3': '*****',
'skey': '*****[40]'}
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] The RADIUS Server has no connectivity problems.
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] SUMMARY
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] No issues detected

```

6. FMC で、[オブジェクト (Object)] > [RADIUSサーバグループ (RADIUS Server Group)] に移動します。
7. [RADIUSサーバグループの追加 (Add RADIUS Server Group)] をクリックします。
- Duo_Auth_Proxy** グループを呼び出します。
 - 緑色の [+] 記号をクリックして RADIUS サーバを追加します。

8. 次の情報を入力します（その他の属性はデフォルトのままにしておきます）。
- [IPアドレス/ホスト名 (IP Address/Hostname)]に「**198.19.10.100**」と入力します。
 - [キー (Key)]に「**C1sco12345**」と入力します。
 - [特定のインターフェイス (Specific interface)]ラジオボタンを選択し、ドロップダウン メニューから [InZone] を選択します。

New RADIUS Server

IP Address/Hostname:* 198.19.10.100
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* 1812 (1-65535)

Key:*

Confirm Key:*

Accounting Port: 1813 (1-65535)

Timeout: 10 (1-300) Seconds

Connect using: Routing Specific Interface ⓘ

InZone

Redirect ACL:

InZone

OutZone

Save Cancel

9. [保存 (Save)]をクリックし、この RADIUS サーバを RADIUS サーバグループに追加します。完了すると、RADIUS サーバグループは以下になるはずですが、[保存 (Save)]をクリックします。

Add RADIUS Server Group

Name:* Duo_Auth_Proxy

Description:

Group Accounting Mode: Single

Retry Interval:* 10 (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update

Interval:* 24 (1-120) hours

Enable dynamic authorization

Port:* 1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
198.19.10.100

NGFW1 が Duo API のホスト名を解決できるように DNS サーバを設定する

1. [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [DNSサーバグループ (DNS Server Group)] に移動します。[DNSサーバグループの追加 (Add DNS Server Group)] をクリックします。
 - a. [名前 (Name)] に「**DCloud-DNS**」と入力します。
 - b. [デフォルトドメイン (Default Domain)] に「**dcloud.local**」と入力します。
 - c. [DNSサーバ (DNS Server)] に「**198.19.10.100**」を入力します。
 - d. [保存 (Save)] をクリックします。

New DNS Server Group Object ? x

Name*:

Default Domain:

Timeout:
Range: 1 - 30 Seconds

Retries:
Range: 0 - 10

DNS Servers:
(Multiple values in IPv4 or IPv6 addresses can be specified as comma separated entries)

2. [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] の順に選択します。[新しい脅威防御設定ポリシーの追加 (Add a new Threat Defense Settings Policy)] をクリックします。
 - a. [名前 (Name)] に「**NGFW1_Platform_Settings**」を入力します。
 - b. [選択されたデバイス (Selected Device)] に [NGFW1] を追加します。
 - c. [保存 (Save)] をクリックします。

New Policy ? x

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

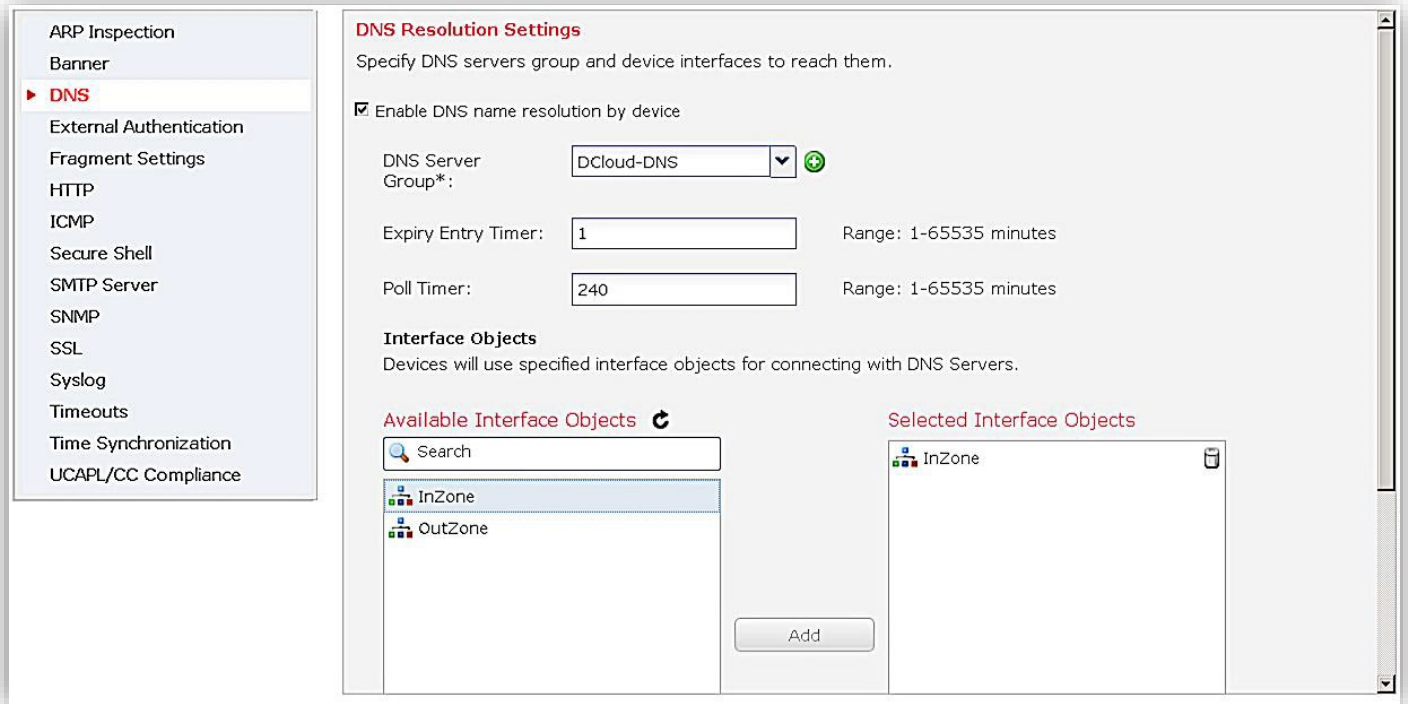
Available Devices

NGFW1
NGFWBR1

Selected Devices

NGFW1

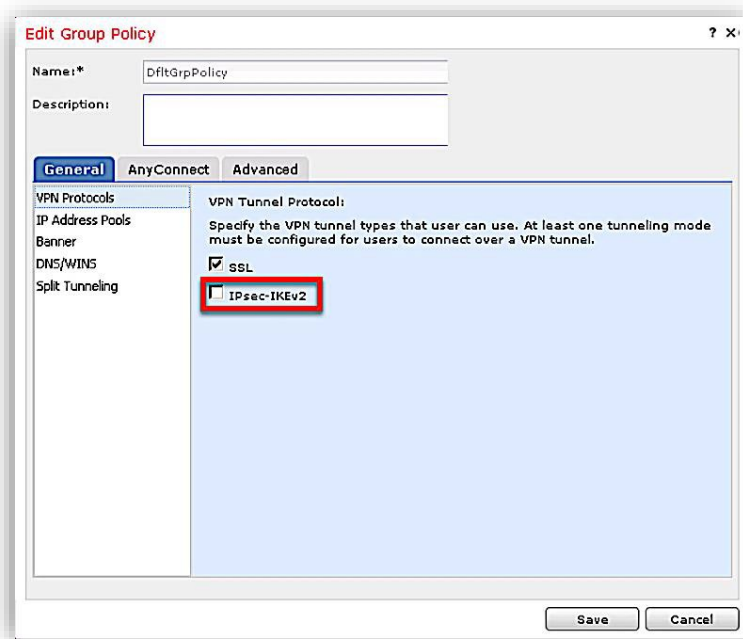
3. [DNS] に移動します。
 - a. [デバイスによるDNS名解決を有効にする (Enable DNS name resolution by device)] をオンにします。
 - b. [DNSサーバグループ (DNS Server Group)] ドロップダウンから [DCloud-DNS] を選択します。
 - c. [インターフェイスオブジェクト (Interface Objects)] に [InZone] を追加します。
 - d. [保存 (Save)] をクリックします。



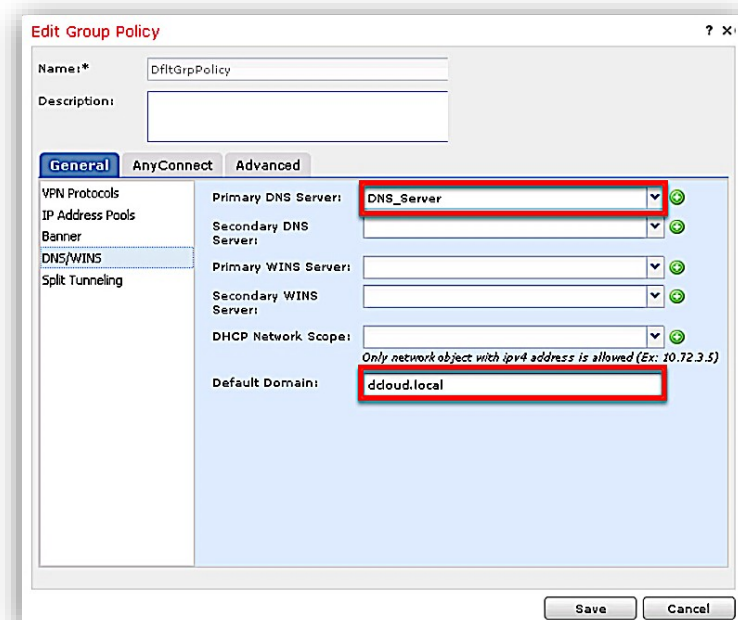
デフォルト グループ ポリシー (DfltGrpPolicy) を編集する

注：通常 VPN グループ ポリシーの編集 (または新しいグループ ポリシーの追加) は、RA VPN ウィザードの実行中に行います。ここでは、作業の明確化のためと RA VPN ウィザードの実行を容易にするために、このタスクを独立して行います。

1. 左側のナビゲーション ウィンドウで、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [VPN] > [グループポリシー (Group Policy)] に移動します。鉛筆アイコンをクリックして、**DfltGrpPolicy** を編集します。
2. [一般 (General)] > [VPNプロトコル (VPN Protocols)] の下で、[IPsec-IKEv2] をオフにします。



3. [一般 (General)] > [DNS/Wins] を選択します。
 - a. [プライマリDNSサーバ (Primary DNS Server)] ドロップダウン リストから [DNS_Server] を選択します。
 - b. [デフォルトドメイン (Default Domain)] に「**dcloud.local**」と入力します。



4. [一般 (General)] > [スプリットトンネル (Split Tunnel)] を選択します。
 - a. [IPv4スプリットトンネリング (IPv4 Split Tunneling)] ドロップダウン リストから、[以下に指定したネットワークを除外する (Exclude networks specified below)] を選択します。
 - b. [標準アクセスリスト (Standard Access List)] ドロップダウンリストから、[SplitTunnel] を選択します。

The screenshot shows the 'Edit Group Policy' dialog box with the 'Advanced' tab selected. The 'Split Tunneling' section is active. The 'IPv4 Split Tunneling' dropdown menu is set to 'Exclude networks specified below'. The 'Standard Access List' dropdown menu is set to 'SplitTunnel'. The 'Split Tunnel Network List Type' is set to 'Standard Access List'. The 'DNS Request Split Tunneling' section is also visible, with 'DNS Requests' set to 'Send DNS requests as per split tunnel policy'.

5. [AnyConnect] > [プロファイル (Profiles)] を選択します。[クライアントプロファイル (Client Profile)] ドロップダウン リストから、[AnyConnectProfile.xml] を選択します。

The screenshot shows the 'Edit Group Policy' dialog box with the 'AnyConnect' tab selected. The 'Profiles' section is active. The 'Client Profile' dropdown menu is set to 'AnyConnectProfile.xml'. The 'AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.' text is visible. Below this, there is a note: 'Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from Cisco Software Download Center.'

6. [保存 (Save)] をクリックして **DfltGrpPolicy** への変更を保存します。

注：通常、この時点で AnyConnect ライセンスを有効にすることもできます。ただし、これはすでに設定済みです。それを確認するには [システム (System)] > [ライセンス (Licenses)] > [スマートライセンス (Smart License)] に移動します。FMC で評価ライセンスが使用されている一方で、輸出規制対象の機能が有効になっていることがわかります。通常はこのことは不可能であるため、評価ライセンスでは SSL VPN をライセンス供与できません。

リモート アクセス VPN ウィザードを実行する

1. [デバイス (Devices)] > [VPN] > [リモートアクセス (Remote Access)] に移動します。
2. [追加 (Add)] ボタン、または [新しい設定の追加 (Add new configuration)] テキストをクリックします。
3. [ポリシー割り当て (Policy Assignment)] ページで、以下の手順を実行し、[次へ (NEXT)] をクリックします。
 - a. [名前 (Name)] に「**RAVPN**」と入力します。
 - b. [VPNプロトコル (VPN Protocols)] で [IPsec-IKEv2] をオフにします。
 - c. [ターゲットデバイス (Target Devices)] で [NGFW1] を選択します。

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Targeted Devices and Protocols
This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name: *

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices: Available Devices Selected Devices

Available Devices: Search
NGFW1
NGFWBR1

Selected Devices: NGFW1

Add

Before You
Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server
Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

AnyConnect Client Package
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface
Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

4. [接続プロファイル (Connection Profile)] ページで、以下の手順を実行し、[次へ (NEXT)] をクリックします。
 - a. [認証方式 (Authentication Method)] で、[クライアント証明書とAAA (Client Certificate & AAA)] を選択します。
 - b. ユーザ名は共通名から抽出するため、[証明書のユーザ名 (Username From Certificate)] はそのままにしておきます。
 - c. [認証サーバ (Authentication Server)]、[認可サーバ (Authorization Server)]、[アカウンティングサーバ (Accounting Server)] で、[ISE_RADIUS] を選択します。
 - d. [IPv4アドレスプール (IPv4 Address Pools)] で [VPNPool] を選択します。

Remote Access VPN Policy Wizard

① Policy Assignment → ② Connection Profile → ③ AnyConnect → ④ Access & Certificate → ⑤ Summary

Connection Profile:
 Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
 Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

Authentication Server:* (Real or RADIUS)

Authorization Server: (RADIUS)

Accounting Server: (RADIUS)

Client Address Assignment:
 Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools: ⓘ

IPv6 Address Pools:

Group Policy:
 A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* ⓘ
[Edit Group Policy](#)

5. [AnyConnect] ページで、利用可能な唯一の AnyConnect イメージを選択し、[次へ (Next)] をクリックします。

Remote Access VPN Policy Wizard

① Policy Assignment → ② Connection Profile → ③ AnyConnect → ④ Access & Certificate → ⑤ Summary

Remote User → AnyConnect Client → Internet → Outside → VPN Device → Inside → Corporate Resources

AnyConnect Client Image
 The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#). [Show Re-order buttons](#) ⓘ

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	anyconnect-win-4.7.01076-webd...	anyconnect-win-4.7.01076-webdeploy-k9.pkg	Windows

6. [アクセスと証明書 (Access & Certificate)] ページで、以下の手順を実行し、[次へ (NEXT)] をクリックします。
- [インターフェイスグループ/セキュリティゾーン (Interface group/Security Zone)] で、[OutZone] を選択します。
 - [証明書の登録 (Certificate Enrollment)] で、[NGFW1_Outside] を選択します。
 - [復号されたトラフィックでアクセスコントロールポリシーをバイパスする (sysopt permit-vpn) (Bypass Access Control policy for decrypted traffic (sysopt permit-vpn))] チェックボックスはオンにしないでください。このチェックボックスをオンにすると、内部ネットワークへの VPN トラフィックは Snort をバイパスします。

Remote Access VPN Policy Wizard

① Policy Assignment > ② Connection Profile > ③ AnyConnect > ④ Access & Certificate > ⑤ Summary

Network Interface for Incoming VPN Access
 Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone: *

Enable DTLS on member interfaces

Device Certificates
 Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment: *

Select on the target devices

Access Control for VPN Traffic
 All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

7. [サマリー (Summary)] ページで設定を確認します。ネットワーク インターフェイス設定に関する警告は無視できます。[完了 (Finish)] をクリックします。また、[終了 (Finish)] をクリックすると、デバイス証明書の登録が自動的に開始され、ステータスが [デバイス (Device)] > [証明書 (Certificates)] に表示されます。

Remote Access VPN Policy Wizard

① Policy Assignment > ② Connection Profile > ③ AnyConnect > ④ Access & Certificate > ⑤ Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: RAVPN

Device Targets: NGFW1

Connection Profile: RAVPN

Connection Alias: RAVPN

AAA:

Authentication Method: Client Certificate & AAA

Username From Certificate: CN (Common Name) & OU (Organisational Unit)

Authentication Server: ISE_RADIUS

Authorization Server: ISE_RADIUS

Accounting Server: ISE_RADIUS

Address Assignment:

Address from AAA: -

DHCP Servers: -

Address Pools (IPv4): VPNPool

Address Pools (IPv6): -

Group Policy: DRtGrpPolicy

AnyConnect Images: anyconnect-win-4.7.01076-webdeploy-k9.pkg

Interface Objects: OutZone

Device Certificates: NGFW1_Outside

Device Identity Certificate Enrollment

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

① **Access Control Policy Update**
 An `Access_Control` rule must be defined to allow VPN traffic on all targeted devices.

① **NAT Exemption**
 If NAT is enabled on the targeted devices, you must define a `NAT_Policy` to exempt VPN traffic.

① **DNS Configuration**
 To resolve hostname specified in AAA Servers or CA Servers, configure DNS using `FlexConfig_Policy` on the targeted devices.

① **Port Configuration**
 SSL will be enabled on port 443. Please ensure that these ports are not used in `NAT_Policy` or other services before deploying the configuration.

⚠ **Network Interface Configuration**
 Make sure to add interface from targeted devices to SecurityZone object 'OutZone'

8. Duo の設定を RAVPN プロファイルに適合させるために、これから、セカンダリ認証サーバとして追加します。
9. [接続プロファイル (Connection Profile)] タブの **RAVPN** プロファイルを編集します。

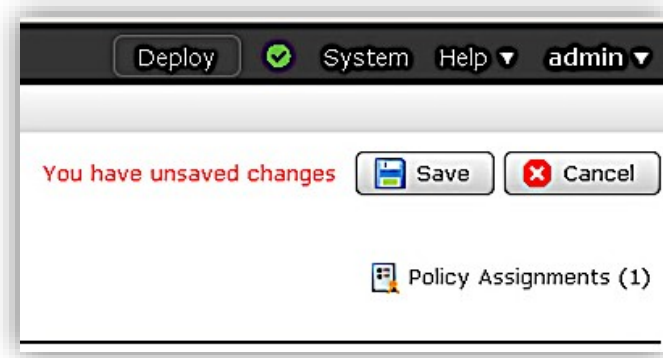
10. [AAA] タブに移動し、[セカンダリ認証を使用 (Use secondary authentication)] を選択します。
 - a. [クライアント証明書からのユーザ名のマッピング (Map username from client certificate)] を展開します。[ユーザログインウィンドウの証明書からユーザ名を事前入力 (Prefill username from certificate on user login window)] を選択します。
 - b. 選択した Duo 統合の方法に応じて、[認証サーバ (Authentication Server)] に [Duo-LDAPS] または [Duo_Auth_Proxy] のいずれかを選択します。次の手順では、[Duo-LDAPS] を使用します。
 - c. [セカンダリ認証のユーザ名 (Username for secondary authentication)] を展開し、[クライアント証明書からのユーザ名のマッピング (Map username from client certificate)] を選択します。
 - d. [ユーザログインウィンドウの証明書からユーザ名を事前入力 (Prefill username from certificate on user login window)] を選択します。[ログインウィンドウのユーザ名を非表示 (Hide username in login window)] を選択します。
 - e. [保存 (Save)] をクリックします。

The screenshot shows the 'Edit Connection Profile' dialog box with the following configuration:

- Connection Profile: RAVPN
- Group Policy: DftGrpPolicy
- Client Address Assignment: AAA
- Map username from client certificate:
 - Map specific field:
 - Primary Field: CN (Common Name)
 - Secondary Field: OU (Organisational Unit)
 - Use entire DN (Distinguished Name) as username:
 - Prefill username from certificate on user login window:
 - Hide username in login window:
- Use secondary authentication:
 - Authentication Server: Duo-LDAPS (LDAP)
 - Username for secondary authentication:
 - Map username from client certificate:
 - Map specific field:
 - Primary Field: CN (Common Name)
 - Secondary Field: OU (Organisational Unit)
 - Use entire DN (Distinguished Name) as username:
 - Prefill username from certificate on user login window:
 - Hide username in login window:
 - Use primary authentication username:
 - Prompt:

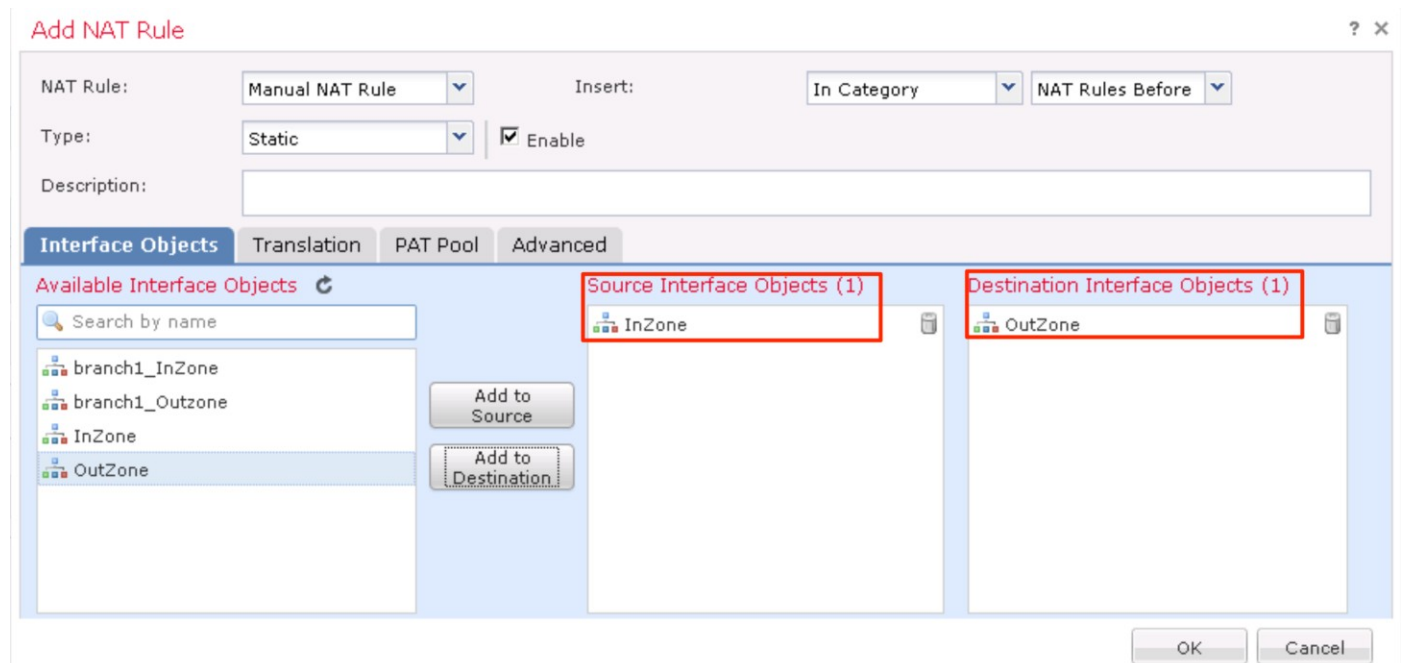
Buttons: Save, Cancel

11. [保存 (Save)] をクリックします。



NAT 免除の追加

1. [デバイス (Devices)] > [NAT] に移動します。デフォルト NAT ポリシーと呼ばれる NAT ポリシーを編集します。
2. [ルールの追加 (Add Rule)] をクリックします。
 - a. [送信元インターフェイスオブジェクト (Source Interface Objects)] に [InZone] を選択し、[宛先インターフェイスオブジェクト (Destination Interface Objects)] に [OutZone] を選択します。



- b. [変換 (Translation)] タブで、[元の送信元 (Original Source)] および [変換済み送信元 (Translated Source)] として [LAN_Network] を選択します。[元の宛先 (Original Destination)] および [変換済み宛先 (Translated Destination)] として [VPNPoolIPs] を選択します。

Add NAT Rule ? x

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="LAN_Network"/>	Translated Source: <input type="text" value="Address"/>
Original Destination: <input type="text" value="Address"/>	Translated Source: <input type="text" value="LAN_Network"/>
<input type="text" value="VPNPoolIPs"/>	Translated Destination: <input type="text" value="VPNPoolIPs"/>
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text"/>	Translated Destination Port: <input type="text"/>

- c. [OK] をクリックして NAT ルールを保存します。

3. NAT ポリシーの最後のルールを編集します。[送信元インターフェイスオブジェクト (Source Interface Objects)] を [InZone] から [any] に変更します。これで、インターネットを送信先とする VPN クライアントからのトラフィックが正しく NAT 処理されるようになります。[OK] をクリックして、NAT ルールの変更を保存します。

Edit NAT Rule ? x

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Available Interface Objects

- branch1_InZone
- branch1_Outzone
- InZone
- OutZone

Source Interface Objects (0)

Destination Interface Objects (1)

4. [保存 (Save)] をクリックして NAT ポリシーの変更を保存します。

アクセス コントロール ポリシーを変更する

1. [ポリシー (Policies)] > [アクセス制御 (Access Control)] に移動し、[Base_Policy] というアクセス ポリシーを編集します。
2. [ルールの追加 (Add Rule)] をクリックします。
 - a. このルールの名前を「**RAVPN_Access**」にします。
 - b. [挿入 (Insert)] を [ルールの上 (above rule)] に設定し、[7] を指定します。
 - c. [アクション (Action)] を [許可 (Allow)] に設定します。
 - d. [ゾーン (Zones)] タブで、[OutZone] を [送信元ゾーン (Source Zones)] に追加します。

Add Rule ? x

Name: Enabled Insert:

Action:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Zones

- InZone
- OutZone**
- GRE

Source Zones (1):

Destination Zones (0):

- e. [ネットワーク (Networks)] タブで、[VPNPoolIPs] を [送信元ネットワーク (Source Networks)] に追加します。

Add Rule ? x

Name: Enabled Insert:

Action:

Zones **Networks** VLAN Tags Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Networks

Networks Geolocation

- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast
- ISE_Server
- LAN_Network
- VPNPoolIPs
- wwwin
- wwwout

Source Networks (1)

Source	Original Client
VPNPoolIPs	

- f. [インスペクション (Inspection)] タブで、侵入ポリシーに [デモ侵入ポリシー (Demo Intrusion Policy)] を選択し、ファイルポリシーに [デモファイルポリシー (Demo File Policy)] を選択します。

Add Rule ? x

Name: Enabled Insert:

Action:

Zones Networks VLAN Tags Applications Ports URLs SGT/ISE Attributes **Inspection** Logging Comments

Intrusion Policy: Variable Set:

File Policy:

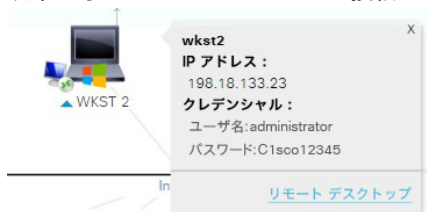
- g. [ロギング (Logging)] タブで、[接続終了時にロギング (Log at End of Connection)] をオンにします。イベントは FMC のイベント ビューアに送信されます。これによりトラブルシューティングが容易になりますが、多くの場合、実稼働環境では実行されません。

3. [追加 (Add)]、[保存 (Save)] の順にクリックします。

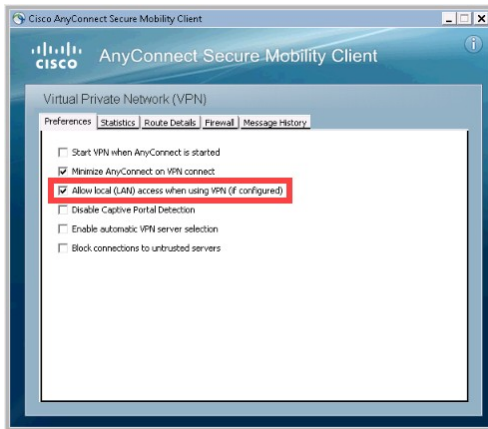
設定を導入しテストする

注：このシナリオでは、コンプライアンス対応システムの定義は、デスクトップに compliant.txt というファイルを持つシステムです。この演習では、Wkst2 は非コンプライアンス対応として開始されます。また、Wkst2 には、ポスチャ モジュールがインストールされています。

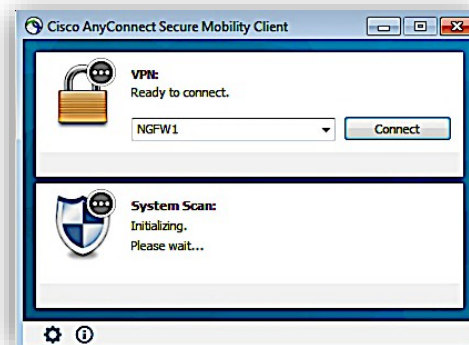
1. 設定を導入し、導入が完了するまで待ちます。
2. **Wkst2** に接続します。管理者として自動的にログインされます。2 つの方法のいずれかを使用して接続できます。
 - 以下に示すトポロジ マップから接続します。これは推奨される方法です。



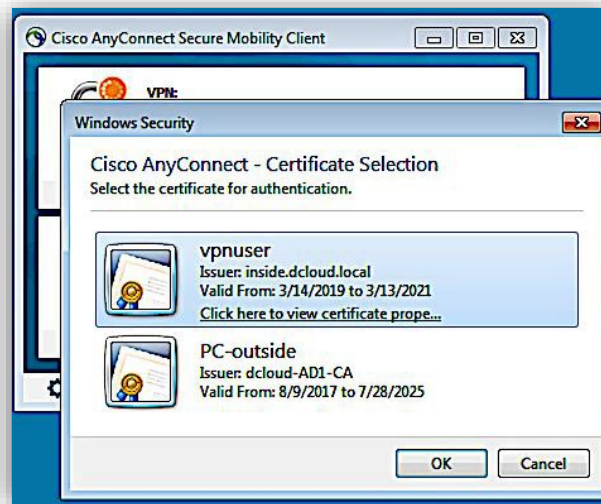
- Jumpbox デスクトップの **Remote Desktops** フォルダの **Wkst2 (Outside PC)** ショートカットをクリックします。ただし、これを行う場合は、AnyConnect クライアントでローカル LAN アクセスを許可する必要があります。



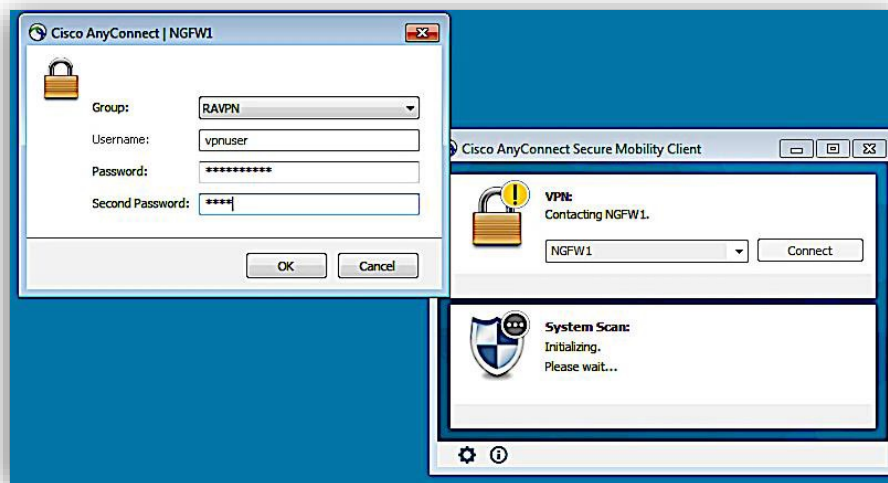
- VPN 経由でポッドに接続している場合は、ラップトップ上の RDP クライアントを使用して **198.18.133.23** に接続します。Administrator としてログインします。パスワードは **C1sco12345** を使用します。
3. [スタート] メニューから AnyConnect を開きます。[接続先 (Connect To)] フィールドに [NGFW1 FQDN] が自動的に入力されます。[接続 (Connect)] をクリックします。



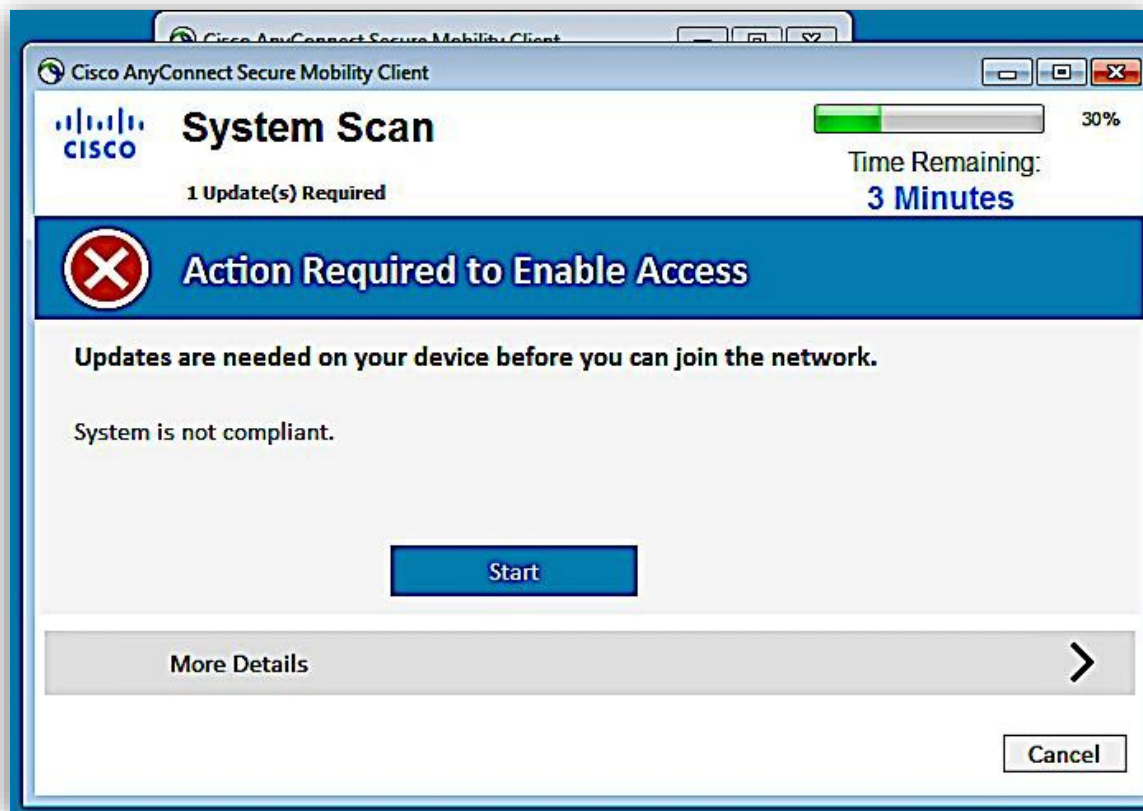
4. テストでは、**vpnuser** と同じ名前のクライアント証明書を使用します。[vpnuser] 証明書を選択します。



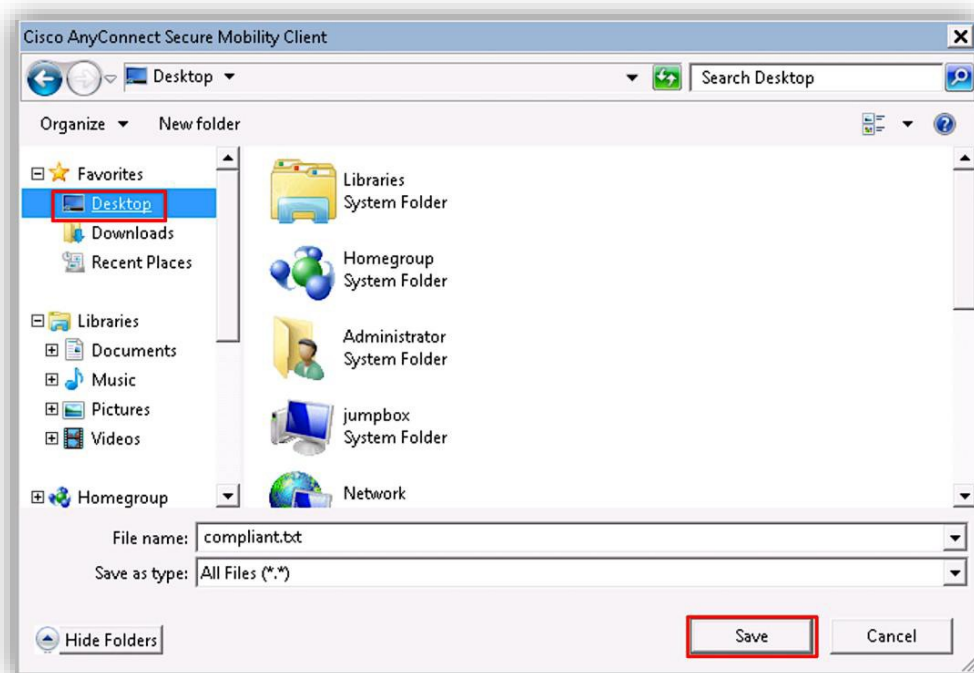
5. [パスワード (Password)] に「**C1sco12345**」を、[2番目のパスワード (Second Password)] に「**push**」を入力します。[OK] をクリックします。Duo 認証で Push 方式を使用するため、ここでは「push」を指定しましたが、必要に応じて電話または SMS を設定できます。モバイル デバイスでプッシュ通知を受け取って承認する必要があります。その際に、VPN トンネルが確立されることがわかります。



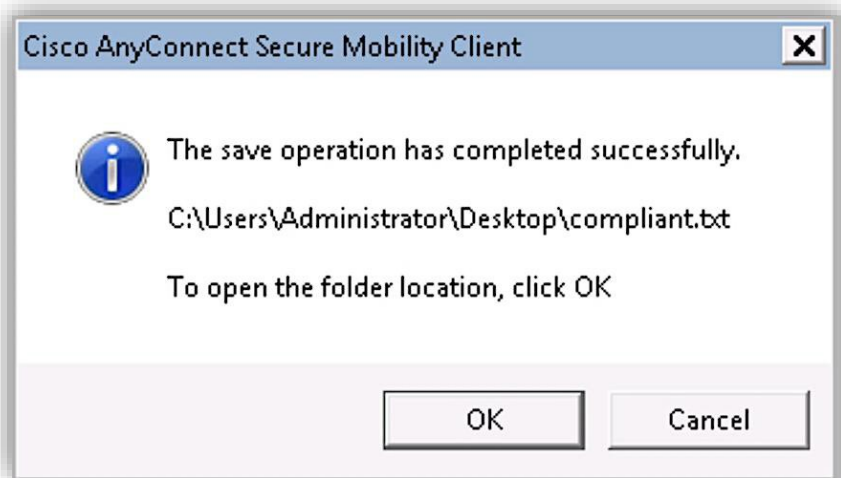
6. 最初の接続で、AnyConnect コンプライアンス モジュールがダウンロードされていることを確認できます。
7. 最初の接続ではシステムが基準を満たしていないため、準拠の対応を求めるプロンプトが表示されます。[開始 (Start)] をクリックします。



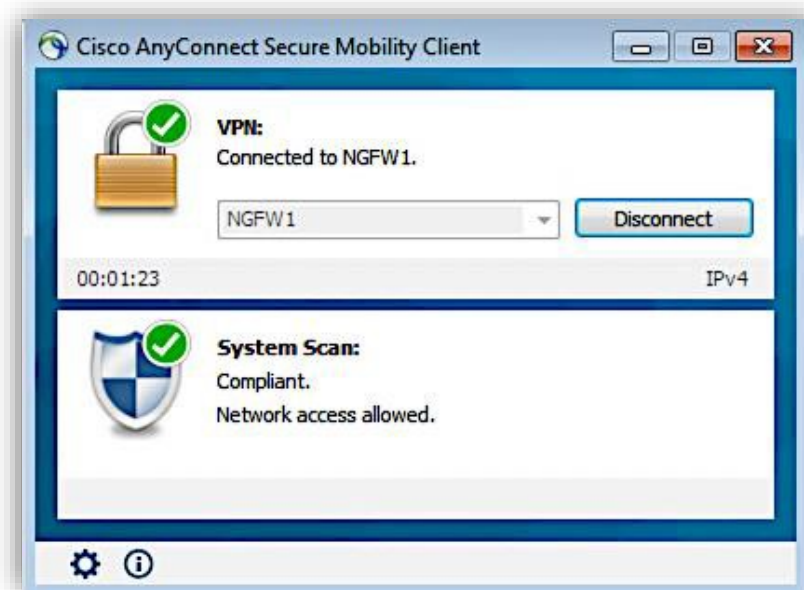
8. **compliant.txt** ファイルの保存を促すプロンプトが表示されます。宛先フォルダを **Desktop** に変更します。



9. 「The save operation has completed successfully」というメッセージが表示されたダイアログボックスでは、[キャンセル (Cancel)] をクリックできます。フォルダを開く必要はありません。



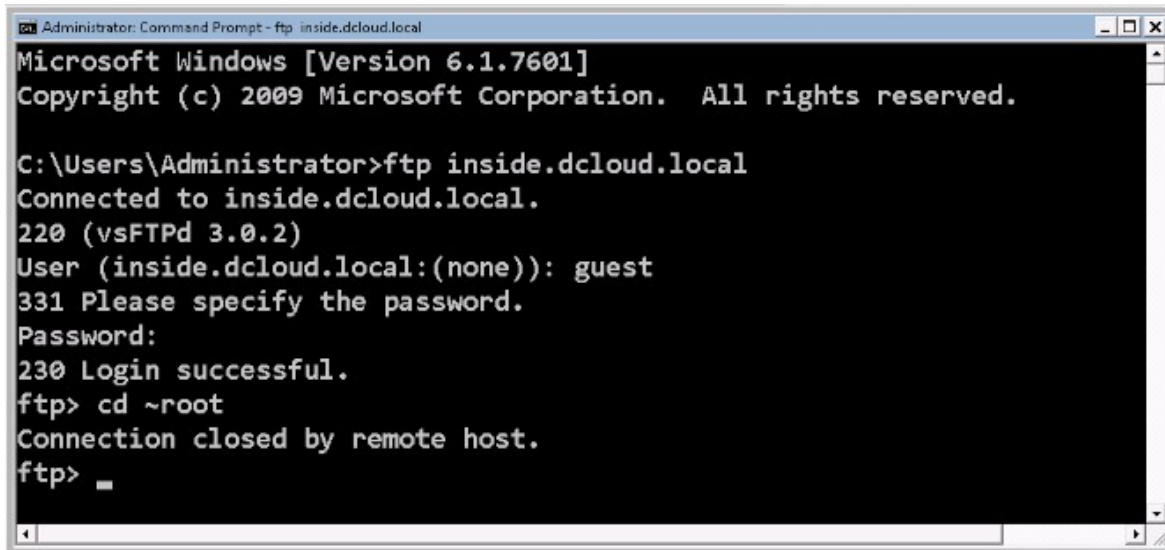
10. ファイルのインストール後、クライアントによってシステムがコンプライアンス対応であることが宣言されます。



11. Wkst2 上の Firefox ブラウザのブックマークを使用して、ブックマークが作成されている 3 つの内部 Web サイト ([内部 (Inside)]、[代替内部 (Alt Inside)]、[内部ハニーポット (Inside Honeypot)]) にアクセスできることを確認します。
12. これらの内部サーバのいずれかで、[ファイル (Files)] リンクをクリックし、[Zombies.pdf] をクリックします。これはマルウェアと見なされるファイルです。ファイルがブロックされることを確認します。ProjectX.pdf のような無害のファイルがブロックされていないことを確認します。

注：クラウドルックアップタイムアウト（これらのポッドで発生することがあります）によって演習が中断されないように、Zombies.pdf ファイルは FMC カスタム検出リストに追加されています。実際にクラウドルックアップを必要とするテストを実行する場合は、URL として「<http://altoutside.dcloud.local/malware>」と入力し、Buddy.exe のダウンロードを試みてください。

13. 侵入がブロックされていることを確認します。これは、Wkst2 でコマンド プロンプトを開き、**inside.dcloud.local** への FTP 接続を確立することによって実行できます。接続を許可します。ゲストとして、パスワード **C1sco12345** でログインします。ログインしたら、「**cd ~root**」と入力します。接続をリセットします。これは、Snort シグネチャ 336 がトリガされたためです。



```
Administrator: Command Prompt - ftp inside.dcloud.local
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp inside.dcloud.local
Connected to inside.dcloud.local.
220 (vsFTPd 3.0.2)
User (inside.dcloud.local:(none)): guest
331 Please specify the password.
Password:
230 Login successful.
ftp> cd ~root
Connection closed by remote host.
ftp> _
```

14. (オプション) FMC で、マルウェア イベント ([分析 (Analyze)] > [ファイル (Files)] > [マルウェアイベント (Malware Events)]) と侵入イベント ([分析 (Analyze)] > [侵入 (Intrusions)] > [イベント (Events)]) を調べます。また、[概要 (Overview)] > [ダッシュボード (Dashboards)] > [アクセス制御されたユーザの統計情報 (Access Controlled User Statistics)] > [VPN] に移動して、RA VPN ユーザの統計情報を調べることもできます。

シナリオ 5： FDM におけるリモート アクセス VPN の強化

以前の Firepower Device Manager (FDM) の RA VPN 機能は非常に基本的なものでした。6.4 では、こうした機能が大幅に拡張され、FMC の機能とほぼ同等になっています。クライアント証明書認証と二重認証（セカンダリ認証サーバ）がサポートされたため、RA VPN に、多要素認証とポストチャ評価（ISE を使用する CoA）を設定できます。このシナリオでは、認証形式の 1 つとして Duo を使用します。FDM で、RADIUS ベースの Duo 認証プロキシを使用して Duo と統合できます。

注：このシナリオでは ISE を使用します。時間の節約のためとラボでの ISE の調整を回避するために、ISE は事前に設定されています。このラボには ISE-PIC も含まれていますが、完全には設定されていません。

このシナリオの目的：

- MFA と、認可変更による ISE ポスチャ評価を使用する RA VPN の設定に必要なオブジェクトを作成する。
- RA VPN セットアップ ウィザードを実行する。
- ISE のポストチャ評価を使用して RA VPN MFA をテストする。

Duo アカウントを作成してモバイル デバイスを登録する

注：すでに Duo アカウントがあり、モバイル デバイスをそのアカウントに登録済みの場合は、このセクションをスキップできます。

1. RA VPN 認証の要素として Duo を使用するため、最初に自身の Duo アカウントを設定します。Duo では、無料トライアルアカウントを作成して、モバイル デバイスにリンクさせることができます。これは、ラボ演習で十分に使用できる設定です。
2. <https://duo.com/docs/getting-started> [英語] に移動して「Getting Started」セクションの手順 1 ~ 4 に従います。

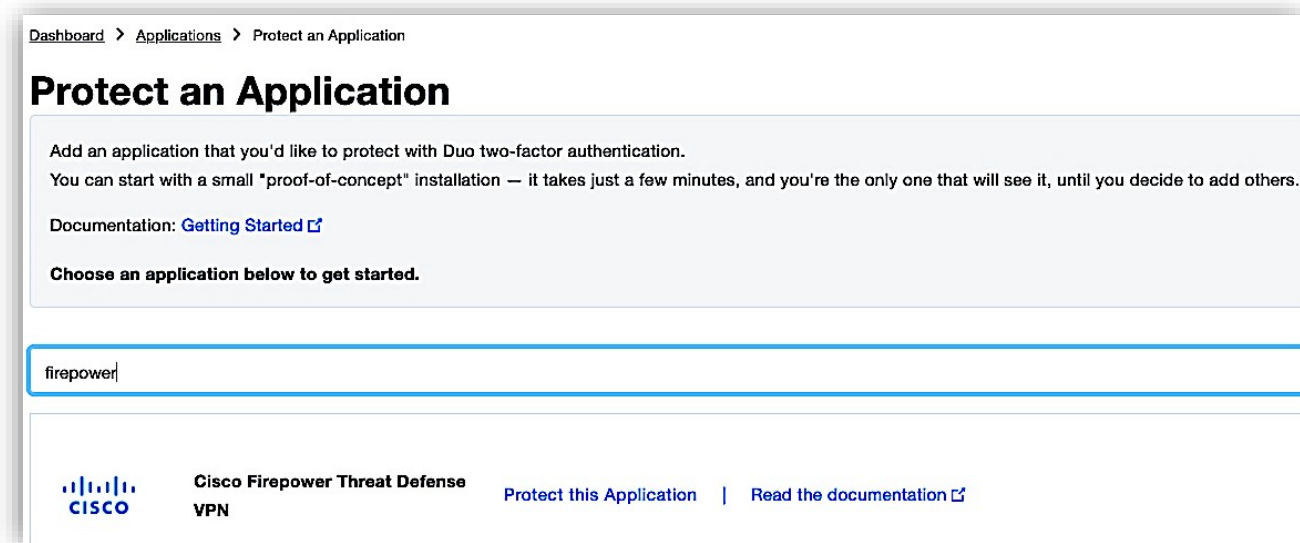
The image shows a web form titled "Get Your Free Duo Account" with the subtitle "Current customers can upgrade now to try more features." The form contains the following elements:

- Two input fields for "First Name" and "Last Name".
- An "Email Address" field and a phone number field with a dropdown for country code (showing "(201) 555-0123").
- A "Company / Account Name" field and a "Select an Option" dropdown menu.
- Two checkboxes: "I'm an MSP, Reseller, or Partner" and "By signing up I agree to the Terms and Services Privacy Notice.".
- A reCAPTCHA widget with the text "I'm not a robot" and a "reCAPTCHA Privacy - Terms" link.
- A large green button at the bottom labeled "Create My Account".

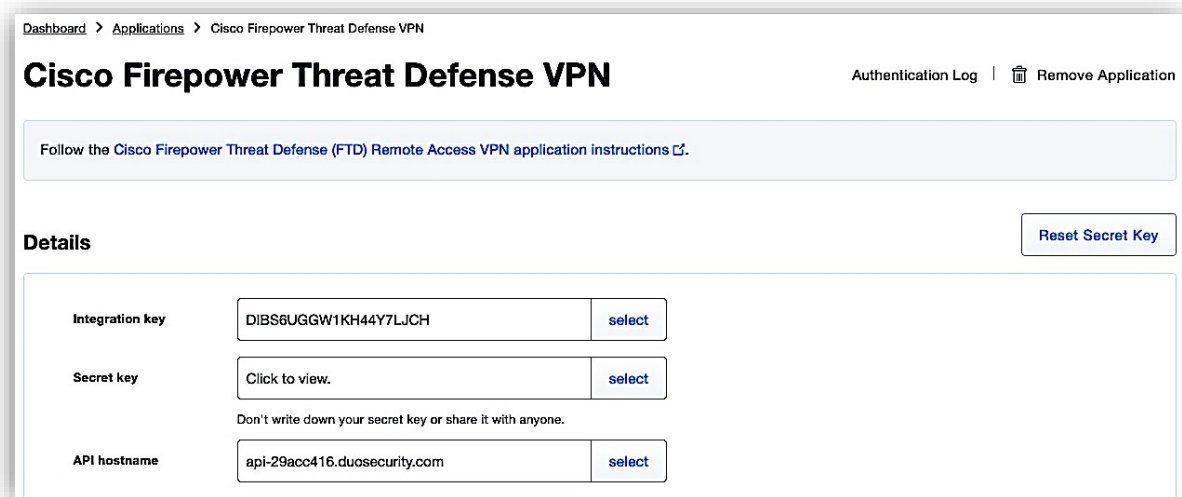
- 完了したら、次のセクションに進んで、テスト VPN ユーザと Firepower アプリケーションを自分のアカウントに追加できます。

Firepower アプリケーションを追加して VPN ユーザを Duo アカウントに登録する

- [Duo Admin Panel](#) にログインし、[Applications] に移動します。
- アプリケーション リストで [Cisco Firepower Threat Defense VPN] を見つけます。



- [Protect this Application] をクリックして、**統合キー**、**秘密キー**、および **API のホスト名** を取得します。



注：秘密キーはパスワードと同じように取り扱う

Duo アプリケーションのセキュリティは、秘密キー (skey) のセキュリティに関連付けられています。機密性の高いクレデンシャルと同じようにそれを保護します。どのような場合にも、それを、許可されていない個人と共有したり、電子メールで他人に送信したりしないでください。

- このアプリケーションに関連付けられた機能は、「ポリシー」など、その他にも多数ありますが、このラボでは取り上げません。
- ここで、テストに使用する VPN ユーザ アカウントを追加してみましょう。[Duo Admin Panel] の [Users] に移動し、[Add User] をクリックします。[Username] フィールドに「vpnuser」と入力し、[Add User] をクリックします。

注：登録用の SMS メッセージを受信できない場合は、手順 6 に従ってください。それ以外の場合は、手順 7 に進みます。

- [vpnuser] ダッシュボードで、登録に使用できる電子メール アドレスを追加します。[Save Changes] をクリックします。ここで、[Send Enrollment Email] リンクをクリックすると、電話番号やその他の 2FA 認証デバイスを追加できるリンクが含まれたメッセージを受信できます。手順 12 に進みます。

- 登録メッセージが送信されるように、[vpnuser] ダッシュボードで電話番号を追加します。新しいユーザの詳細ページを下にスクロールして [Phones] テーブルに移動し、[Add Phone] をクリックします。

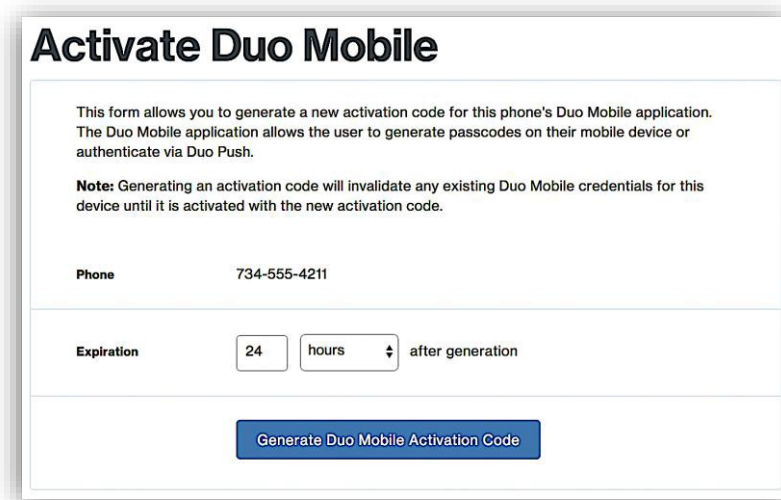
8. [Phone] を選択し、電話番号を入力します（タブレットを追加する場合は、このフィールドは空白のままにします）。[Add Phone] ボタンをクリックします。

The screenshot shows the 'Add Phone' form in the Cisco dCloud interface. The breadcrumb navigation is 'Dashboard > Users > avandalay > Add Phone'. The form title is 'Add Phone'. Under the 'Type' section, the 'Phone' radio button is selected, and the 'Tablet' radio button is unselected. The 'Phone number' field contains '+1 734-555-8008' with a US flag icon and a 'Show extension field' link. At the bottom, there is an 'Add Phone' button.

9. ドロップダウン メニューから適切な電話の [Type] と [Platform] を選択し、[Device name] を入力します（このフィールドは空白のままでも構いません）。デバイスがスマートフォンであることがわかっていて、プラットフォームが不明の場合は、[Generic Smartphone] を選択します。実際のプラットフォームは、ユーザがアクティベーションを完了したときに設定されます。[Save Changes] ボタンをクリックします。

The screenshot shows the 'Settings' form in the Cisco dCloud interface. The breadcrumb navigation is 'Dashboard > Users > avandalay > Settings'. The form title is 'Settings'. Under the 'Number' section, the 'Number' field contains '+1 734-555-8008' with a US flag icon and a 'Show extension settings' link. The 'Device name' field is empty, with a note below it: 'Optional. Examples: "Work phone", "Old iPod touch"'. Under the 'Type' section, the 'Type' dropdown menu is set to 'Mobile'. Under the 'Platform' section, the 'Platform' dropdown menu is set to 'iOS'. At the bottom, there is a 'Save Changes' button.

10. [Device Info] セクションで [Activate Duo Mobile] リンクをクリックします。このリンクは、電話機のタイプを [Mobile] に設定し、プラットフォームに [Unknown] 以外を選択した場合にのみ使用できます。次のページで [Duo Mobile Activation Code] ボタンをクリックします。



The screenshot shows a form titled "Activate Duo Mobile". The form contains the following text and fields:

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone 734-555-4211

Expiration hours after generation

[Generate Duo Mobile Activation Code](#)

11. 次に、送信可能な2つのテキストメッセージが表示されます。最初のメッセージには、ユーザが Duo Mobile をインストールするのに役立つリンクがあります。2番目のメッセージには、アカウントを、自分の Duo Mobile アプリにすぐに追加できるコードがあります。[Send Instructions by SMS] ボタンをクリックして、ユーザの電話機にテキストメッセージを送信します。

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. You now have the option to deliver the installation instructions and/or activation instructions to the user by SMS.

Phone 734-555-4211

Installation instructions Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions Send activation instructions via SMS

To activate the app, tap and open this link with Duo Mobile: <https://m-xxxxxxx.duosecurity.com/activate/LScDPKMB2312Hkt aAKcli>

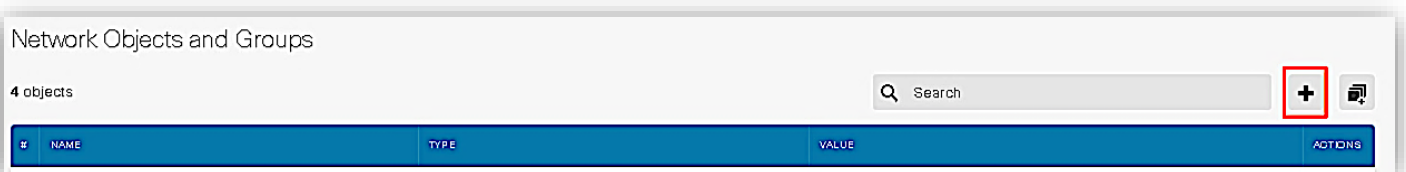
Send Instructions by SMS or skip this step

12. 電子メール メッセージまたは SMS メッセージが届きます。それには、アクティベーション リンクと QR コードのほか、すべてのサポート対象プラットフォームの Duo Mobile アプリにアクセス可能なリンクが記載されています。デバイスでリンクを開くか、Duo Mobile アプリで QR コードをスキャンして、Duo アカウントを追加し、vpuser を有効にする必要があります。完了すると、Duo アカウントが追加され、vpuser が完全に有効になります。

このシナリオに必要なオブジェクトを作成する

注：これらのオブジェクトのほとんどは、RA VPN ウィザードを実行しながら作成できます。RA VPN 設定のコンポーネントに慣れていない管理者には、ウィザードの方が効率的なアプローチかもしれませんが、このシナリオでは独立したタスクでオブジェクトを作成します。オブジェクトを作成しておくことで、RA VPN ウィザードを後で容易に実行できます。

1. Jumpbox で、[Firefox] タブを開き、[NGFW2 (FDM)] をクリックしてこの演習を進めます。クレデンシャルに、**admin** と **C1sco12345** を使用して FDM にログインします。
2. [オブジェクト (Objects)] > [ネットワーク (Network)] に移動します。[+] をクリックします。



3. 次のオブジェクトを作成します。

名前	タイプ	ネットワーク
LAN_Network	ネットワーク	198.19.10.0/24
VPN_Pool	ネットワーク	198.19.10.64/29
ISE_Server	ホスト	198.19.10.130
DNS_Server	ホスト	198.19.10.100
DCloud_LAN1	ネットワーク	10.0.0.0/8
DCloud_LAN2	ネットワーク	198.19.255.0/24
DCloud_Jumpbox	ホスト	198.18.133.50

Network Objects and Groups

11 objects

Search

#	NAME	TYPE	VALUE	ACTIONS
1	DCloud-Jumpbox	HOST	198.18.133.50	
2	DCloud-LAN1	NETWORK	10.0.0.0/8	
3	DCloud-LAN2	NETWORK	198.19.255.0/24	
4	DNS_Server	HOST	198.19.10.100	
5	ISE_Server	HOST	198.19.10.130	
6	LAN_Network	NETWORK	198.19.10.0/24	
7	OutsidelPv4DefaultRoute	NETWORK	0.0.0.0/0	
8	OutsidelPv4Gateway	HOST	198.18.128.1	
9	VPN_Pool	NETWORK	198.19.10.64/29	
10	any-ipv4	NETWORK	0.0.0.0/0	
11	any-ipv6	NETWORK	::/0	

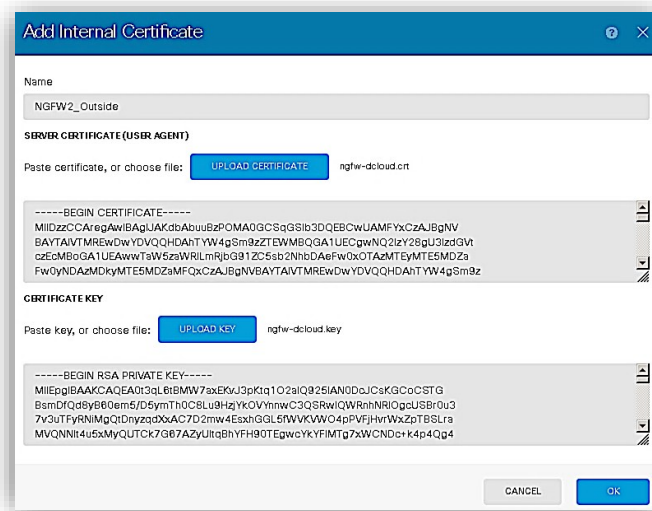
4. [ポート (Ports)]に移動して、[+] をクリックします。

- a. [名前 (Name)]に「DNS_UDP」を設定します。
- b. [プロトコル (Protocol)]に「UDP」を、[ポート (Port)]に「53」を指定します。
- c. [OK] をクリックします。

5. ISE ポスチャのリダイレクト アクセスリストで最終的に使用できるように、上記のポート オブジェクトを追加しました。また、同じ目的で、ポート番号 8443 の TCP ポートが必要です。6.4 では、名前とコンテンツで、オブジェクトとアクセスポリシーを検索できるようになりました。これを使用して、8443 のポート オブジェクトが存在するかどうかを確認します。

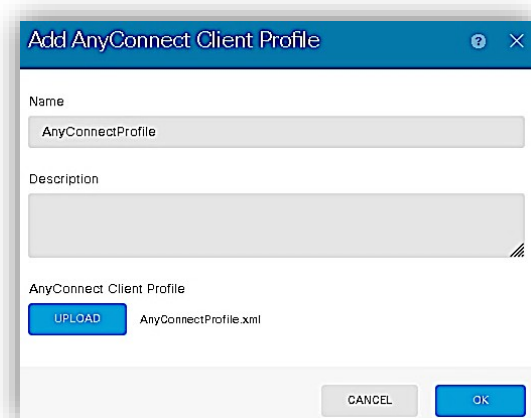
6. [証明書 (Certificates)] に移動します。[+] をクリックして、[信頼できるCA証明書の追加 (Add Trusted CA Certificate)] を選択します。
- [名前 (Name)] に「DCloud_CA」と入力します。
 - [証明書のアップロード (Upload Certificate)] をクリックします。[デスクトップ (Desktop)] > [証明書 (Certificates)] に移動し、[dcloudCA] を選択します。
 - [OK] をクリックします。

7. [+] をクリックして、[内部証明書の追加 (Add Internal Certificate)] を選択します。[証明書とキーのアップロード (Upload Certificate and Key)] をクリックします。
 - a. [名前 (Name)] に「NGFW2_Outside」と入力します。
 - b. [証明書のアップロード (Upload Certificate)] をクリックします。[デスクトップ (Desktop)] > [証明書 (Certificates)] に移動し、[ngfw-dcloud] を選択します。
 - c. [キーのアップロード (Upload Key)] をクリックします。[デスクトップ (Desktop)] > [証明書 (Certificates)] に移動し、[ngfw-dcloud] を選択します。
 - d. [OK] をクリックします。



AnyConnect プロファイルのアップロード

1. FDM で、[オブジェクト (Objects)] > [AnyConnectクライアントプロファイル (AnyConnect Client Profiles)] に移動します。[+] をクリックします。
 - a. [アップロード (Upload)] をクリックします。[デスクトップ (Desktop)] > [RA VPN] に移動し、[AnyConnectProfile] を選択します。
 - b. [OK] をクリックします。



Duo 認証プロキシ サーバの作成と設定

1. 便宜上、すでに、内部の Active Directory サーバで Duo 認証プロキシ アプリケーションを設定しています。このサーバへの RDP セッションを開始して、次の場所にある認証プロキシ設定ファイルを編集できます。C:\Program Files (x86)\Duo Security Authentication Proxy\conf

```

|; Complete documentation about the Duo Auth Proxy can be found
here:
; https://duo.com/docs/authproxy_reference

; MAIN: Include this section to specify global configuration
options.
; Reference: https://duo.com/docs/authproxy_reference#main-
section
; [main]

; CLIENTS: Include one or more of the following configuration
sections.
; To configure more than one client configuration of the same
type, append a
; number to the section name (e.g. [ad_client2])

[duo_only_client]

; SERVERS: Include one or more of the following configuration
sections.
; To configure more than one server configuration of the same
type, append a
; number to the section name (e.g. radius_server_auto1,
radius_server_auto2)

[radius_server_auto]
ikey=DIB86UGGWLKH44Y7LJCH
skey=aHGHby4M4f8cnmwDuXzQSOM0ADtHxgtRJcmzq7l0
api_host=api-29acc416.duosecurity.com
radius_ip_1=198.19.10.1
radius_secret_1=C1sco12345
radius_ip_2=198.19.10.2
radius_secret_2=C1sco12345
radius_ip_3=198.19.10.3
radius_secret_3=C1sco12345
failmode=safe
client=duo_only_client

```

2. **ikey**、**skey**、および **api_host** を、Duo アカウントの値に変更します。完了後、保存してファイルを閉じます。
3. AD サーバで、**Services.msc** を開き、**Duo 認証プロキシ**のサービスを再起動します。これが成功したことを確認します。
4. C:\Program Files (x86)\Duo Security Authentication Proxy\bin に移動して、**authproxy_connectivity_tool** を実行します。
5. 接続テストが成功したかどうかを確認するには、C:\Program Files (x86)\Duo Security Authentication Proxy\log に移動し、**connectivity_tool** ファイルを開きます。ファイルの一番下までスクロールし、次のログが出力されていることを確認します。

```

2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] Testing section 'duo_only_client' with
configuration:
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] {}
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] There are no configuration problems
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] Testing section 'radius_server_auto' with
configuration:
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] {'api_host': 'api-29acc416.duosecurity.com',

```

```

'client': 'duo_only_client',
'failmode': 'safe',
'apikey': 'DIBS6UGGW1KH44Y7LJCH',
'port': '1812',
'radius_ip_1': '198.19.10.1',
'radius_ip_2': '198.19.10.2',
'radius_ip_3': '198.19.10.3',
'radius_secret_1': '*****',
'radius_secret_2': '*****',
'radius_secret_3': '*****',
'skey': '*****[40]}'
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] There are no configuration problems
2019-03-17T23:38:08+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] Testing section 'duo_only_client' with
configuration:
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] {}
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] No testing to be done for section.
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] Testing section 'radius_server_auto' with
configuration:
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] {'api_host': 'api-29acc416.duosecurity.com',
'client': 'duo_only_client',
'failmode': 'safe',
'apikey': 'DIBS6UGGW1KH44Y7LJCH',
'port': '1812',
'radius_ip_1': '198.19.10.1',
'radius_ip_2': '198.19.10.2',
'radius_ip_3': '198.19.10.3',
'radius_secret_1': '*****',
'radius_secret_2': '*****',
'radius_secret_3': '*****',
'skey': '*****[40]}'
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] The RADIUS Server has no connectivity problems.
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] -----
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] SUMMARY
2019-03-17T23:38:13+0000 [duoauthproxy.lib.log#info] No issues detected

```

6. [オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] に移動します。[+] をクリックし、[RADIUSサーバ (RADIUS Server)] を選択します。
 - a. [名前 (Name)] に「**Duo_Server**」と入力します。
 - b. [IPアドレス (IP Address)] に「**198.19.10.100**」と入力します。
 - c. [サーバ秘密キー (Server Secret Key)] に「**C1sco12345**」と入力します。
 - d. [RA VPNのみ (RA VPN Only)] セクションを展開します。[RADIUSサーバに接続するために使用されるインターフェイス (Interface used to connect to RADIUS server)] を [インターフェイスを手動で選択する (Manually choose interface)] に設定して、ドロップダウンから [inside] を選択します。
 - e. [OK] をクリックします。

Add RADIUS Server

Name
Duo_Server

Server Name or IP Address: 198.19.10.100 Authentication Port: 1812

Timeout ⓘ
10 seconds
7-300

Server Secret Key
●●●●●●●●

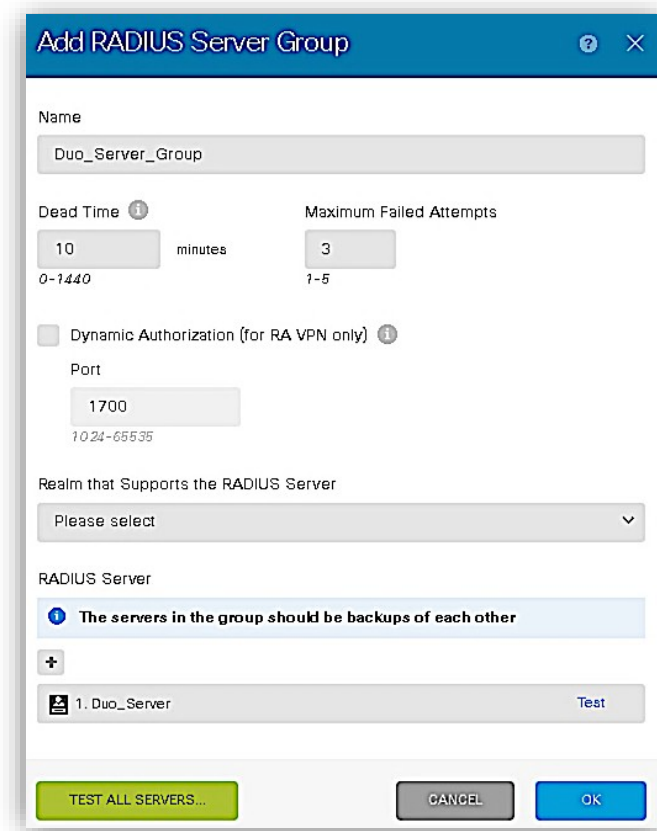
RA VPN Only (if this object is used in RA VPN Configuration)

Redirect ACL
Please select

Interface used to connect to Radius server ⓘ
 Resolve via route lookup
 Manually choose interface
inside

CANCEL OK

7. [+] をクリックし、[RADIUSサーバグループ (RADIUS Server Group)] を選択します。
 - a. [名前 (Name)] を「**Duo_Server_Group**」に設定します。
 - b. [RADIUSサーバ (RADIUS Server)] で [+] をクリックし、先ほど作成した Duo_Server オブジェクトを選択します。
 - c. [OK] をクリックします



注：管理インターフェイスを使用しているため、テストは失敗します。

ポスチャ評価を行う ISE サーバの作成と設定

1. [デバイス (Device)] > [詳細設定 (Advanced Configuration)] > [設定の表示 (View Configuration)] > [スマートCLIオブジェクトの作成 (Create Smart CLI object)] に移動します。
2. ISE ポスチャ評価に必要なリダイレクト アクセスリストを作成します。[+] をクリックします。
 - a. [名前 (Name)] を「**redirect**」に設定します。
 - b. [CLIテンプレート (CLI Template)] ドロップダウンから [拡張アクセスリスト (Extended Access List)] を選択します。
 - c. テンプレートで、次の設定を入力します。
 - i. 2 行目で、**action** を **deny** に変更します。3 ~ 5 行目が表示されます。
 - ii. 3 行目で、**source-network** を **any-ipv4** に、**destination-network** を **ISE_Server** に変更します。
 - iii. 4 行目で、オプションを **any-source** に変更します。5 行目が表示されます。
 - iv. 5 行目で、**destination-port** を **HTTP_PORTS-8443** に変更します。

- v. 6 行目で **log-state** を **default** に変更します。7 行目が表示されます。
 - vi. 2 行目に戻り、**configure access-list-entry** コマンドの横にある ... 記号をクリックして、[Duplicate] をクリックします。
 - vii. 8 行目で、**action** を **deny** に変更します。9 ~ 11 行が表示されます。
 - viii. 9 行目で、**source-network** を **any-ipv4** に、**destination-network** を **DNS_Server** に変更します。
 - ix. 10 行目で、オプションを **any-source** に変更します。11 行目が表示されます。
 - x. 11 行目で、**destination-port** を **DNS_UDP** に変更します。
 - xi. 12 行目で **log-state** を **default** に変更します。13 行目が表示されます。
 - xii. 8 行目に戻り、**configure access-list-entry** コマンドの横にある ... 記号をクリックして、[Duplicate] をクリックします。
 - xiii. 14 行目で、**action** を **permit** に変更します。15 ~ 17 行が表示されます。
 - xiv. 15 行目で、**source-network** を **any-ipv4** に、**destination-network** を **any-ipv4** に変更します。
 - xv. 16 行目で、オプションを **any** に変更します。17 行目が表示されます。
 - xvi. 18 行目で、**log-state** を **default** に変更します。19 行目が表示されます。
- d. [OK] をクリックします。

Add Smart CLI Object ? X

Name

Description

CLI Template

Extended Access List v

Template

Access List Name
Show disabled | Reset

```

1 access-list redirect extended
2 configure access-list-entry deny v
3 deny network source [ any-ipv4 x v ] destination [ ISE_Server x v ]
4 configure deny port any-source v
5 deny port source ANY destination [ HTTP_PORTS-8443 x v ]
6 configure logging default v
7 default log set log-level INFORMATIONAL log-interval 300
8 configure access-list-entry deny v
9 deny network source [ any-ipv4 x v ] destination [ DNS_Server x v ]
10 configure deny port any-source v
11 deny port source ANY destination [ DNS_UDP x v ]
12 configure logging default v
13 default log set log-level INFORMATIONAL log-interval 300
14 configure access-list-entry permit v
15 permit network source [ any-ipv4 x v ] destination [ any-ipv4 x v ]
16 configure permit port any v
17 permit port source ANY destination ANY
18 configure logging default v
19 default log set log-level INFORMATIONAL log-interval 300

```

3. [オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] に移動します。[+] をクリックし、[RADIUSサーバ (RADIUS Server)] を選択します。
 - a. [名前 (Name)] に「ISE_Server」と入力します。
 - b. [IPアドレス (IP Address)] に「198.19.10.130」と入力します。
 - c. [サーバ秘密キー (Server Secret Key)] に「C1sco12345」と入力します。
 - d. [RA VPNのみ (RA VPN Only)] セクションを展開します。[リダイレクトACL (Redirect ACL)] ドロップダウンから [redirect] を選択します。
 - e. [RADIUSサーバに接続するために使用されるインターフェイス (Interface used to connect to RADIUS server)] を [インターフェイスを手動で選択する (Manually choose interface)] に設定して、ドロップダウンから [inside] を選択します。
 - f. [OK] をクリックします。

Capabilities of RADIUS Server ⓘ

Authentication Authorization

Name

ISE_Server

Server Name or IP Address Authentication Port

198.19.10.130 1812

Timeout ⓘ

10 seconds

1-300

Server Secret Key

••••••••

RA VPN Only (if this object is used in RA VPN Configuration)

Redirect ACL

redirect

Interface used to connect to Radius server ⓘ

Resolve via route lookup

Manually choose interface

inside

TEST CANCEL OK

4. [+] をクリックし、[RADIUSサーバグループ (RADIUS Server Group)] を選択します。
 - a. [名前 (Name)] を「ISE_Server_Group」に設定します。
 - b. [ダイナミック認証 (Dynamic Authorization)] をオンにします。
 - c. [RADIUSサーバ (RADIUS Server)] で [+] をクリックし、先ほど作成した ISE_Server オブジェクトを選択します。
 - d. [OK] をクリックします。

注 : VPN の RADIUS サーバ接続をテストします。

- 1) RADIUS サーバを RA VPN プロファイルに割り当てて、設定を導入します。
- 2) NGFW2 CLI にログインし、**system support diagnostic-cli** を入力することで Lina モードに入ります。
- 3) ここでは、**test aaa-server <RADIUS-Server-Group> host <RADIUS サーバの IP> username vpnuser password C1sco12345** を実行できます。

リモート アクセス VPN のセットアップ

1. [デバイス (Devices)] > [リモートアクセスVPN (Remote Access VPN)] > [設定の表示 (View Configuration)] に移動します。ここで、複数の接続プロファイルとグループ ポリシーを作成できます。
2. 左側のパネルで [グループポリシー (Group Policies)] に移動します。[DfltGroupPolicy] が表示されます。次に、それを編集します。
 - a. [全般 (General)] タブで、[DNSサーバ (DNS Server)] の [CustomDNSServerGroup] を選択します。[AnyConnect クライアントプロファイル (AnyConnect Client Profiles)] で [+] をクリックして、[AnyConnectプロファイル (AnyConnect Profile)] を選択します。

Edit Group Policy

Search for attribute

Basic

- General
- Session Settings

Advanced

- Address Assignment
- Split Tunneling
- AnyConnect
- Traffic Filters
- Windows Browser Proxy

Description

DNS Server

CustomDNSServerGroup

Banner Text for Authenticated Clients

This message will be shown to successfully authenticated endpoints in the beginning of their VPN session

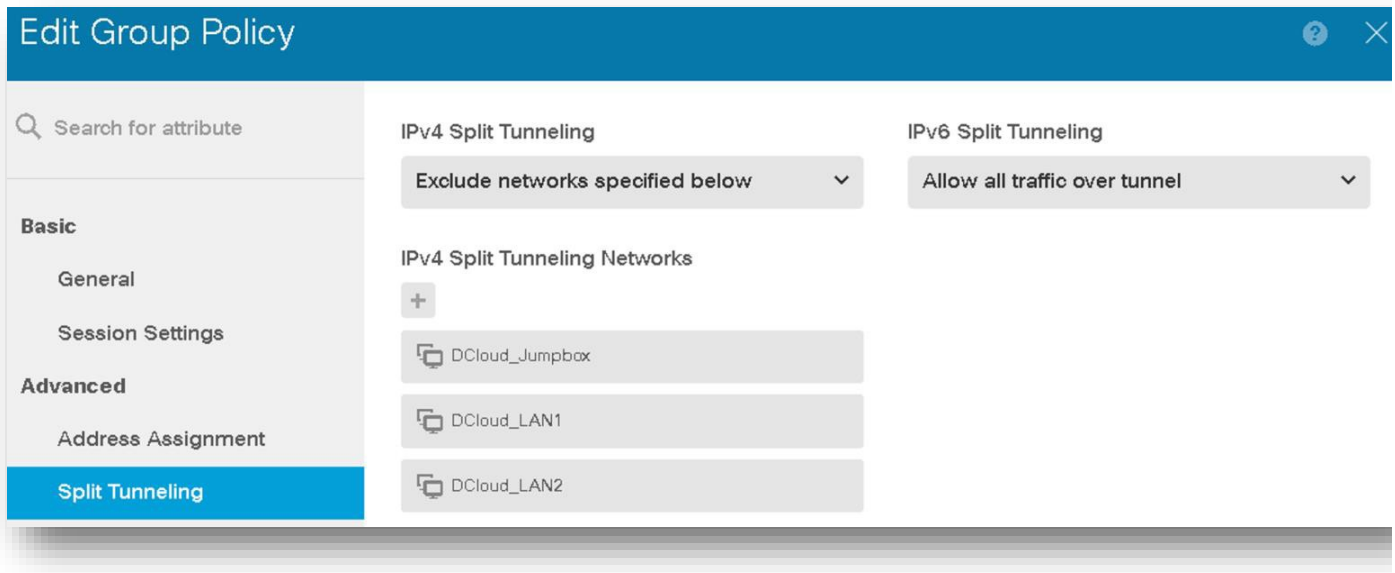
Default domain

AnyConnect client profiles

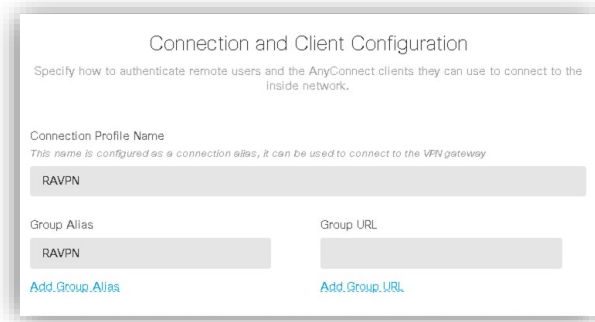
+ AnyConnectProfile

CANCEL OK

- b. [スプリットトンネリング (Split Tunneling)] タブの [IPv4スプリットトンネリング (IPv4 Split Tunneling)] で、[以下に指定したネットワークを除外する (Exclude networks specified below)] を選択します。[IPv4スプリットトンネリングネットワーク (IPv4 Split Tunneling Networks)] の [+] をクリックして、[DCloud-LAN1]、[DCloud-LAN2]、[DCloud-Jumpbox] を選択します。



- c. [OK] をクリックします。
3. 左側のパネルで [接続プロファイル (Connection Profiles)] に移動します。[接続プロファイルの作成 (CREATE CONNECTION PROFILE)] をクリックします。
 - a. [接続プロファイル名 (Connection Profile Name)] を「**RAVPN**」に設定します。[グループエイリアス (Group Alias)] が自動的に更新されます。



- b. [プライマリアイデンティティソース (Primary Identity Source)] で、[認証タイプ (Authentication Type)] に [AAA] と [クライアント証明書 (Client Certificate)] を選択します。
 - i. [ユーザ認証のプライマリアイデンティティソース (Primary Identity Source for User Authentication)] に [ISE_Server_Group] を選択します。
 - ii. ユーザ名は、証明書の CN から事前入力するため、[証明書のユーザ名 (Username from Certificate)] フィールドのユーザ名はそのままにしておきます。
 - iii. [詳細設定 (Advanced)] を展開して、[ユーザログインウィンドウの証明書からユーザ名を事前入力 (Prefill username from certificate on user login window)] を選択します。

Primary Identity Source

Authentication Type

AAA Only Client Certificate Only **AAA and Client Certificate**

Primary Identity Source for User Authentication: ISE_Server_Group

Fallback Local Identity Source ⚠: Please Select Local Identity Source

Strip Identity Source server from username

Strip Group from Username

Username from Certificate

Map Specific Field

Primary Field: CN (Common Name) Secondary Field: OU (Organisational Unit)

Use entire DN (distinguished name) as username

Advanced

Prefill username from certificate on user login window

Hide username in login window

- c. [セカンダリアイデンティティソース (Secondary Identity Source)] に [Duo_Server_Group] を選択します。[詳細設定 (Advanced)] を展開します。
- i. ユーザ名は、証明書の CN から事前入力するため、[証明書のユーザ名 (Username from Certificate)] フィールドのユーザ名はそのままにしておきます。
 - i. [ユーザログインウィンドウの証明書からユーザ名を事前入力 (Prefill username from certificate on user login window)] を選択します。[ログインウィンドウのユーザ名を非表示 (Hide username in login window)] を選択します。

Secondary Identity Source

Secondary Identity Source for User Authentication: Duo_Server_Group

Advanced

Fallback Local Identity Source for Secondary: Please Select Local Identity Source

Use Primary username for Secondary login

Username from Certificate

Map Specific Field

Primary Field: CN (Common Name) Secondary Field: OU (Organisational Unit)

Use entire DN (distinguished name) as username

Prefill username from certificate on user login window

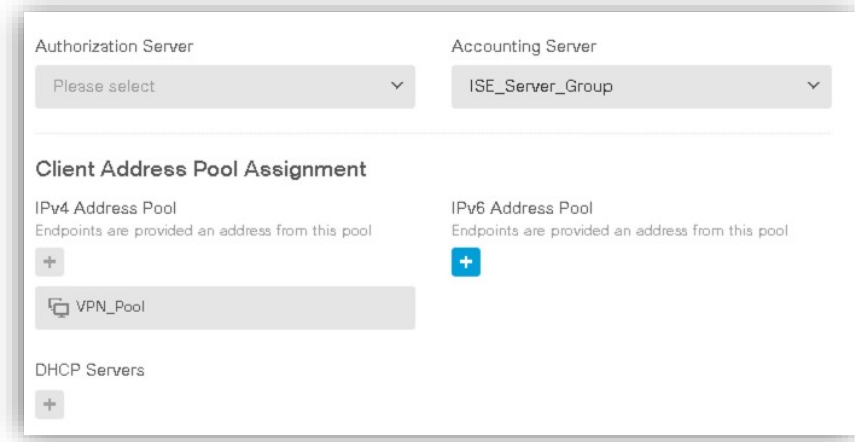
Hide username in login window

Username for session server

Primary Secondary

Password Type: Prompt

- d. [アカウンティングサーバ (Accounting Server)] を [ISE_Server_Group] に設定します。
- e. [IPv4アドレスプール (IPv4 Address Pool)] の [+] をクリックして、[VPN_Pool] を選択します。
- f. [次へ (Next)] をクリックします。



4. 次の手順では、グループポリシーを設定しますが、それはすでに完了しているため、[次へ (Next)] をクリックします。
5. [グローバル設定 (Global Settings)] で以下を行います。
 - a. [デバイスアイデンティティの証明書 (Certificate of Device Identity)] を [NGFW2_Outside] に設定します。
 - b. [外部インターフェイス (Outside Interface)] を [outside] に設定します。
 - c. [外部インターフェイスの完全修飾ドメイン名 (Fully-qualified Domain Name for the Outside Interface)] に「**ngfw2-outside.dcloud.local**」と入力します。
 - d. [NAT適用除外 (NAT Exempt)] の [内部インターフェイス (Inside Interface)] にある [+] をクリックして、[inside] を選択します。
 - e. [NAT適用除外 (NAT Exempt)] の [内部ネットワーク (Inside Networks)] にある [+] をクリックして、[LAN_Network] を選択します。
 - f. [AnyConnectパッケージ (AnyConnect Package)] で、[パッケージのアップロード (Upload Package)] をクリックします。[Windows] を選択します。[デスクトップ (Desktop)] > [RA VPN] に移動して、[anyconnect-win-4.7.01076-webdeploy-k9.pkg] を選択します。[開く (Open)] をクリックします。
 - g. AnyConnect パッケージをアップロードしたら、[次へ (Next)] をクリックします。

Certificate of Device Identity: NGFW2_Outside

Outside Interface: outside

Fully-qualified Domain Name for the Outside Interface: ngfw2-outside.dcloud.local

Access Control for VPN Traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt

Inside Interfaces: inside

Inside Networks: LAN_Network

AnyConnect Package

Packages: Windows: anyconnect-win-4.7.01076-webdeploy-k9.pkg

BACK NEXT

6. 設定の概要を確認して、[完了 (Finish)] をクリックします。

NAT とアクセス ポリシーの設定を編集する

1. アクセス ポリシーを変更する前に、ライセンスを確認します。[デバイス (Devices)] > [スマートライセンス (Smart License)] > [設定の表示 (View Configuration)] に移動します。
2. すでに有効になっているすべてのライセンスが表示されます。実際の導入では、スマート ライセンス サーバに登録して、輸出管理ライセンスを有効にする必要があります。

注: FDM は、CLI 経由でのみ表示される VPN トラフィックに NAT 適用除外のステートメントを追加します。

3. [ポリシー (Policies)] > [NAT] に移動します。ポスタチャ評価をトリガーするために、デフォルトの [InsideOutsideNatRule] を変更して VPN トラフィックも許可します。

4. [InsideOutsideNatRule] を編集します。[送信元インターフェイス (Source Interface)] を [Inside] から [Any] に変更します。[OK] をクリックします。

5. [アクセス制御 (Access Control)] に移動して [+] をクリックします。
- a. 新しいルールの [順序 (Order)] を [1] に設定します。
 - b. [名前 (Name)] に [RAVPN_Access] を、[アクション (Action)] に [許可 (Allow)] を、それぞれ設定します。
 - c. [送信元 (Source)] で、[ゾーン (Zones)] を [outside_zone] に、[ネットワーク (Networks)] を [VPN_Pool] にそれぞれ設定します。

Add Access Rule

Order	Title	Action
1	RAVPN_Access	Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	VPN_Pool	ANY	ANY	ANY	ANY

- d. [侵入ポリシー (Intrusion Policy)] に移動します。[侵入ポリシー (Intrusion policy)] を有効にして、[レベル (Level)] を [バランスのとれたセキュリティと接続 (Balanced Security and Connectivity)] に設定します。

Add Access Rule

Order	Title	Action
1	RAVPN_Access	Allow

Source/Destination | Applications | URLs | Users | **Intrusion Policy** | File policy | Logging

INTRUSION POLICY

Level of Intrusion Policy

Balanced Security and Connectivity

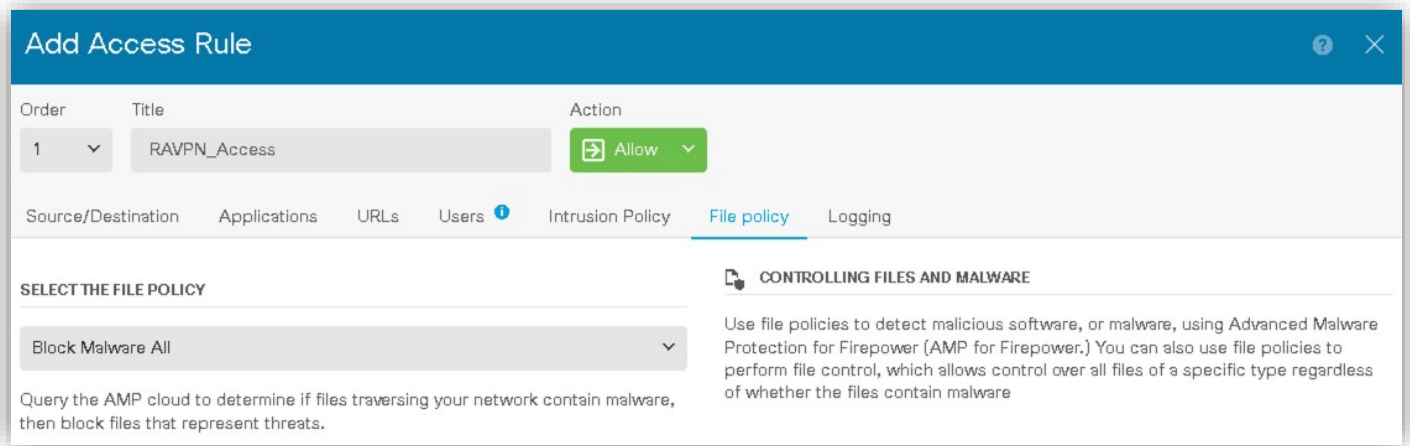
Balanced Security and Connectivity

This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.

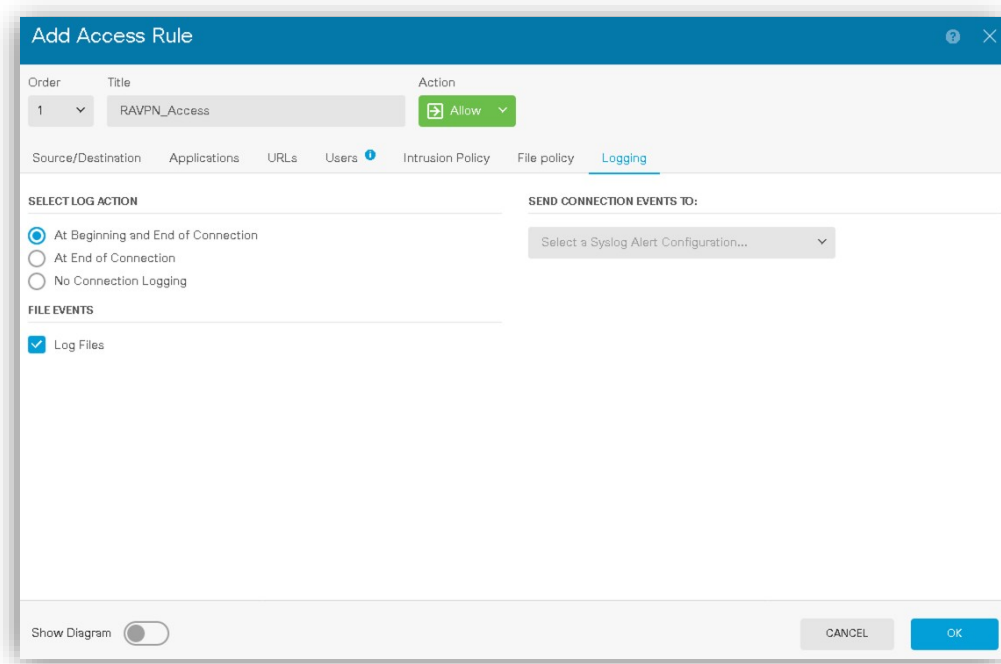
PREVENTING INTRUSIONS

Use intrusion policies as a last line of defense against unwanted traffic that you are otherwise allowing. An intrusion policy examines decoded packets for intrusions, exploits, and other attacks based on patterns, and can block or alter malicious traffic. Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings.

- e. [ファイルポリシー (File Policy)] に移動します。[マルウェアをすべてブロックする (Block Malware All)] を選択します。



- f. [ロギング (Logging)] に移動します。[ログアクションの選択 (Select Log Action)] で [接続の開始時と終了時 (At Beginning and End of Connection)] を選択します。[OK] をクリックします。



設定を導入しテストする

注：このシナリオでは、コンプライアンス対応システムの定義は、デスクトップに compliant.txt というファイルを持つシステムです。前のシナリオを完了している場合は準拠していると見なされるため、そのようなユーザは手順 6 ~ 9 を省略できます。これが最初の RA VPN シナリオの場合、Wkst2 を非準拠と見なして手順を開始します。また、Wkst2 には、ポスチャ モジュールがインストールされています。

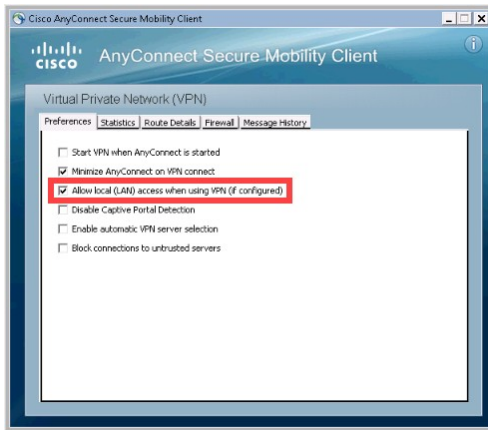
1. 設定を導入し、導入が完了するまで待ちます。

2. **Wkst2** に接続します。管理者として自動的にログインされます。2つの方法のいずれかを使用して接続できます。

- 以下に示すトポロジ マップから接続します。これは推奨される方法です。

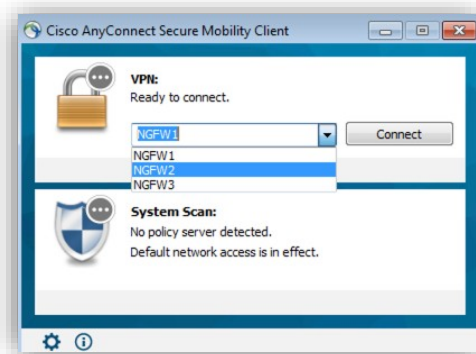


- Jumpbox デスクトップの **Remote Desktops** フォルダの **Wkst2 (Outside PC)** ショートカットをクリックします。ただし、これを行う場合は、AnyConnect クライアントでローカル LAN アクセスを許可する必要があります。

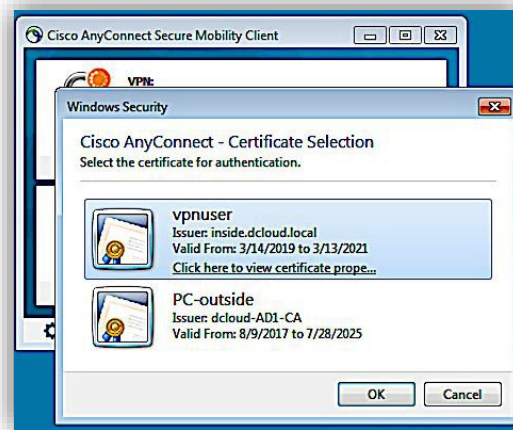


- VPN 経由でポッドに接続している場合は、ラップトップ上の RDP クライアントを使用して **198.18.133.23** に接続します。**Administrator** としてログインします。パスワードは **C1sco12345** を使用します。

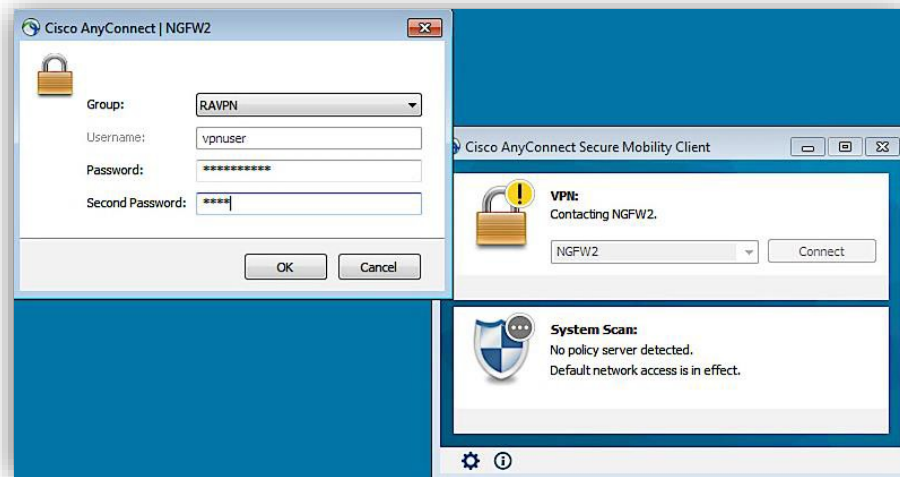
3. [スタート] メニューから **AnyConnect** を開きます。[接続先 (Connect To)] フィールドに [NGFW2 FQDN] が自動的に入力されます。[接続 (Connect)] をクリックします。



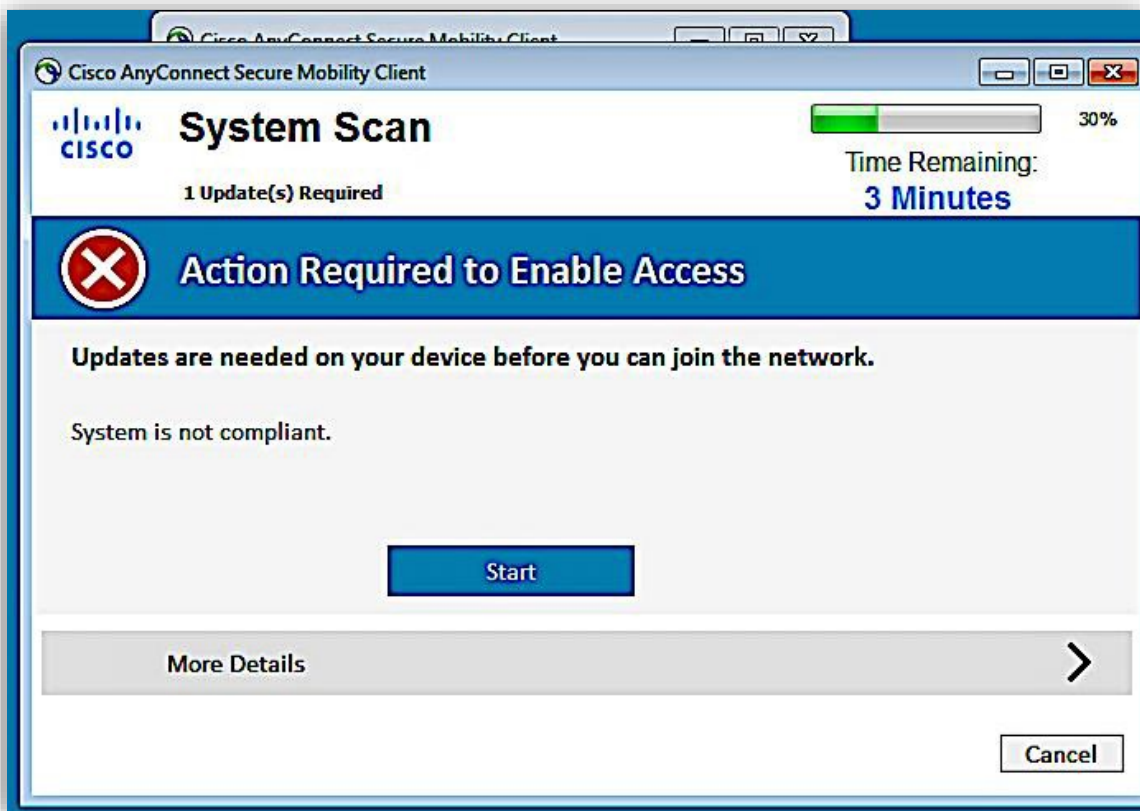
4. テストでは、**vpnuser** と同じ名前のクライアント証明書を使用します。[vpnuser] 証明書を選択します。



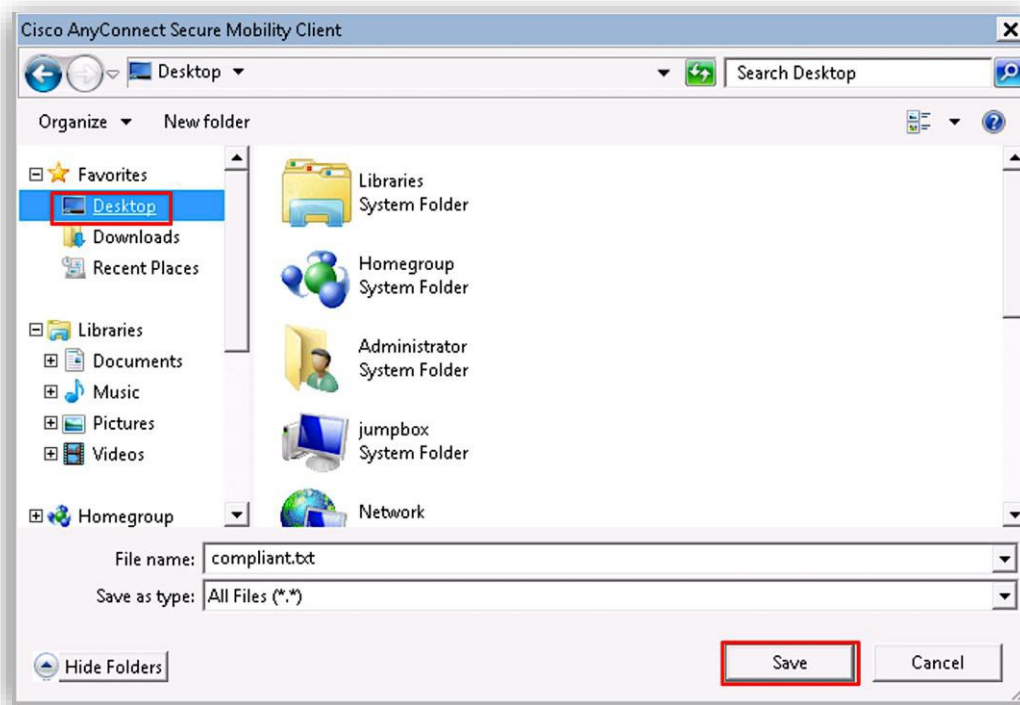
5. [パスワード (Password)]に「**C1sco12345**」を、[2番目のパスワード (Second Password)]に「**push**」を入力します。[OK] をクリックします。Duo 認証で Push 方式を使用するため、ここでは「push」を指定しましたが、必要に応じて電話または SMS を設定できます。モバイル デバイスでプッシュ通知を受け取って承認する必要があります。その際に、VPN トンネルが確立されることがわかります。



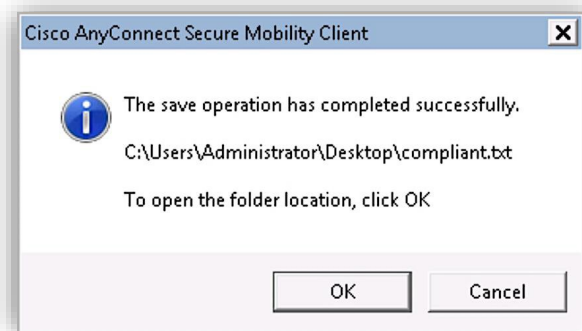
6. 最初の接続で、AnyConnect コンプライアンス モジュールがダウンロードされていることを確認できます。
7. 最初の接続ではシステムが基準を満たしていないため、準拠の対応を求めるプロンプトが表示されます。[開始 (Start)] をクリックします。



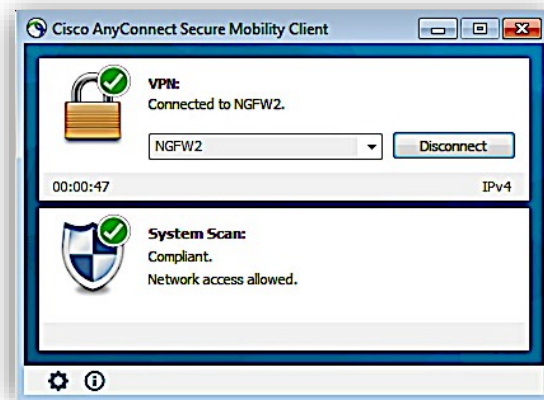
8. **compliant.txt** ファイルの保存を促すプロンプトが表示されます。宛先フォルダを **Desktop** に変更します。



9. 「The save operation has completed successfully」というメッセージが表示されたダイアログボックスでは、[キャンセル (Cancel)] をクリックできます。フォルダを開く必要はありません。



10. ファイルのインストール後、クライアントによってシステムがコンプライアンス対応であることが宣言されます。



11. Wkst2 上の Firefox ブラウザのブックマークを使用して、ブックマークが作成されている 3 つの内部 Web サイト ([内部 (Inside)]、[代替内部 (Alt Inside)]、[内部ハニーポット (Inside Honeypot)]) にアクセスできることを確認します。
12. これらの内部サーバのいずれかで、[ファイル (Files)] リンクをクリックし、[Zombies.pdf] をクリックします。これはマルウェアと見なされるファイルです。ファイルがブロックされることを確認します。ProjectX.pdf のような無害のファイルがブロックされていないことを確認します。

シナリオ 6： 証明書ベースの認証を使用して、FMC と FDM の管理対象デバイスでサイト間 VPN 接続を行う

6.4 では、いくつかのサイト間 (S2S) VPN 拡張機能を利用できます。このシナリオでは、NGFW2 (FDM) と NGFW ブランチ 1 (FMC) の間の S2S トンネルで使用する、証明書ベースの認証を設定します。トンネルの設定時には、それ以外の拡張機能にも注目してください。この機能では、FMC と FDM の両方で、ダイナミック ピアリングを明示的に設定できます。これにより、ブランチ管理に応じて、Firepower の S2S VPN 機能を拡張可能です。

このシナリオの目的：

- NGFW2 と NGFW ブランチ 1 での S2S VPN の設定に必要なオブジェクトを作成する。
- NGFW2 と NGFW ブランチ 1 で S2S VPN セットアップ ウィザードを実行する。
- 確立された S2S トンネルのトラフィックをテストする。

NGFW ブランチ 1 を管理する FMC で S2S VPN を設定する

1. **Jumpbox** で、[Firefox] を開き、ブックマーク リストの [FMC] をクリックします。**FMC** にログインします。
2. [オブジェクト (Objects)] > [ネットワーク (Network)] に移動します。[オブジェクトの追加 (Add Object)] をクリックします。
 - a. 名前に「**NGFWBr1_LAN**」を入力します。
 - b. [ネットワーク (Network)] を [ネットワーク (Network)] に設定し、「**198.19.11.0/24**」を入力します。
 - c. [保存 (Save)] をクリックします。

3. [オブジェクトの追加 (Add Object)] をクリックします。
 - a. 名前に「**NGFW2_LAN**」を入力します。
 - b. [ネットワーク (Network)] を [ネットワーク (Network)] に設定し、「**198.19.10.0/24**」を入力します。
 - c. [保存 (Save)] をクリックします。

New Network Object

Name: NGFW2_LAN

Description:

Network: Host Range Network FQDN

198.19.10.0/24

Allow Overrides:

Save Cancel

4. [オブジェクト (Objects)] > [PKI] > [証明書登録 (Cert Enrollment)] に移動します。[証明書の登録の追加 (Add Cert Enrollment)] をクリックします。
 - a. [名前 (Name)] に「NGFWBr1_Outside」と入力します。
 - b. [登録タイプ (Enrollment Type)] に「**PKCS 12 File**」を設定します。
 - c. [PKCS12ファイルの参照 (Browse PKCS12 File)] をクリックして、[デスクトップ (Desktop)] > [証明書 (Certificates)] に移動します。[ngfwbr1-outside.pfx] を選択します。
 - d. [パスワード (Passphrase)] に「**C1sco12345**」と入力します。
 - e. [保存 (Save)] をクリックします。

Add Cert Enrollment

Name*: NGFWBr1_Outside

Description:

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: ngfwbr1-outside.pfx Browse PKCS12 File

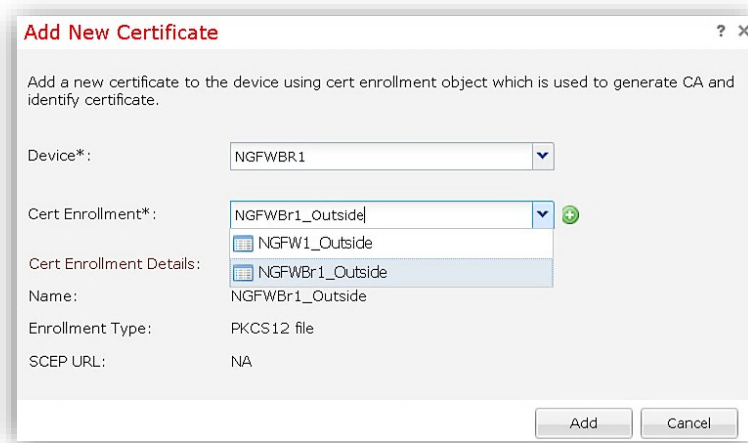
Passphrase:

Allow Overrides:

Save Cancel

5. アップロードした証明書を使用して NGFW ブランチ 1 を登録するには、[デバイス (Devices)] > [証明書 (Certificates)] に移動します。[追加 (Add)] をクリックします。

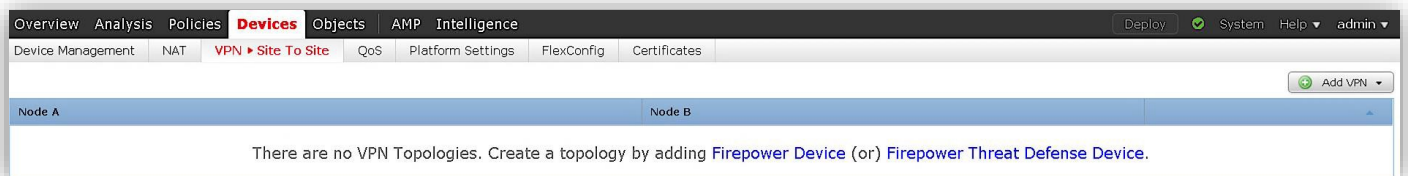
- a. [デバイス (Device)] に [NGFWBR1] を選択します。
- b. [証明書登録 (Cert Enrollment)] に [NGFWBr1_Outside] を選択します。
- c. [追加 (Add)] をクリックします。



- d. 証明書がすぐにデバイスに登録されます。登録は正常に終了します。



6. [デバイス (Devices)] > [VPN] > [サイト間 (Site to Site)] に移動します。[Firepower Threat Defenseデバイス (Firepower Threat Defense Device)] をクリックします。



- a. [トポロジ名 (Topology Name)] に「S2SVPN」と入力します。
- b. [IKEバージョン (IKE Version)] を [IKEv1] のみに設定します。
- c. [エンドポイント (Endpoints)] で、[Node A] の [+] をクリックします。
 - i. [デバイス (Device)] に [エクストラネット (Extranet)] を選択します。
 - ii. [デバイス名 (Device Name)] に「NGFW2」を入力します。
 - iii. [IPアドレス (IP Address)] で [静的 (Static)] を指定し、「198.18.133.82」と入力します。
 - iv. [保護されたネットワーク (Protected Networks)] で、「NGFW2_LAN」オブジェクトを追加します。

- v. [OK] をクリックします。

Add Endpoint ? X

Device:* Extranet ▼

Device Name:* NGFW2

IP Address:* Static Dynamic
198.18.133.82

Certificate Map: ▼ +

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended) +

NGFW2_LAN

OK Cancel

- d. [エンドポイント (Endpoints)] で、[Node B] の [+] をクリックします。
- i. [デバイス (Device)] に [NGFWBR1] を選択します。
 - ii. [インターフェイス (Interface)] に [outside] を設定します。
 - iii. [IPアドレス (IP Address)] に 「198.18.128.81」 を設定します。
 - iv. [保護されたネットワーク (Protected Networks)] で 「NGFWBr1_LAN」 オブジェクトを追加します。
 - v. [OK] をクリックします。

Add Endpoint

Device:* NGFWBR1

Interface:* outside

IP Address:* 198.18.128.81

This IP is Private

Connection Type: Bidirectional

Certificate Map:

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)

NGFWBr1_LAN

OK Cancel

Create New VPN Topology

Topology Name:* S2SVPN

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints

Node A:		
Device Name	VPN Interface	Protected Networks
NGFW2	198.18.133.82	NGFW2_LAN
Node B:		
Device Name	VPN Interface	Protected Networks
NGFWBR1	outside/198.18.128.81	NGFWBr1_LAN

e. [IKE] に移動します。

- i. [IKEv1ポリシー (IKEv1 Policy)] を [certificate_sha_aes256_dh5_1] に変更します。
- i. [証明書 (Certificate)] に [NGFWBr1_Outside] を選択します。

f. [IPSec] に移動します。

i. [リバースルートインジェクションを有効にする (Enable Reverse Route Injection)] をオフにします。

g. [保存 (Save)] をクリックします。

7. [デバイス (Devices)] > [NAT] に移動して、[Branch_NAT_Policy] を編集します。

NAT Policy	Device Type	Status
Branch NAT Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices
Default NAT Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

8. [ルールの追加 (Add Rule)] をクリックします。

a. [送信元インターフェイスオブジェクト (Source Interface Objects)] に [InZone] を選択し、[宛先インターフェイスオブジェクト (Destination Interface Objects)] に [OutZone] を選択します。

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- branch1_InZone
- branch1_Outzone
- InZone
- OutZone

Source Interface Objects (1)
InZone

Destination Interface Objects (1)
OutZone

- b. [変換 (Translation)]タブで、[元の送信元 (Original Source)]および [変換済み送信元 (Translated Source)]に [NGFWBr1_LAN] を選択します。 [元の宛先 (Original Destination)]および [変換済み宛先 (Translated Destination)]に [NGFW2_LAN] を選択します。

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source: *

Original Destination:

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source:

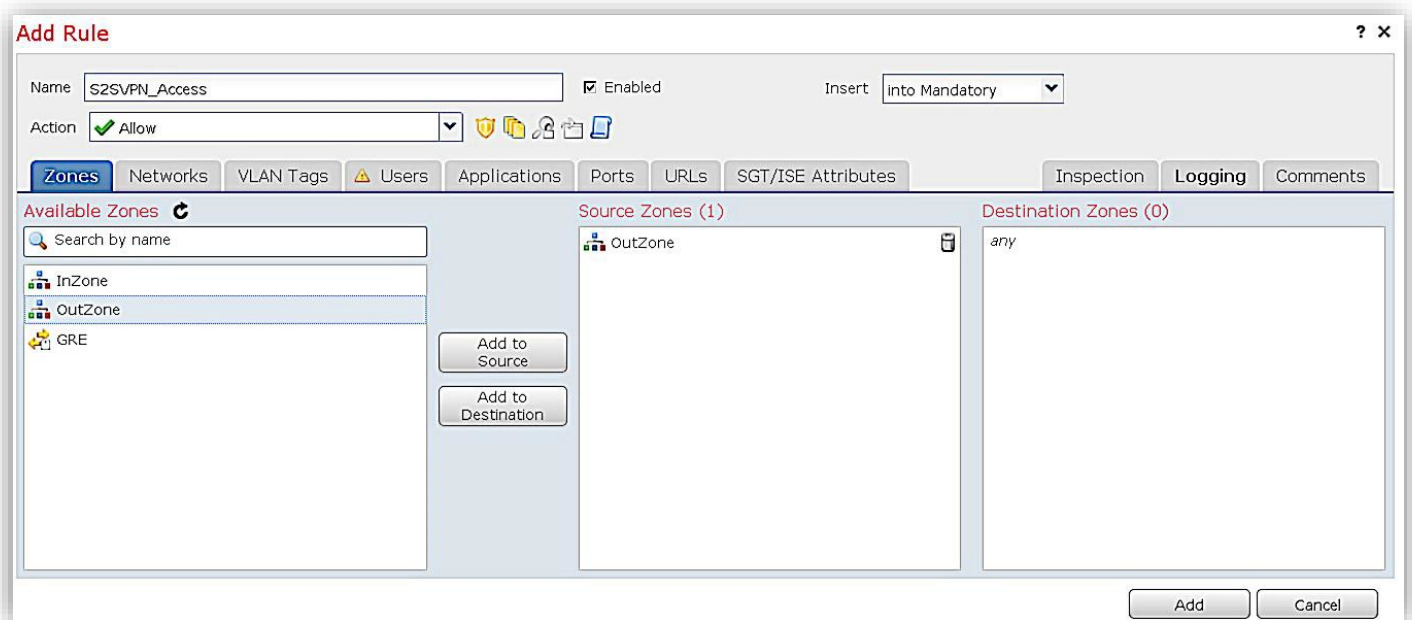
Translated Destination:

Translated Source Port:

Translated Destination Port:

- c. [OK] をクリックして NAT ルールを保存します。 [保存 (Save)] をクリックします。

9. [ポリシー (Policies)] > [アクセス制御 (Access Control)] に移動して、[ブランチのアクセスコントロールポリシー (Branch Access Control Policy)] を編集します。[ルールの追加 (Add Rule)] をクリックします。
 - a. [名前 (Name)] に「S2SVPN_Access」と入力します。
 - b. [挿入 (Insert)] を [必須にする (Into Mandatory)] に変更します。
 - c. [ソースゾーン (Source Zones)] に [OutZone] を、[送信元ネットワーク (Source Networks)] に [NGFW2_LAN] をそれぞれ追加します。
 - d. [インスペクション (Inspection)] で、[侵入ポリシー (Intrusion Policy)] に [デモ侵入ポリシー (Demo Intrusion Policy)] を、[ファイルポリシー (File Policy)] に [デモファイルポリシー (Demo File Policy)] を設定します。
 - e. [ロギング (Logging)] で、[接続の終了時にロギングする (Log at End of Connection)] をオンにします。
 - f. [追加 (Add)] をクリックします。[保存 (Save)] をクリックします。

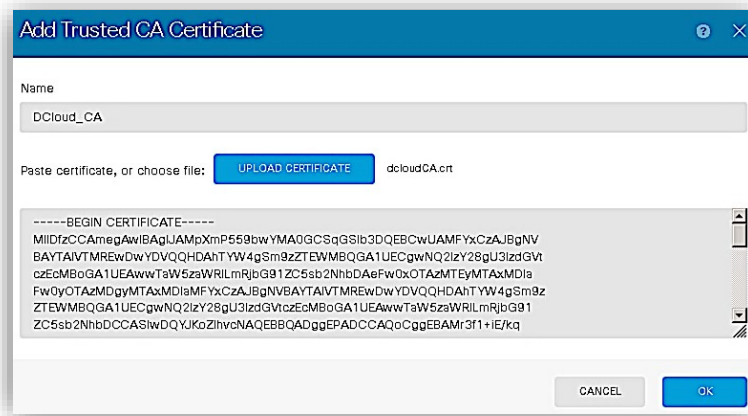


NGFW2 を管理する FDM で S2S VPN を設定する

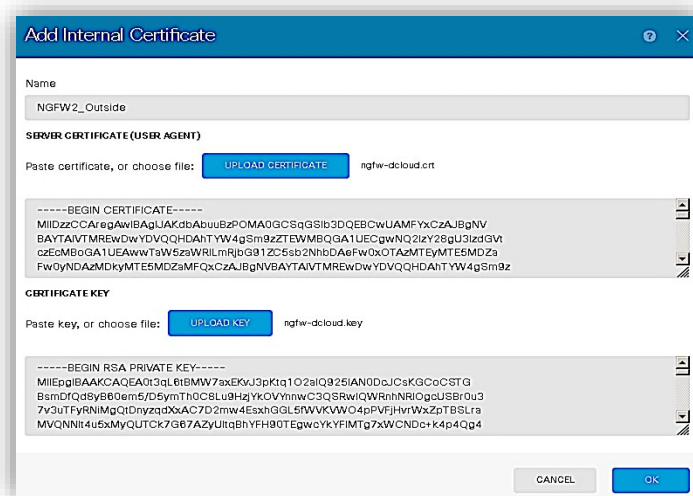
1. **Jumpbox** で、[Firefox] を開き、ブックマーク リストの [NGFW2 (FDM)] をクリックします。NGFW2 FDM にログインします。
2. [オブジェクト (Objects)] > [ネットワーク (Network)] に移動します。[+] をクリックします。
 - a. [名前 (Name)] に「NGFWBr1_LAN」と入力します。また、[タイプ (Type)] に [ネットワーク (Network)] を指定して、[ネットワーク (Network)] に「198.19.11.0/24」と入力します。

- b. [名前 (Name)]に「**NGFW2_LAN**」と入力します。また、[タイプ (Type)]に[ネットワーク (Network)]を指定して、[ネットワーク (Network)]に「**198.19.10.0/24**」と入力します。

3. FDM で RA VPN シナリオを完了している場合は、手順 3 と 4 をスキップします。それ以外の場合は、[オブジェクト (Objects)] > [証明書 (Certificates)] に移動します。[+] をクリックして、[信頼できるCA証明書の追加 (Add Trusted CA Certificate)] を選択します。
- a. [名前 (Name)]に「**DCloud_CA**」と入力します。
 - b. [証明書のアップロード (Upload Certificate)] をクリックします。[デスクトップ (Desktop)] > [証明書 (Certificates)] に移動し、[dcloudCA] を選択します。
 - c. [OK] をクリックします。



4. [+] をクリックして、[内部証明書の追加 (Add Internal Certificate)] を選択します。[証明書とキーのアップロード (Upload Certificate and Key)] をクリックします。
 - a. [名前 (Name)] に「NGFW2_Outside」と入力します。
 - b. [証明書のアップロード (Upload Certificate)] をクリックします。[デスクトップ (Desktop)] > [証明書 (Certificates)] に移動し、[ngfw-dcloud] を選択します。
 - c. [キーのアップロード (Upload Key)] をクリックします。[デスクトップ (Desktop)] > [証明書 (Certificates)] に移動し、[ngfw-dcloud] を選択します。
 - d. [OK] をクリックします。



5. [デバイス (Devices)] > [サイト間VPN (Site to Site VPN)] > [設定の表示 (View Configuration)] に移動します。[+] をクリックします。
 - a. [接続プロファイル名 (Connection Profile Name)] に「S2SVPN」と入力します。
 - b. [ローカルVPNアクセスインターフェイス (Local VPN Access Interface)] ドロップダウンから [outside] を選択します。

- c. [ローカルネットワーク (Local Network)] に [NGFW2_LAN] を追加します。
- d. [リモートIPアドレス (Remote IP Address)] に「198.18.128.81」と入力します。
- e. [リモートネットワーク (Remote Network)] に [NGFWBr1_LAN] を選択します。
- f. [次へ (Next)] をクリックします。

Connection Profile Name
SZ2VPN

LOCAL SITE

Local VPN Access Interface
outside

Local Network
+
NGFW2_LAN

REMOTE SITE

Static Dynamic

Remote IP Address
198.18.128.81

Remote Network
+
NGFWBr1_LAN

CANCEL NEXT

- g. **IKEv1** を有効にして、**IKEv2** を無効にします。
- h. [IKEポリシー (IKE Policy)] を編集して、SHA-AES256-GROUP5-CERTIFICATE を有効にします。
- i. [IPSecプロポーザル (IPSec Proposal)] を編集して [デフォルトに設定する (Set Default)] を選択し、[OK] をクリックします。
- j. [認証タイプ (Authentication Type)] に [証明書 (Certificate)] を選択します。[証明書 (Certificate)] ドロップダウンから、[NGFW2_Outside] を選択します。
- k. [その他のオプション (Additional Options)] で、[NAT適用除外 (NAT Exempt)] ドロップダウンから [inside] を選択します。
- l. [次へ (Next)] をクリックします。

IKE Policy

1 IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE Version 2

IKE Version 1

IKE Policy **Globally applied** EDIT...

IPSec Proposal **Default set selected** EDIT...

Authentication Type
 Pre-shared Manual Key Certificate

Certificate
 NGFW2_Outside

Additional Options

NAT Exempt
 inside

Diffie-Hellman Group for Perfect Forward Security
 No Perfect Forward Security (turned off)

BACK NEXT

m. [サマリー (Summary)] を確認してから [完了 (Finish)] をクリックします。

注 : FDM は、CLI 経由でのみ表示される VPN トラフィックに NAT 適用除外のステートメントを追加します。

6. [ポリシー (Policies)] > [アクセス制御 (Access Control)] に移動します。[+] をクリックします。
 - a. 新しいルールの [順序 (Order)] を [1] に設定します。
 - b. [名前 (Name)] に [S2SVPN_Access] を、[アクション (Action)] に [許可 (Allow)] を、それぞれ設定します。
 - c. [送信元 (Source)] で、[ゾーン (Zones)] を [outside_zone] に、[ネットワーク (Networks)] を [NGFWBr1_LAN] にそれぞれ設定します。

Add Access Rule

Order	Title	Action
1	S2SVPN_Access	Allow

Source/Destination Applications URLs Users Intrusion Policy File policy Logging

SOURCE

Zones	Networks	Ports
outside_zone	NGFWBr1_LAN	ANY

DESTINATION

Zones	Networks	Ports/Protocols
ANY	ANY	ANY

- d. [侵入ポリシー (Intrusion Policy)] に移動します。[侵入ポリシー (Intrusion policy)] を有効にして、[レベル (Level)] を [バランスのとれたセキュリティと接続 (Balanced Security and Connectivity)] に設定します。

Add Access Rule

Order	Title	Action
1	S2SVPN_Access	Allow

Source/Destination Applications URLs Users **Intrusion Policy** File policy Logging

INTRUSION POLICY

Level of Intrusion Policy

Balanced Security and Connectivity

Balanced Security and Connectivity

This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.

PREVENTING INTRUSIONS

Use intrusion policies as a last line of defense against unwanted traffic that you are otherwise allowing. An intrusion policy examines decoded packets for intrusions, exploits, and other attacks based on patterns, and can block or alter malicious traffic. Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings.

- e. [ファイルポリシー (File Policy)] に移動します。[マルウェアをすべてブロックする (Block Malware All)] を選択します。

Add Access Rule

Order	Title	Action
1	S2SVPN_Access	Allow

Source/Destination Applications URLs Users Intrusion Policy **File policy** Logging

SELECT THE FILE POLICY

Block Malware All

Query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.

CONTROLLING FILES AND MALWARE

Use file policies to detect malicious software, or malware, using Advanced Malware Protection for Firepower (AMP for Firepower.) You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware

- f. [ロギング (Logging)] に移動します。[ログアクションの選択 (Select Log Action)] で [接続の終了時 (At End of Connection)] を選択します。[OK] をクリックします。

設定を導入しテストする

1. **FMC** の **NGFWBR1** と、**NGFW2 FDM** の両方に設定を導入します。
2. **Jumpbox** で、[内部Linuxサーバ (Inside Linux Server)] への **PuTTY** セッションを開きます。**root/C1sco12345** でログインします。

3. 内部 Linux サーバは、NGFW2 の背後にある LAN に配置されています。198.19.11.225 の IP アドレスを使用して、ブランチ 1 のワークステーションに ping を実行します。ping は成功するはずですが、(1 回目の ping はトンネリングを開始するためにドロップする可能性があります)

```
[root@inside ~]# ping 198.19.11.225
PING 198.19.11.225 (198.19.11.225) 56(84) bytes of data:
64 bytes from 198.19.11.225: icmp_seq=2 ttl=128 time=2.91 ms
64 bytes from 198.19.11.225: icmp_seq=3 ttl=128 time=54.0 ms
64 bytes from 198.19.11.225: icmp_seq=4 ttl=128 time=2.85 ms
64 bytes from 198.19.11.225: icmp_seq=5 ttl=128 time=2.25 ms
64 bytes from 198.19.11.225: icmp_seq=6 ttl=128 time=2.88 ms
64 bytes from 198.19.11.225: icmp_seq=7 ttl=128 time=3.12 ms
64 bytes from 198.19.11.225: icmp_seq=8 ttl=128 time=2.10 ms
^C
--- 198.19.11.225 ping statistics ---
8 packets transmitted, 7 received, 12% packet loss, time 7008ms
rtt min/avg/max/mdev = 2.109/10.027/54.046/17.973 ms
[root@inside ~]#
```

4. NGFW2 または NGFWBR1 のいずれかに、PuTTY 経由でログインし、show crypto ikev1 sa と show crypto ipsec sa を実行することで、トンネル ステータスを確認できます。

```
NGFWBR1
> show crypto ikev1 sa
IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 198.18.133.82
  Type    : L2L           Role    : responder
  Rekey   : no          State   : NM_ACTIVE
>
> show crypto ipsec sa
interface: outside
Crypto map tag: CSM_outside_map, seq num: 1, local addr: 198.18.128.81

access-list CSM_IPSEC_ACL_1 extended permit ip 198.19.11.0 255.255.255.0 198.19.10.0 255.255.255.0/0/0
local ident (addr/mask/prot/port): (198.19.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
current_peer: 198.18.133.82

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 7, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frags needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#valid ICMP Errors rcvd: 0, #invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 198.18.128.81/0, remote crypto endpt.: 198.18.133.82/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 5DDA5050
current inbound spi : 6AB7CCC7

inbound esp sas:
spi: 0x6AB7CCC7 (1790430407)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings = (L2L, Tunnel, IKEv1, )
slot: 0, conn id: 1, crypto-map: CSM_outside_map
sa timing: remaining key lifetime (kB/sec): (3914999/28613)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000000FF
outbound esp sas:
spi: 0x5DDA5050 (1574588496)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings = (L2L, Tunnel, IKEv1, )
slot: 0, conn id: 1, crypto-map: CSM_outside_map
sa timing: remaining key lifetime (kB/sec): (3914999/28613)
IV size: 16 bytes
```

5. NGFW2 または NGFWBR1 のいずれかに、PuTTY 経由でログインし、`show vpn-sessiondb detail I2I` を実行することで使われているトンネル認証方式を確認できます。

```
NGFW2
> show vpn-sessiondb detail I2I

Session Type: LAN-to-LAN Detailed

Connection   : 198.18.128.81
Index        : 1                               IP Addr      : 198.18.128.81
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES256 IPsec: (1)AES256
Hashing      : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx     : 60312                            Bytes Rx     : 60312
Login Time   : 10:38:14 UTC Wed May 8 2019
Duration    : 0h:12m:00s
Tunnel Zone  : 0

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
Tunnel ID    : 1.1
UDP Src Port : 500                               UDP Dst Port : 500
IKE Neg Mode : Main                             Auth Mode    : rsaCertificate
Encryption   : AES256                           Hashing      : SHA1
Rekey Int (T): 86400 Seconds                     Rekey Left(T): 85681 Seconds
D/H Group    : 5
Filter Name  :

IPsec:
Tunnel ID    : 1.2
Local Addr   : 198.19.10.0/255.255.255.0/0/0
Remote Addr  : 198.19.11.0/255.255.255.0/0/0
Encryption   : AES256                           Hashing      : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds                     Rekey Left(T): 28081 Seconds
Rekey Int (D): 4608000 K-Bytes                   Rekey Left(D): 4607942 K-Bytes
Idle Time Out: 30 Minutes                       Idle TO Left : 30 Minutes
Bytes Tx     : 60312                            Bytes Rx     : 60312
Pkts Tx      : 718                             Pkts Rx      : 718

>
```

シナリオ 7: NGFW のデバイス API

6.2.3 以降、デバイス API が公開されています。6.3 および 6.4 リリースでは、デバイス API が、FDM の機能とともに拡張されています。

このシナリオの目的は、デバイス API にアクセスする以下のようなツールを受講者に紹介することです。

- Python スクリプトの使用
- Cisco モジュールと Ansible の使用
- API エクスプローラの使用

最初の 2 つのタスクの後、残りのタスクを任意の順序で実施することも、スキップすることもできます。

Python スクリプトを実行して最初のデバイス設定を行う

内部 Linux サーバの `/usr/local/bin` ディレクトリに **NGFWsetup** という Python スクリプトがあります。このスクリプトは次の操作を実行します。

- FDM EZ セットアップ ウィザードによって実行されるすべてのタスク
 - 内部インターフェイスの設定
 - 脅威、マルウェア、および URL フィルタリングのライセンスを有効にする
1. 新しいブラウザ タブを開いて、ブックマーク バーの [Aux] ブックマークをクリックします。開いたページの [dCloud ラボの API スクリプト (API Scripts for dCloud Lab)] セクションには、このシナリオで確認が必要なスクリプトへのリンクがいくつか表示されます。
 2. Firefox ブラウザで新しいタブを開き、ブックマーク バーの [NGFW3] ブックマークを選択します。**admin** としてログインします。パスワードは **C1sco12345** を使用します。セットアップ ウィザードが実行されていないことを確認します。NGFW3 FDM からログアウトします。
 3. 内部 Linux サーバで、**NGFWsetup** コマンドを実行します。応答を求められたら、[3] を選択して NGFW3 をセットアップします。
 4. スクリプトが実行されている間 (数分かかります)、開いたブラウザのタブで、**NGFWsetup** スクリプトを確認します。認証トークンの生成、EULA への同意、ネットワーク設定、ライセンスの有効化など、主要な API コールを特定してみましょう。

Ansible を使用して NGFW 設定を変更する

Ansible は、プロビジョニング、設定、展開を自動化するシンプルな自動化エンジンです。ノードに接続して（デフォルトでは SSH を使用）、「Ansible モジュール」と呼ばれる小さなプログラムをそのノードにプッシュします。その後、これらのモジュールを実行し、終了後、そのモジュールを削除します。Ansible スクリプトは YAML で記述されています。

このシナリオの目的は、受講者に、Ansible と Cisco FTD Ansible モジュールを紹介することです。Ansible を使用して、前のタスクで作成したアクセス コントロール ポリシー ルールを変更します。

注：このラボでは、Ansible が Docker にインストールされています。受講者が Docker に詳しくない場合は、このラボ演習で簡単に紹介します。

1. 内部 Linux サーバで、**docker images** コマンドを実行して、Cisco FTD Ansible イメージがインストールされていることを確認します。

```
[root@inside ~]# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
<none>              <none>             c22062ef897c      7 days ago        1.02 GB
docker.io/python    3.6                d6b15f660ce8      13 days ago       924 MB
docker.io/python    latest             32260605cf7a      13 days ago       929 MB
docker.io/cisco devnet/ftd-ansible latest             b5d7571749c6     5 weeks ago     1.01 GB
[root@inside ~]#
```

2. **cat /AnsibleInventory/ftd-inventory** コマンドを実行します（タブ補完を使用します）。これは Ansible のインベントリであり、アクセス対象のデバイスと、そのアクセス方法を示しています。この例では、1 つのデバイス NGFW3 があります。

```
[root@inside ~]# cat /AnsibleInventory/ftd-inventory
my-ftd ansible_host=198.19.10.83 ansible_port=443 ansible_network_os=ftd ansible_user=admin
ansible_password=C1sco12345 ansible_httppapi_use_ssl=True ansible_httppapi_validate_certs=False
ansible_httppapi_ftd_token_path=/api/fdm/latest/fdm/token
[root@inside ~]#
```

3. **ls /yaml** コマンドを実行します。YAML ファイルである **changetherule.yml** を Ansible プレイブックとして使用します。
4. **dockerrun changetherule.yml** コマンドを実行します。これにより、次の Docker のコマンドが実行されます。
docker run -v /yaml:/ftd-ansible/playbooks -v /AnsibleInventory:/etc/ansible/hosts cisco
devnet/ftd-ansible playbooks/changetherule.yml
-v オプションは、マウント ボリューム（ファイル システムのホスト ファイル システムにおける絶対パス）をコンテナ内のディレクトリにバインドします。**FAILED - RETRYING** のメッセージは無視しても構いません。これらは想定内のメッセージであり、スクリプトが FDM にポーリングして導入が進行中かどうかを確認することにより生じるものです。
5. スクリプトが実行されている間（数分かかります）、開いたブラウザのタブで、**changetherule.yml** スクリプトの内容を確認します。

- 1 番目のタスクは、バランスのとれた侵入ポリシーの ID を取得します。

- 2 番目のタスクは、サポートされているすべてのマルウェア ファイル タイプをブロックするファイル ポリシーの ID を取得します。
 - 3 番目のタスクは、アクセス コントロール ポリシーの実行を更新します。API コールの **PERMIT** アクションは、FDM の **Allow** に対応しています。
 - 4 番目のタスクは、ポリシーの導入を開始します。
 - 5 番目と 6 番目のタスクは、導入が成功したかどうか、およびいつ成功したかを判断します。
6. NGFW3 FDM の [ポリシー (Policy)] ページを更新します。アクセス コントロール ポリシー ルールが必要に応じて変更されていることを確認します。

注 : docker run コマンドを実行するたびに、新しいコンテナが作成されます。作成されたコンテナはそのまま残ります。docker container list --all コマンドを実行すると、その状況を確認できます。このラボのために、作成されたすべてのコンテナを削除する dockerclear というスクリプトが作成されています。

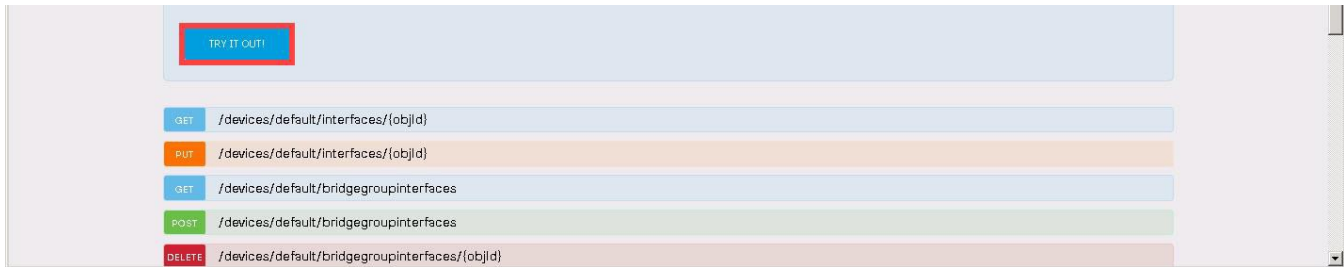
FDM API エクスプローラの使用

ここでは、組み込みの FDM API エクスプローラを使用して、G0/0 のインターフェイス設定を変更します。

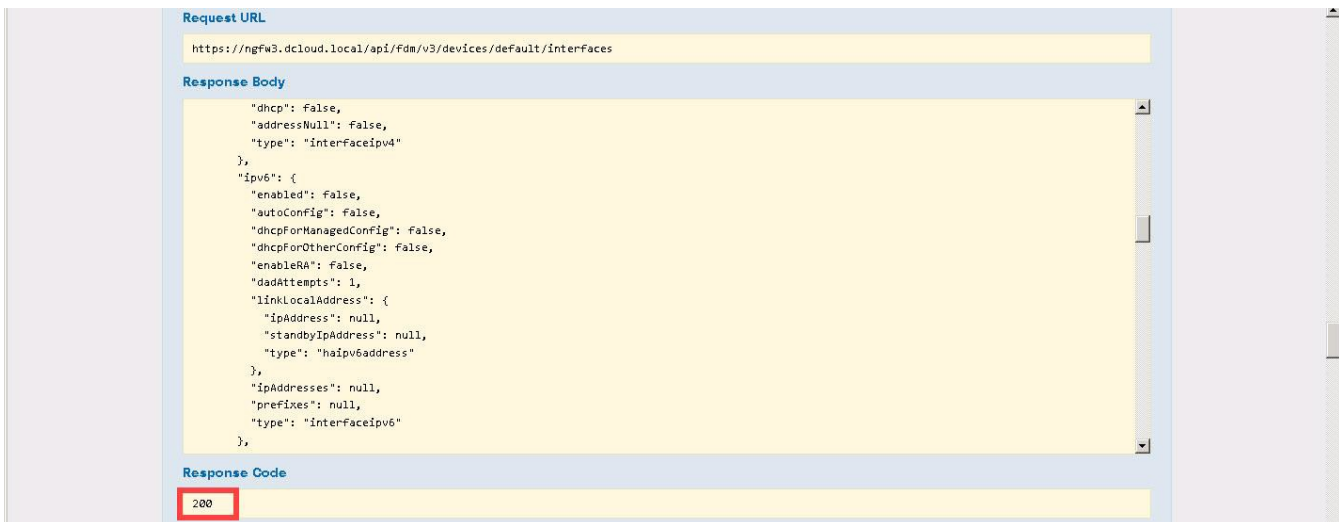
1. API エクスプローラを使用するには、すでに FDM GUI にログインしている必要があります。ログインしていない場合は、タブを開き、[NGFW3 (FDM)] ブックマークをクリックします。admin としてログインします。パスワードは **C1sco12345** を使用します。
2. Firefox で新しいタブを開き、[NGFW3 (API Explorer)] ブックマークをクリックします。
3. ページに目を通して [ヘルプ (Help)] セクションに注目してください。各機能の API コールと、グループ化された使用例を確認できます。
4. 最初にエクスプローラを使用して、NGFW3 のインターフェイス設定を表示します。[インターフェイス (Interface)] をクリックして、それに関連付けられた API コールを展開します。そのセクションの最初に表示されている API **GET /devices/default/interfaces** をクリックします。

IdentityServicesEngine	Show/Hide	List Operations	Expand Operations
IkevOnePolicy	Show/Hide	List Operations	Expand Operations
IkevOneProposal	Show/Hide	List Operations	Expand Operations
IkevTwoPolicy	Show/Hide	List Operations	Expand Operations
IkevTwoProposal	Show/Hide	List Operations	Expand Operations
InitialProvision	Show/Hide	List Operations	Expand Operations
Interface	Show/Hide	List Operations	Expand Operations
GET	/devices/default/interfaces		
GET	/devices/default/interfaces/{objId}		
PUT	/devices/default/interfaces/{objId}		
GET	/devices/default/bridgegroupinterfaces		
POST	/devices/default/bridgegroupinterfaces		
DELETE	/devices/default/bridgegroupinterfaces/{objId}		

- この API コールに提供されている詳細情報をスクロールします。[ステータス確認 (TRY IT OUT!)] というラベルのボタンが表示されたら、そのボタンをクリックしてください。



- さらに下にスクロールして、API コールが応答コード [200] を返したことを確認します。



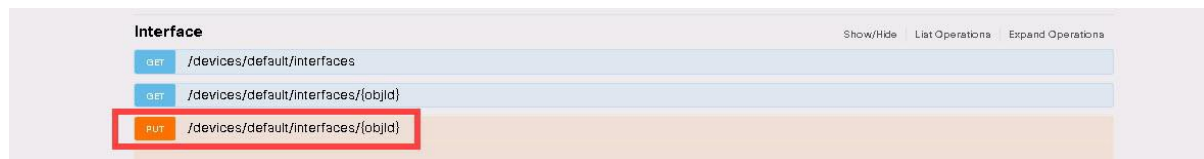
- Jumpbox デスクトップでテキスト ファイルを開きます。GigabitEthernet0/0 の JSON セクションを切り取り、テキスト ドキュメントに貼り付けます。IP アドレスを `198.18.133.83` から `198.18.133.183` に変更します。また、このオブジェクトの ID をメモします。これは、インターフェイス設定の変更に必要です。

```

New Text Document - Notepad
File Edit Format View Help
{
  "version": "f4uryv7v5bwhw",
  "name": "outside",
  "description": null,
  "hardwareName": "GigabitEthernet0/0",
  "monitorInterface": true,
  "ipv4": {
    "ipType": "STATIC",
    "defaultRouteUsingDHCP": false,
    "dhcpRouteMetric": null,
    "ipAddress": {
      "ipAddress": "198.18.133.183",
      "netmask": "18",
      "standbyIpAddress": null,
      "type": "haipv4address"
    },
    "dhcp": false,
    "addressNull": false,
    "type": "interfaceipv4"
  },
  "ipv6": {
    "enabled": false,
    "autoConfig": false,
    "dhcpForManagedConfig": false,
    "dhcpForOtherConfig": false,
    "enablerA": false,
    "dadAttempts": 1,
    "linkLocalAddress": {
      "ipAddress": null,
      "standbyIpAddress": null,
      "type": "haipv6address"
    },
    "ipAddresses": null,
    "prefixes": null,
    "type": "interfaceipv6"
  },
  "managementOnly": false,
  "linkState": "up",
  "mtu": 1500,
  "enabled": true,
  "macAddress": null,
  "standbyMacAddress": null,
  "speedType": "AUTO",
  "duplexType": "AUTO",
  "mode": "ROUTED",
  "managementInterface": false,
  "tenGigabitInterface": false,
  "gigabitInterface": true,
  "id": "8d6c41df-3e5f-465b-8e5a-d336b282f93f",
  "type": "physicalInterface",
  "links": {
    "self": "https://ngfw3.dcloud.local/api/fdm/v3/devices/default/interfaces/8d6c41df-3e5f-465b-8e5a-d336b282f93f"
  }
}

```

8. [GET] をクリックして、API コール ページを折りたたみます。[PUT] をクリックします。[PUT] は [インターフェイス (Interface)] セクションの 3 番目の API コールです。



9. [パラメータ (Parameters)] セクションまでスクロールします。サンプルに注目してください。リクエストの本文を手作業で作成している場合、このサンプルをクリックして本文のテキストボックスに入力し、編集できます。



10. [モデル (Model)] をクリックします。要求本文の各属性の詳細が表示されます。属性の多くはオプションであることを確認します。

The screenshot shows a parameter field labeled 'body' with a '(required)' indicator. Below the field is a dropdown menu for 'Parameter content type' set to 'application/json'. To the right, a sidebar shows a 'Model' tab selected, displaying details for 'PhysicalInterface {'. The description reads: 'An object specifying Physical interface and its properties. (Note: The field level constraints listed here might not cover all the constraints on the field. Additional constraints might exist.)'. A 'version' property is also listed: '(string, optional): A unique string version assigned by the system when the object is created or modified. No assumption can be made on the format or content of this identifier.'

11. インターフェイスの ID を、テキスト ドキュメントから **objId** パラメータ フィールドにコピーします。インターフェイスの開始部分用に変更した JSON を本文のパラメータ フィールドにコピーします。

The screenshot shows the 'Parameters' section with a table-like structure. The 'objId' parameter has a value of '8d6c41df-3e5f-465b-8e5a-d336b282f93f'. The 'body' parameter has a JSON value:

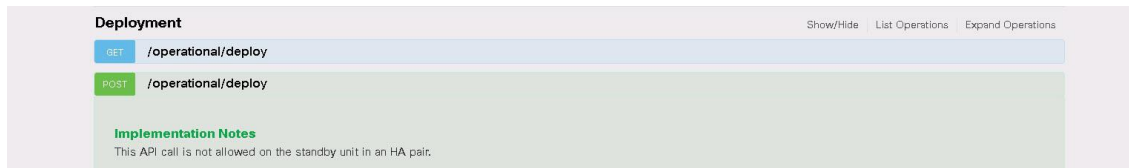
```
{
  "version": "f4uryv7v5bwh",
  "name": "outside",
  "description": null,
  "hardwareName": "GigabitEthernet0/0",
  "monitorInterface": true,
  "ipv4": {
```

. The 'Parameter content type' dropdown is set to 'application/json'.

12. 下にスクロールして [ステータス確認 (TRY IT OUT!)] をクリックします。
13. FDM で、IP アドレスの変更が保留中であることを確認します。

The screenshot shows a 'Pending Changes' dialog box. At the top, it says 'Last Deployment Completed Successfully' on '19 Mar 2019 10:19 PM'. Below this is a table comparing 'Deployed Version (19 Mar 2019 10:19 PM)' and 'Pending Version'. A legend indicates that a blue circle with a double arrow means 'Changed'. The table shows that the 'ipv4.ipAddress.ipAddress' for the interface 'outside' has changed from '198.18.133.83' to '198.18.133.183'.

14. API エクスプローラの [導入 (Deployment)] セクションを開きます。[POST /operational/deploy] API コールを展開し、下にスクロールして [ステータス確認 (TRY IT OUT!)] をクリックします。



15. 必要に応じて、導入 GET メソッド API を使用して、導入のステータスを追跡できます。

©2019 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2019 年 7 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
<http://www.cisco.com/jp>

お問い合わせ先