

FTDでのAnyConnectリモートアクセスVPNでのISEポスチャの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図とトラフィックフロー](#)

[コンフィギュレーション](#)

[FTD/FMC](#)

[ISE](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、Identity Services Engine(ISE)に対してVPNユーザをポスチャするようにFirepower Threat Defense(FTD)バージョン6.4.0を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AnyConnect リモート アクセス VPN
- FTDでのリモートアクセスVPNの設定
- Identity Services Engineとポスチャサービス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

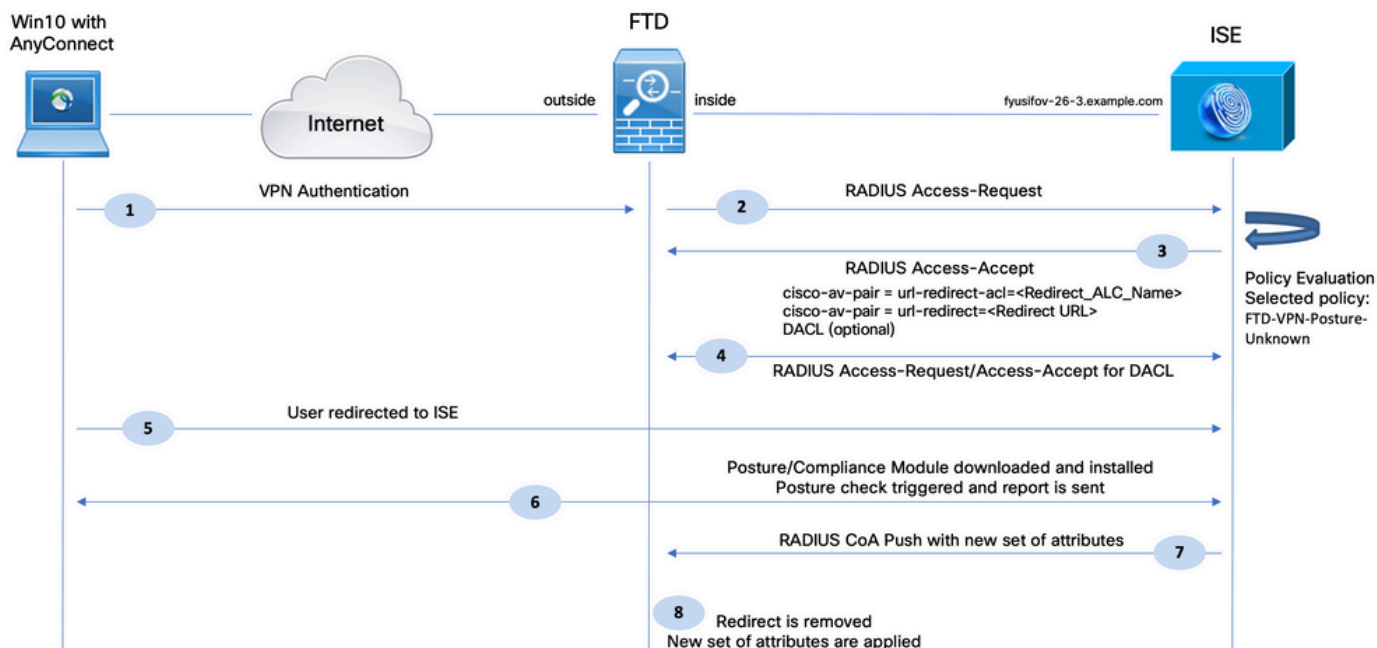
- Cisco Firepower 脅威対策(FTD)ソフトウェアバージョン6.4.0
- Cisco Firepower マネジメント コンソール(FMC)ソフトウェアバージョン6.5.0
- Cisco AnyConnect セキュア モビリティ クライアントバージョン4.7がインストールされた Microsoft Windows 10
- Cisco Identity Services Engine(ISE)バージョン2.6およびパッチ3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図とトラフィック フロー



1. リモートユーザは、FTDへのVPNアクセスにCisco Anyconnectを使用します。

2. FTDがそのユーザのRADIUS Access-RequestをISEに送信します。

3. その要求が、ISE上のFTD-VPN-Posture-Unknownという名前のポリシーにヒットします。ISEは、次の3つの属性を持つRADIUS Access-Acceptを送信します。

- cisco-av-pair = url-redirect-acl=fyusifovredirect : これは、リダイレクトされるトラフィックを決定する、FTD上でローカルに定義されたアクセスコントロールリスト(ACL)の名前です。
- cisco-av-pair = url-redirect=<https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp> : リモートユーザのリダイレクト先となるURLです。
- DACL = PERMIT_ALL_IPV4_TRAFFIC : ダウンロード可能ACL。この属性はオプションです。このシナリオでは、すべてのトラフィックがDACLで許可されます)

4. DACLが送信された場合、DACLのコンテンツをダウンロードするためにRADIUSアクセス要求/アクセス承認が交換されます

5. VPNユーザからのトラフィックがローカルに定義されたACLに一致すると、ISEクライアントプロビジョニングポータルにリダイレクトされます。ISEはAnyConnectポスチャモジュールとコンプライアンスモジュールをプロビジョニングします。

6. エージェントがクライアントマシンにインストールされると、プローブを使用してISEが自動的に検索されます。ISEが正常に検出されると、エンドポイントでポスチャ要件がチェックされます。この例では、エージェントはインストールされているマルウェア対策ソフトウェアを確認します。次に、ポスチャレポートをISEに送信します。

7. ISEがエージェントからポスチャレポートを受信すると、ISEはこのセッションのポスチャステータスを変更し、新しい属性でRADIUS CoAタイプのプッシュをトリガーします。今回は、ポスチャステータスが判明し、別のルールがヒットします。

- ユーザが準拠している場合、フルアクセスを許可するDACL名が送信されます。
- ユーザが非準拠の場合、制限付きアクセスを許可するDACL名が送信されます。

8. FTDがリダイレクションを削除します。FTDがISEからDACLをダウンロードするためにAccess-Requestを送信します。特定の DACL が VPN セッションに付加されます。

コンフィギュレーション

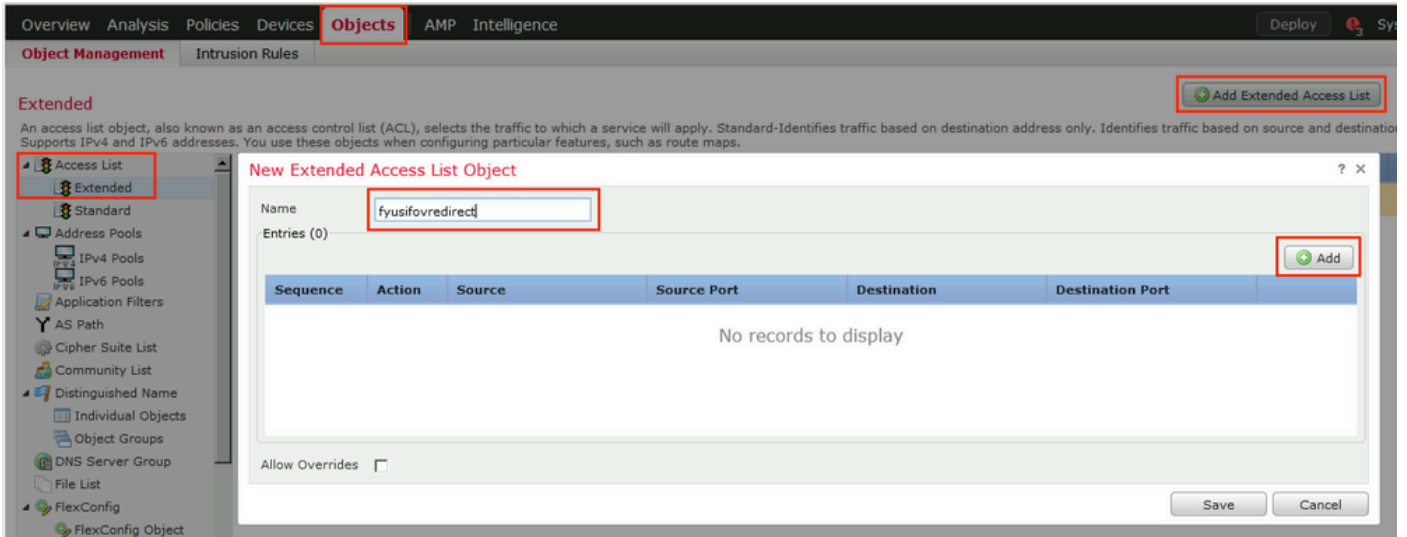
FTD/FMC

ステップ 1 : ISEおよび修復サーバ (存在する場合) のネットワークオブジェクトグループを作成します。Objects > Object Management > Networkの順に移動します。

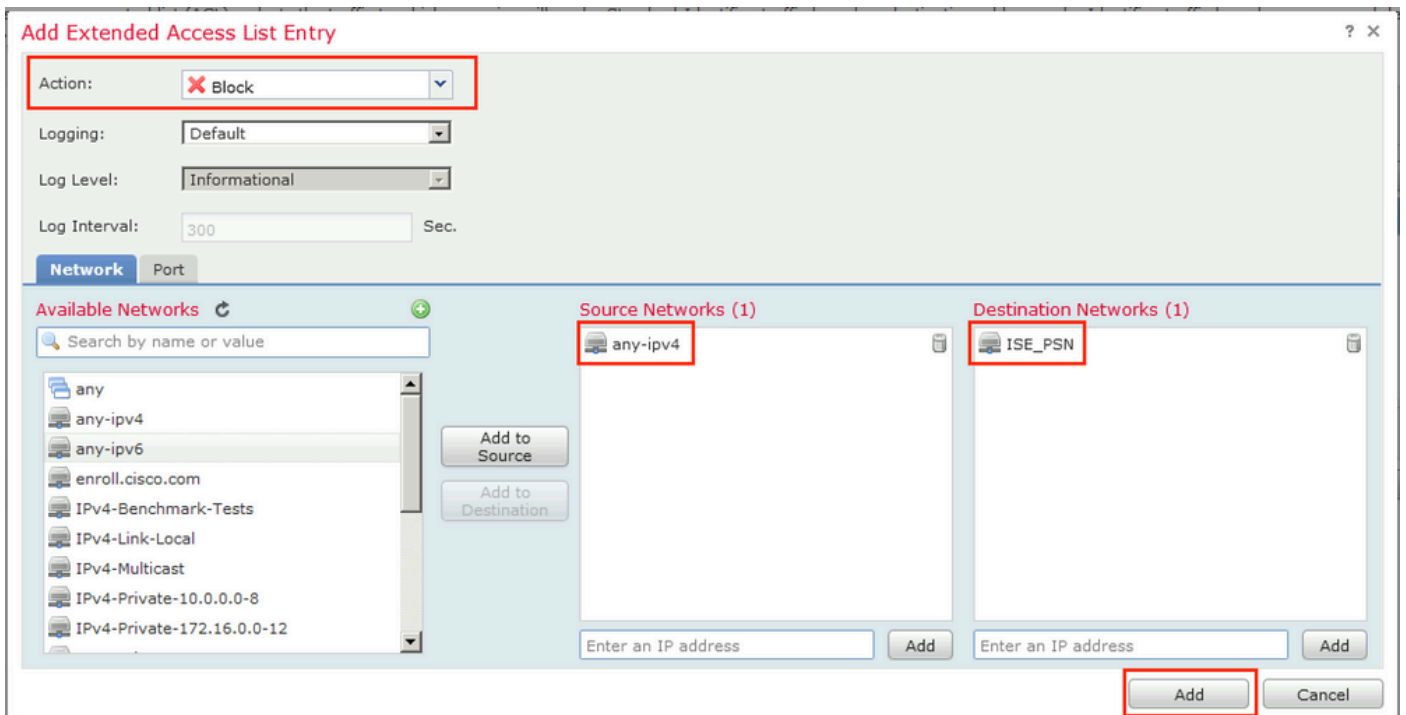
The screenshot shows the Cisco FTD/FMC configuration interface. The 'Objects' tab is selected, and the 'Network' section is active. A dialog box titled 'Edit Network Object' is open, showing the configuration for a new network object. The 'Name' field is 'ISE_PSN', the 'Description' field is empty, and the 'Network' field is '192.168.15.14'. The 'Host' radio button is selected under the 'Network' section. The 'Allow Overrides' checkbox is unchecked. The 'Save' and 'Cancel' buttons are visible at the bottom of the dialog.

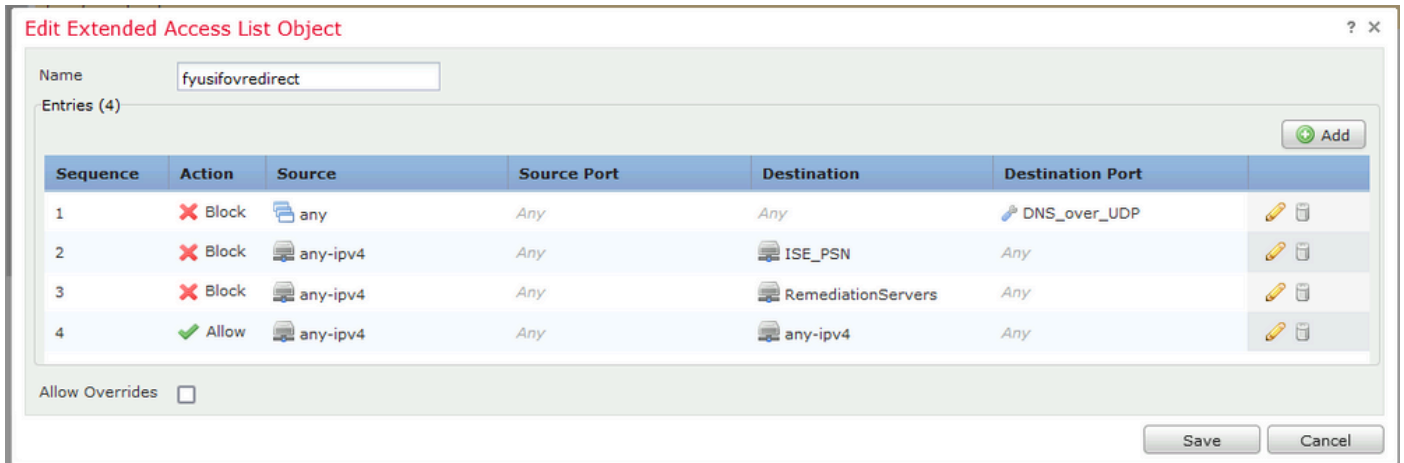
Name	Value
any-ipv4	0.0.0.0/0
any-ipv6	::/0
enroll.cisco.com	72.163.1.80
IPv4-Benchmark-Tests	
IPv4-Link-Local	
IPv4-Multicast	
IPv4-Private-10.0.0.0-8	
IPv4-Private-172.16.0.0-12	
IPv4-Private-192.168.0.0-16	
IPv4-Private-All-RFC1918	
IPv6-IPv4-Mapped	::ffff:0.0.0.0/96
IPv6-Link-Local	fe80::/10
IPv6-Private-Unique-Local-Addresses	fc00::/7
IPv6-to-IPv4-Relay-Anycast	192.88.99.0/24

ステップ 2 : リダイレクトACLを作成します。Objects > Object Management > Access List > Extendedの順に移動します。Add Extended Access Listをクリックして、リダイレクトACLの名前を指定します。この名前は、ISE認可結果と同じである必要があります。



ステップ 3 : リダイレクトACLエントリを追加します。[Add] ボタンをクリックします。DNS、ISE、および修復サーバへのトラフィックをブロックして、リダイレクトから除外します。残りのトラフィックを許可すると、リダイレクトがトリガーされます (必要に応じてACLエントリをより具体的にすることができます)。





ステップ 4 : ISE PSNノードを追加します。Objects > Object Management > RADIUS Server Groupの順に移動します。Add RADIUS Server Groupをクリックし、名前を入力して、すべてのチェックボックスをオンにし、プラス記号のアイコンをクリックします。

Edit RADIUS Server Group ? X

Name:* ISE

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
No records to display

Save Cancel

ステップ 5 : 開いたウィンドウで、ISE PSN IPアドレスとRADIUSキーを入力し、[Specific Interface] を選択し、ISEが到達可能なインターフェイス (このインターフェイスはRADIUSトラフィックの送信元として使用されます) を選択してから、以前に設定した[Redirect ACL] を選択します。

New RADIUS Server

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

Authentication Port:* (1-65535)

Key:*

Confirm Key:*

Accounting Port: (1-65535)

Timeout: (1-300) Seconds

Connect using: Routing Specific Interface i

v +

Redirect ACL: v +

手順 6 : VPNユーザー用のアドレスプールを作成します。Objects > Object Management > Address Pools > IPv4 Poolsの順に移動します。Add IPv4 Poolsをクリックして、詳細を入力します。

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy 5

Object Management Intrusion Rules

IPv4 Pools Add IPv4 Pools

IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.

Address Pools

- Standard
- Address Pools**
 - IPv4 Pools
 - IPv6 Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- Distinguished Name
- Individual Objects
- Object Groups
- DNS Server Group
- File List
- FlexConfig
 - FlexConfig Object
 - Text Object
- Geolocation
- Interface

Edit IPv4 Pool

Name*

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

Mask

Description

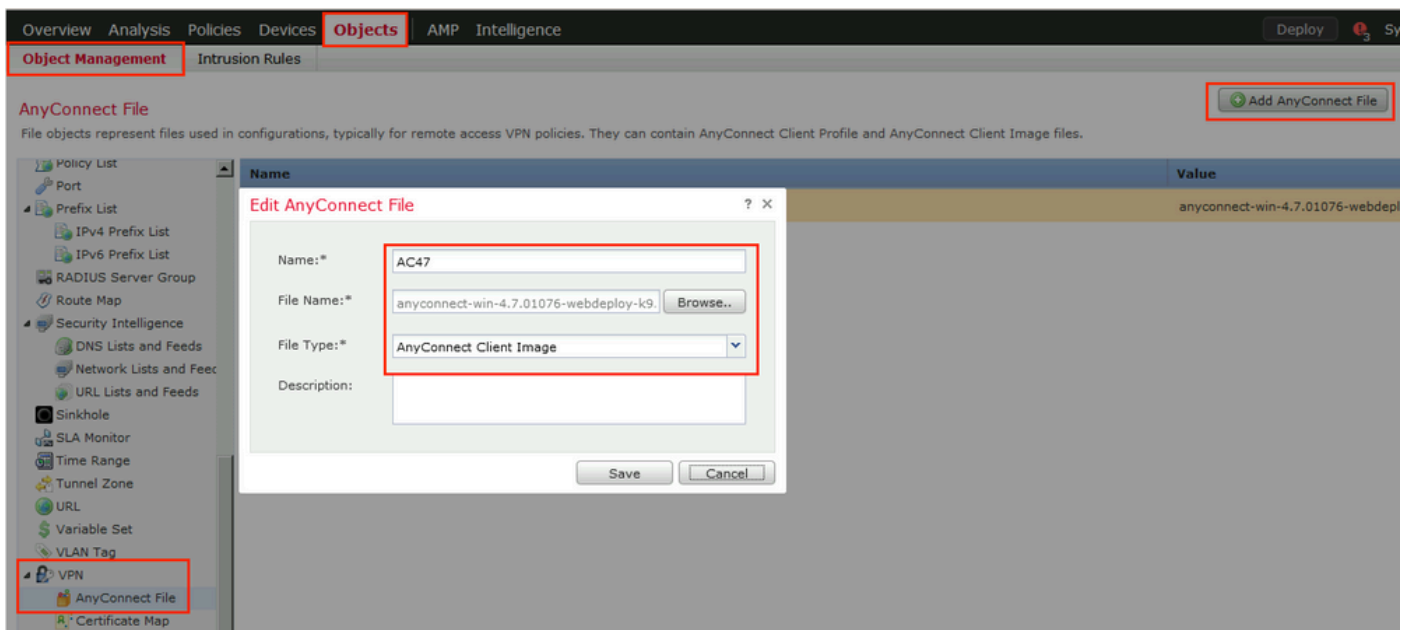
Allow Overrides

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

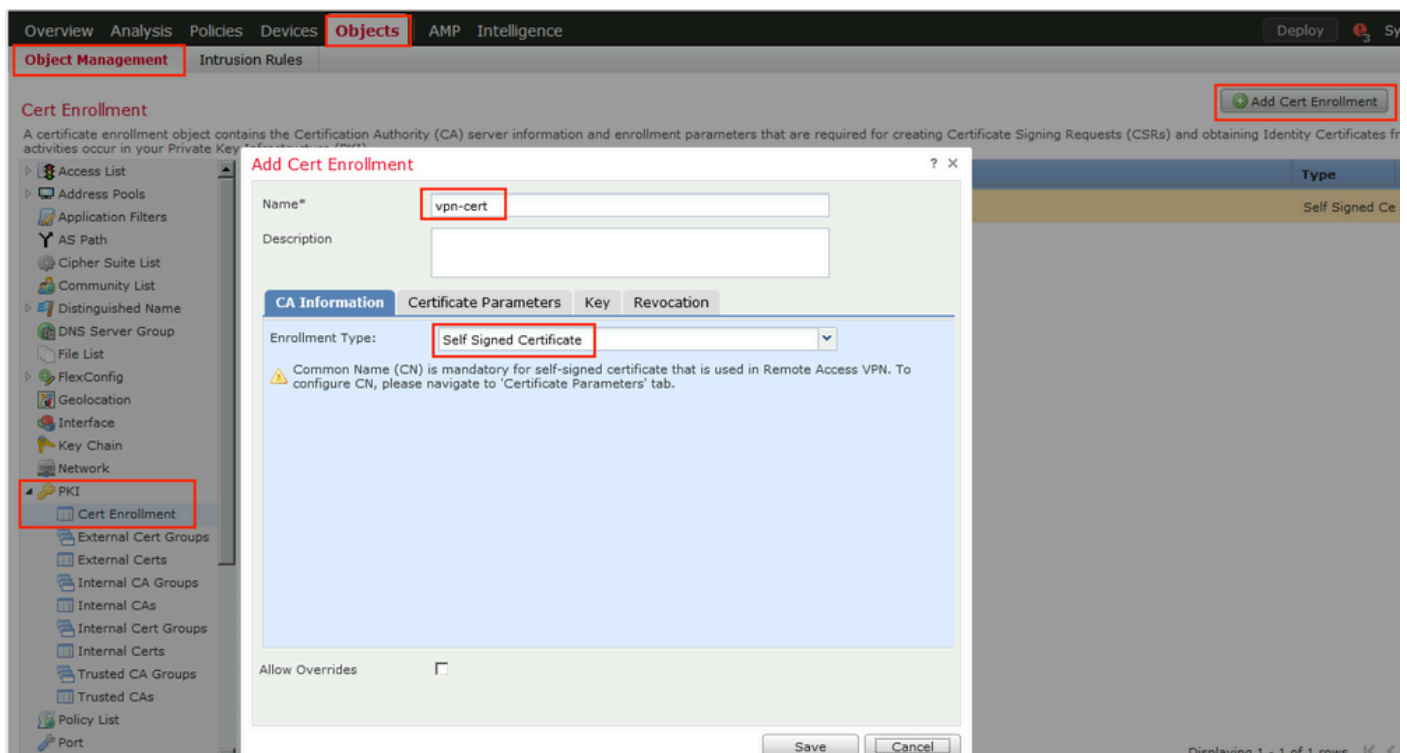
Override (0)

手順 7 : AnyConnectパッケージを作成します。Objects > Object Management > VPN > AnyConnect Fileの順に移動します。Add AnyConnect Fileをクリックしてパッケージ名を指定し

、Cisco Software Downloadからパッケージをダウンロードして、Anyconnect Client Image File Typeを選択します。



ステップ 8 : Certificate Objects > Object Management > PKI > Cert Enrollmentの順に移動します。Add Cert Enrollmentをクリックして名前を入力し、Self Signed Certificate in Enrollment Typeを選択します。Certificate Parametersタブをクリックして、CNを指定します。



Add Cert Enrollment

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

ステップ 9 : リモートアクセスVPNウィザードを起動します。Devices > VPN > Remote Accessの順に移動し、Addをクリックします。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Name	Status	Last Modified
No configuration available Add a new configuration		

ステップ 10 : 名前を入力し、VPNプロトコルとしてSSLをチェックし、VPNコンセンレータとして使用されるFTDを選択して、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

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:
192.168.15.11

Selected Devices: 192.168.15.11

Before You Start
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.

Back Next Cancel

ステップ 11 Connection Profileの名前を入力し、Authentication/Accounting Serversを選択し、以前に設定したアドレスプールを選択して、Nextをクリックします。

 注：認証サーバは選択しないでください。1人のユーザに対して2つのアクセス要求がトリガーされます(1回目はユーザパスワード、2回目はパスワードcisco)。

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

Authentication Method:

Authentication Servers:* (Realm 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

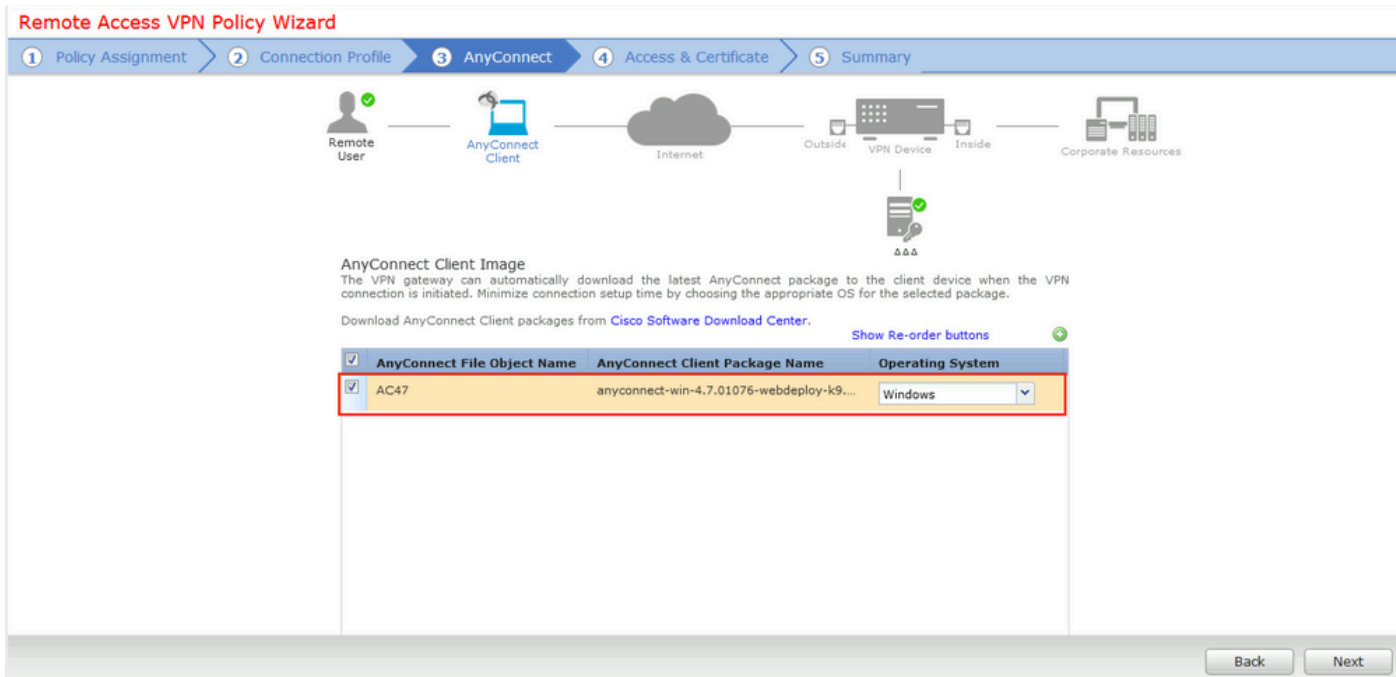
IPv4 Address:
IPv6 Address:

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.

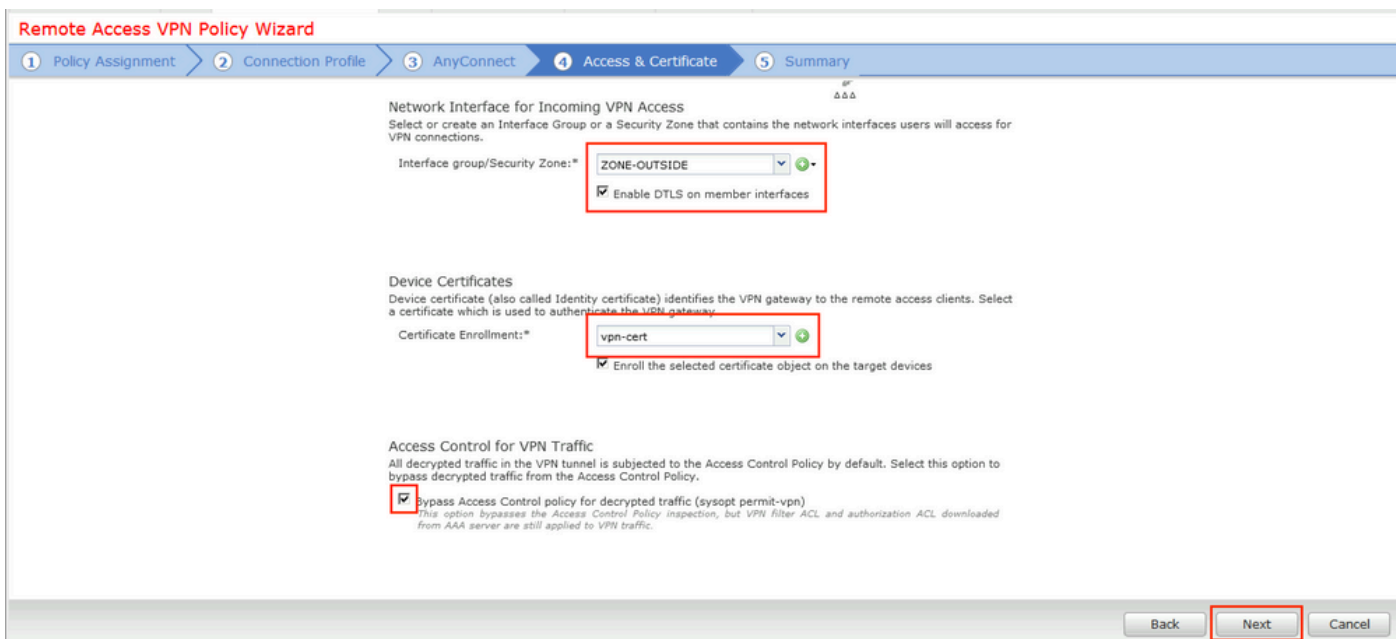
Group Policy:* ⓘ
[Edit Group Policy](#)

Back Next Cancel

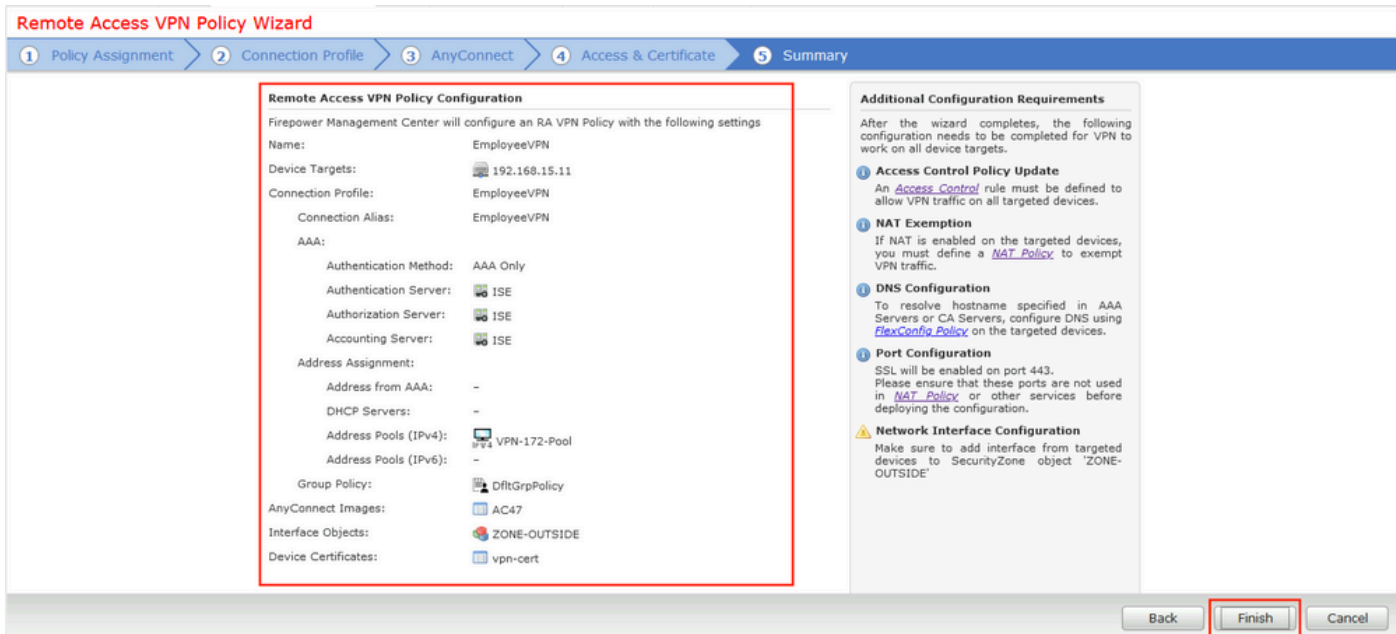
ステップ 12以前に設定したAnyConnectパッケージを選択し、Nextをクリックします。



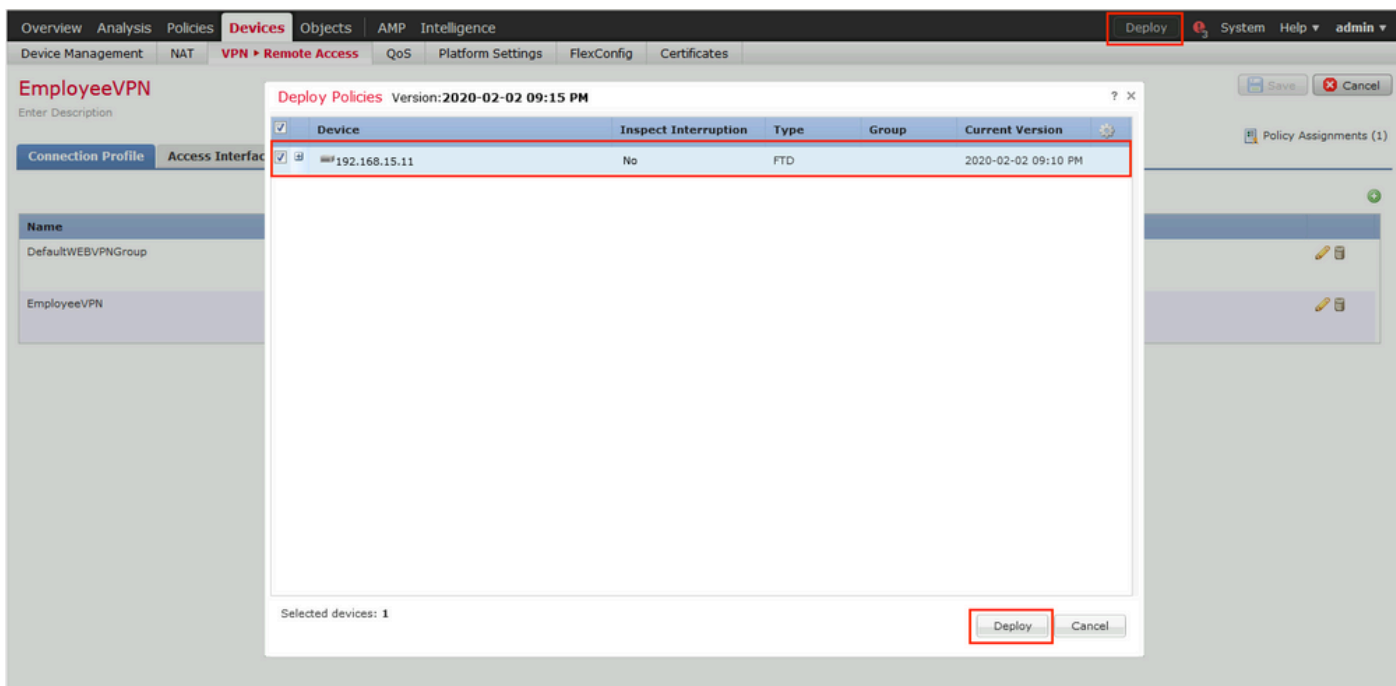
ステップ 13 VPNトラフィックが予想されるインターフェイスを選択し、以前に設定した Certificate Enrollmentを選択して、Nextをクリックします。



ステップ 14 : サマリーページを確認し、Finishをクリックします。



ステップ 15 : FTDに設定を展開します。Deployをクリックし、VPNコンセントレータとして使用するFTDを選択します。



ISE

ステップ 1 : ポスチャ更新を実行します。[Administration] > [System] > [Settings] > [Posture] > [Updates] に移動します。

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

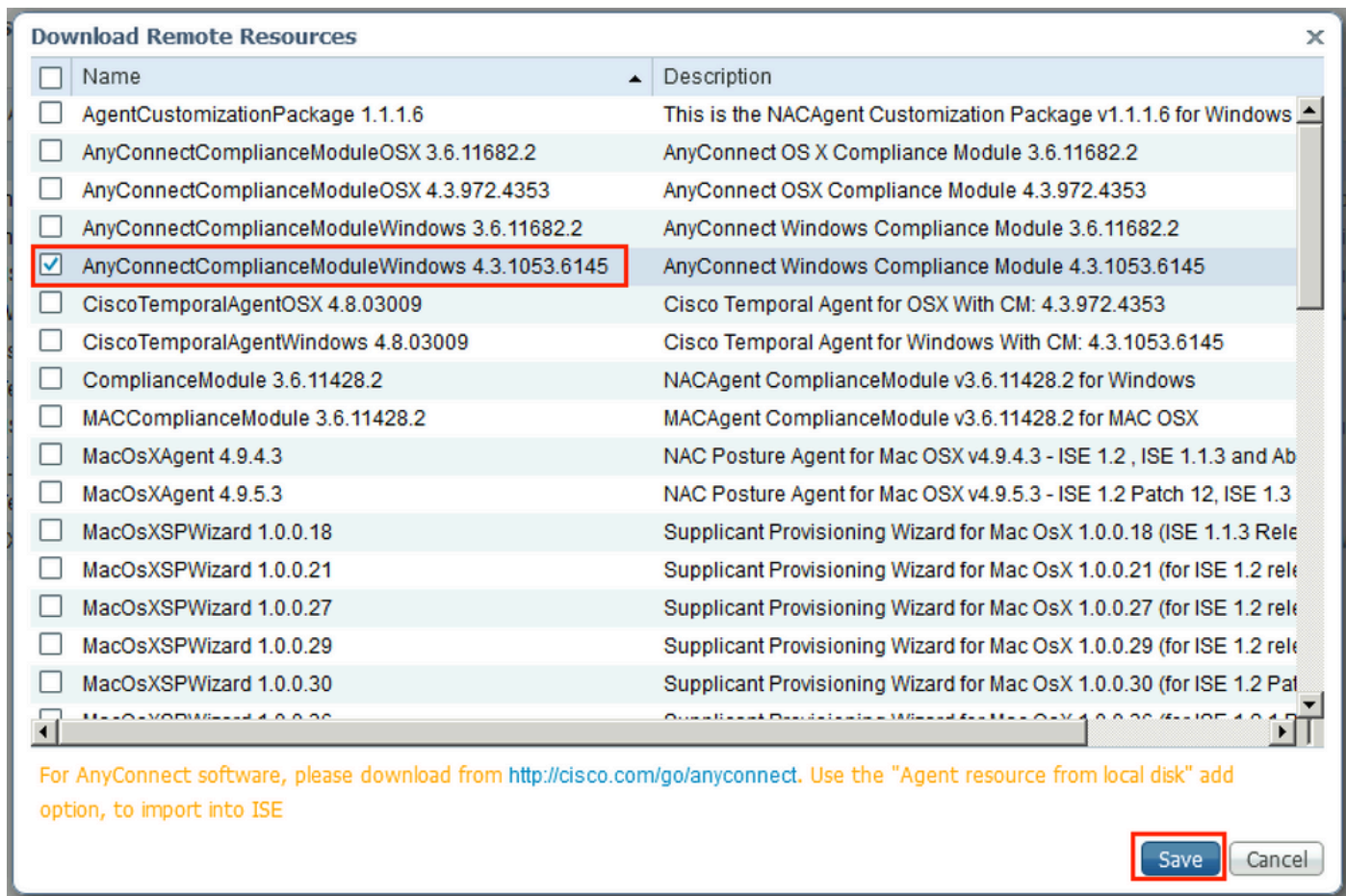
Proxy Port HH MM SS

Automatically check for updates starting from initial delay every hours ⓘ

▼ Update Information

Last successful update on	2020/02/02 20:44:27 ⓘ
Last update status since ISE was started	Last update attempt at 2020/02/02 20:44:27 was successful ⓘ
Cisco conditions version	257951.0.0.0
Cisco AV/AS support chart version for windows	227.0.0.0
Cisco AV/AS support chart version for Mac OSX	148.0.0.0
Cisco supported OS version	49.0.0.0

ステップ 2 : コンプライアンスモジュールをアップロードします。Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動します。Addをクリックし、Agent resources from Cisco siteを選択します



ステップ 3 : [シスコソフトウェアダウンロード](#)からAnyConnectをダウンロードし、ISEにアップロードします。Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動します。

Addをクリックし、Agent Resources From Local Diskを選択します。Categoryの下でCisco Provided Packagesを選択し、ローカルディスクからAnyConnectパッケージを選択して、Submitをクリックします。

Category

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.10...	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secure Mobility Cle...

ステップ 4 : AnyConnectポスチャップロファイルを作成します。Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動します。

Addをクリックし、AnyConnect Posture Profileを選択します。名前とポスチャップロトコルを入力します。

*Server name rulesの下に*を入力し、Discovery hostの下にダミーIPアドレスを入力します。

ISE Posture Agent Profile Settings > AC_Posture_Profile

* Name:

Description:

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	<input style="border: 1px solid red;" type="text" value="1.2.3.4"/>		The server that the agent should connect to
* Server name rules	<input style="border: 1px solid red;" type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List	<input type="text"/>	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPAddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

ステップ 5 : Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動し、AnyConnect Configurationを作成します。Addをクリックし、AnyConnect Configurationを選択します。AnyConnect Packageを選択し、Configuration Nameを指定し、Compliance Moduleを選択し、Diagnostic and Reporting Toolにチェックマークを入れ、Posture Profileを選択してSaveをク

リックします。

* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC CF 47

Description:

DescriptionValue	Notes
* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1012.6	

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC_Posture_Profile

VPN

Network Access Manager

Web Security

AMP Enabler

Network Visibility

Umbrella Roaming Security

Customer Feedback

手順 6 : Policy > Client Provisioningの順に移動し、Client Provisioning Policyを作成します。EditをクリックしてからInsert Rule Aboveを選択し、名前を指定して、OSを選択し、前のステップで作成したAnyConnect Configurationを選択します。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Client Provisioning Policy
 Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AC_47_Win	If Any	and Windows All	and Condition(s)	then AC_CF_47
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.7.00135 And MacOSXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

手順 7 : Policy > Policy Elements > Conditions > Posture > Anti-Malware Conditionでポスチャ条件を作成します。この例では、定義済みの「ANY_am_win_inst」が使用されます。

を参照。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Anti-Malware Conditions

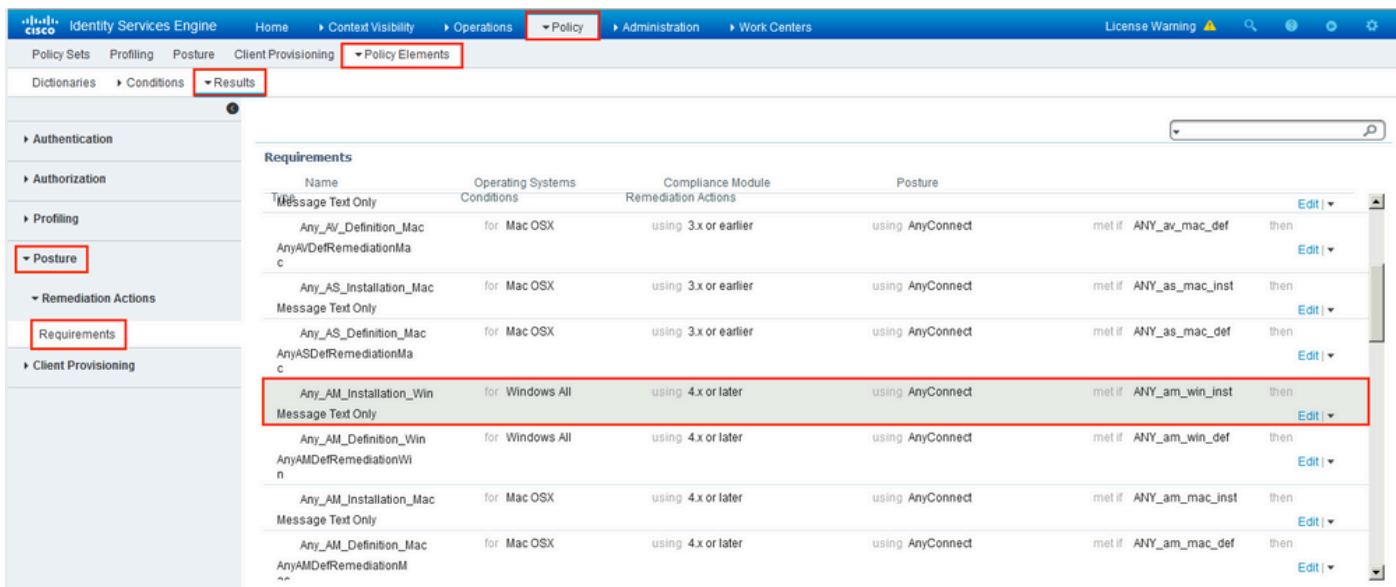
Edit Add Duplicate Delete

Name	Description
ANY_am_win_inst	Any AM installation check on Wi...
ANY_am_win_def	Any AM definition check on Wind...
ANY_am_mac_inst	Any AM installation check on Mac
ANY_am_mac_def	Any AM definition check on Mac

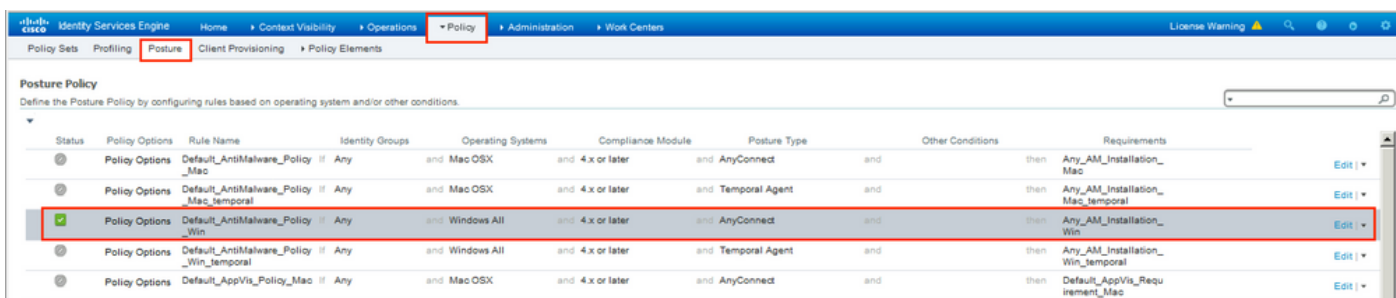
Library Conditions
 Smart Conditions
 Time and Date
 Profiling
 Posture
 Anti-Malware Condition
 Anti-Spyware Condition
 Anti-Virus Condition
 Application Condition
 Compound Condition
 Disk Encryption Condition
 File Condition
 Firewall Condition

ステップ 8 : Policy > Policy Elements > Results > Posture > Remediation Actionsの順に移動し、Posture Remediationを作成します。この例では、これはスキップされます。修復アクションはテキストメッセージにすることができます。

ステップ 9 : Policy > Policy Elements > Results > Posture > Requirementsの順に移動し、Posture Requirementsを作成します。定義済みの要件Any_AM_Installation_Winが使用されます。



ステップ 10 : Policies > Postureでポスチャポリシーを作成します。Windows OSのアンチマルウェアチェックのデフォルトのポスチャポリシーが使用されます。



ステップ 11 Policy > Policy Elements > Results > Authorization > Downloadable ACLSの順に移動し、異なるポスチャステータス用のDAACLを作成します。

この例では、

- ポスチャ不明DAACL:DNS、PSN、およびHTTPとHTTPSのトラフィックを許可します。
- ポスチャ非準拠DAACL：プライベートサブネットへのアクセスを拒否し、インターネットトラフィックのみを許可します。
- Permit All DAACL：ポスチャ準拠ステータスのすべてのトラフィックを許可します。

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic [?](#)

* DACL Content

1234567	permit	udp	any	any	eq	domain
8910111	permit	ip	any	host		192.168.15.14
2131415	permit	tcp	any	any	eq	80
1617181	permit	tcp	any	any	eq	443
9202122						
2324252						
6272829						
3031323						
3343536						
3738394						

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic [?](#)

* DACL Content

1234567	deny	ip	any	10.0.0.0	255.0.0.0	
8910111	deny	ip	any	172.16.0.0	255.240.0.0	
2131415	deny	ip	any	192.168.0.0	255.255.0.0	
1617181	permit	ip	any	any		
9202122						
2324252						
6272829						
3031323						
3343536						
3738394						

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic [?](#)

* DACL Content

123456	permit	ip	any	any		
7891011						
121314						
151617						
181920						
212223						
242526						
272829						
303132						
333435						
363738						

[▶ Check DACL Syntax](#)



3つの認可プロファイルを作成します。これを行うには、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動します。Posture Unknownプロファイルで、Posture Unknown DACLを選択し、Web Redirectionにチェックマークを付け、Client Provisioningを選択し、Redirect ACL名 (FTDで設定) を指定して、ポータルを選択します。

Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ **Common Tasks**

DACL Name

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

 ACL Value

▼ **Attributes Details**

Access Type = ACCESS_ACCEPT
DACL = PostureUnknown
cisco-av-pair = url-redirect-acl=fyusifovredirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp

Posture NonCompliantプロファイルで、ネットワークへのアクセスを制限するためにDACLを選択します。

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PostureNonCompliant

Posture Compliantプロファイルで、ネットワークへのフルアクセスを許可するためにDACLを選択します。

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PermitAll

ステップ 13 Policy > Policy Sets > Default > Authorization Policyで認可ポリシーを作成します。As条件として、Posture StatusとVPN TunnelGroup Nameが使用されます。

The screenshot shows the Cisco ISE Policy configuration interface. The 'Policy' tab is active, and the 'Default' policy set is selected. Under the 'Authorization Policy (18)' section, three rules are configured:

Status	Rule Name	Conditions	Results	Hits	Actions
✔	FTD-VPN-Posture-Compliant	AND Session PostureStatus EQUALS Compliant Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	PermitAll	4	
✔	FTD-VPN-Posture-NonCompliant	AND Session PostureStatus EQUALS NonCompliant Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	FTD-VPN-NonCompliant	0	
✔	FTD-VPN-Posture-Unknown	AND Session PostureStatus EQUALS Unknown Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS EmployeeVPN	FTD-VPN-Redirect	9	

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ISEでは、最初の検証ステップはRADIUSライブログです。Operations > RADIUS Live Logの順に移動します。ここで、ユーザAliceが接続され、期待される認可ポリシーが選択されます。

The screenshot shows the Cisco ISE RADIUS Live Log interface. The 'Live Sessions' tab is active, and a table of session records is displayed. The record for user 'alice@training.e...' is highlighted, showing a status of 'Pending' and a posture status of 'Pending'.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture Sta...
Feb 03, 2020 07:13:31.92...	●		0	alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	172.16.1.10	FTD			Pending
Feb 03, 2020 07:13:29.74...	✔	#ACSACL#IP-P...									FTD			
Feb 03, 2020 07:13:29.73...	✔			alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...		FTD	Workstation		Pending

認可ポリシーFTD-VPN-Posture-Unknownが一致し、その結果、FTD-VPN-ProfileがFTDに送信されます。

Overview

Event 5200 Authentication succeeded

Username alice@training.example.com

Endpoint Id 00:0C:29:5C:5A:96 ⓘ

Endpoint Profile Windows10-Workstation

Authentication Policy Default >> Default

Authorization Policy Default >> FTD-VPN-Posture-Unknown

Authorization Result FTD-VPN-Redirect

Authentication Details

Source Timestamp 2020-02-03 07:13:29.738

Received Timestamp 2020-02-03 07:13:29.738

Policy Server fysisfov-26-3

Event 5200 Authentication succeeded

Username alice@training.example.com

ポストチャステータスは保留中です。

NAS IPv4 Address 192.168.15.15

NAS Port Type Virtual

Authorization Profile FTD-VPN-Redirect

Posture Status Pending

Response Time 365 milliseconds

結果セクションには、FTDに送信される属性が表示されます。

Result

Class	CACS:000000000000c0005e37c81a:fyusifov-26-3/368560500/45
cisco-av-pair	url-redirect-acl=fyusifovredirect
cisco-av-pair	url-redirect=https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=000000000000c0005e37c81a&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp&token=0d90f1cdf40e83039a7ad6a226603112
cisco-av-pair	ACS: CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

FTDで、VPN接続を確認するために、ボックスにSSHで接続し、system support diagnostic-cliを実行してから、show vpn-sessiondb detail anyconnectを実行します。この出力から、ISEから送信された属性がこのVPNセッションに適用されていることを確認します。

```
<#root>
```

```
fyusifov-ftd-64#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : alice@training.example.com
```

```
Index         : 12
```

```
Assigned IP   : 172.16.1.10
```

```
Public IP    : 10.229.16.169
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

```
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
```

```
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
```

```
Bytes Tx     : 15326 Bytes Rx      : 13362
```

```
Pkts Tx      : 10 Pkts Rx       : 49
```

```
Pkts Tx Drop : 0 Pkts Rx Drop  : 0
```

```
Group Policy : DfltGrpPolicy
```

```
Tunnel Group : EmployeeVPN
```

```
Login Time   : 07:13:30 UTC Mon Feb 3 2020
```

```
Duration     : 0h:06m:43s
```

```
Inactivity   : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN           : none
```

```
Audt Sess ID : 000000000000c0005e37c81a
```

```
Security Grp : none Tunnel Zone   : 0
```


AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 12.1
Public IP : 10.229.16.169
Encryption : none Hashing : none
TCP Src Port : 56491 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes
Client OS : win
Client OS Ver: 10.0.18363
Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076

Bytes Tx : 7663 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 12.2
Assigned IP : 172.16.1.10 Public IP : 10.229.16.169
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 56495
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7663 Bytes Rx : 592
Pkts Tx : 5 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

DTLS-Tunnel:

Tunnel ID : 12.3
Assigned IP : 172.16.1.10 Public IP : 10.229.16.169
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 59396
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 0 Bytes Rx : 12770
Pkts Tx : 0 Pkts Rx : 42
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

ISE Posture:

Redirect URL : <https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=00000000000c0005e37c81>
Redirect ACL : fyusifovredirect

fyusifov-ftd-64#

クライアントプロビジョニングポリシーを確認できます。Operations > Reports > Endpoints and Users > Client Provisioningの順に移動します。

Logged At	Server	Event	Identity	Endpoint ID	IP Address	Client Provisioning Pol
2020-02-03 08:08:4...	fysifov-26-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	AC_47_Win

AnyConnectから送信されたポスチャレレポートをチェックできます。Operations > Reports > Endpoints and Users > Posture Assessment by Endpointの順に移動します。

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS
2020-02-03 08:07:5...	✓	🔍	N/A	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	Windows 10 Professional

ポスチャレレポートの詳細を表示するには、Detailsをクリックします。

Client Details	Value
Username	alice@training.example.com
Mac Address	00:0C:29:5C:5A:96
IP address	172.16.1.10
Location	All Locations
Session ID	0000000000c0005e37c81a
Client Operating System	Windows 10 Professional 64-bit
Client NAC Agent	AnyConnect Posture Agent for Windows 4.7.01076
PRA Enforcement	0
CoA	Received a posture report from an endpoint
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEnabled
System Name	DESKTOP-IE3566M
System Domain	n/a

ISEでレポートを受信すると、ポスチャステータスが更新されます。この例では、ポスチャステータスは準拠しており、CoAプッシュは新しい属性セットでトリガーされます。

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture
Feb 03, 2020 08:07:52.05...	✓	🔍			10.229.16.169				PermitAccess		FTD			Complia
Feb 03, 2020 08:07:50.03...	ⓘ	🔍	0	alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...	172.16.1.10				Complia
Feb 03, 2020 07:13:29.74...	✓	🔍		#ACSACL#IP-P...							FTD			
Feb 03, 2020 07:13:29.73...	✓	🔍		alice@training.e...	00:0C:29:5C:5A:96	Windows10...	Default >> ...	Default >> ...	FTD-VPN-R...		FTD		Workstation	Pending

Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Standard Time)

Records Shown: 4

Overview

Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	10.55.218.19 ⓘ
Endpoint Profile	
Authorization Result	PermitAll

Authentication Details

Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fysifov-26-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	000000000000e0005e385132
Network Device	FTD
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.15.15
Authorization Profile	PermitAll
Posture Status	Compliant
Response Time	2 milliseconds

Other Attributes

ConfigVersionId	21
Event-Timestamp	1580749119
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	af49ce55-d55c-4778-ad40-b03ea12924d2
CoASourceComponent	Posture
CoAReason	posture status changed
CoAType	COA-push
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Device IP Address	192.168.15.15
CiscoAVPair	audit-session-id=000000000000e0005e385132, coa-push=true, ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PermitAll-5e384dc0

FTDで、VPNセッション用の新しいリダイレクトACLとリダイレクトURLが削除され、PermitAll DACLが適用されていることを確認します。

```
<#root>
```

```
fyusifov-ftd-64#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      :
```

```
alice@training.example.com
```

```
Index         : 14
```

```
Assigned IP   : 172.16.1.10      Public IP     : 10.55.218.19
```

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 53990 Bytes Rx : 23808
Pkts Tx : 73 Pkts Rx : 120
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

EmployeeVPN

Login Time : 16:58:26 UTC Mon Feb 3 2020
Duration : 0h:02m:24s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000000e0005e385132
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 14.1
Public IP : 10.55.218.19
Encryption : none Hashing : none
TCP Src Port : 51965 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : win
Client OS Ver: 10.0.18363
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7663 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 14.2
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 51970
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 7715 Bytes Rx : 10157
Pkts Tx : 6 Pkts Rx : 33
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PermitAll-5e384dc0

DTLS-Tunnel:

Tunnel ID : 14.3
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19
Encryption : AES256 Hashing : SHA1
Ciphersuite : DHE-RSA-AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 51536
UDP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076
Bytes Tx : 38612 Bytes Rx : 13651
Pkts Tx : 62 Pkts Rx : 87
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PermitAll-5e384dc0

fyusifov-ftd-64#

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ポスチャフローの詳細と、AnyConnectおよびISEのトラブルシューティングについては、次のリンクを確認してください。 [ISE ポスチャスタイルの 2.2 前後の比較](#)。

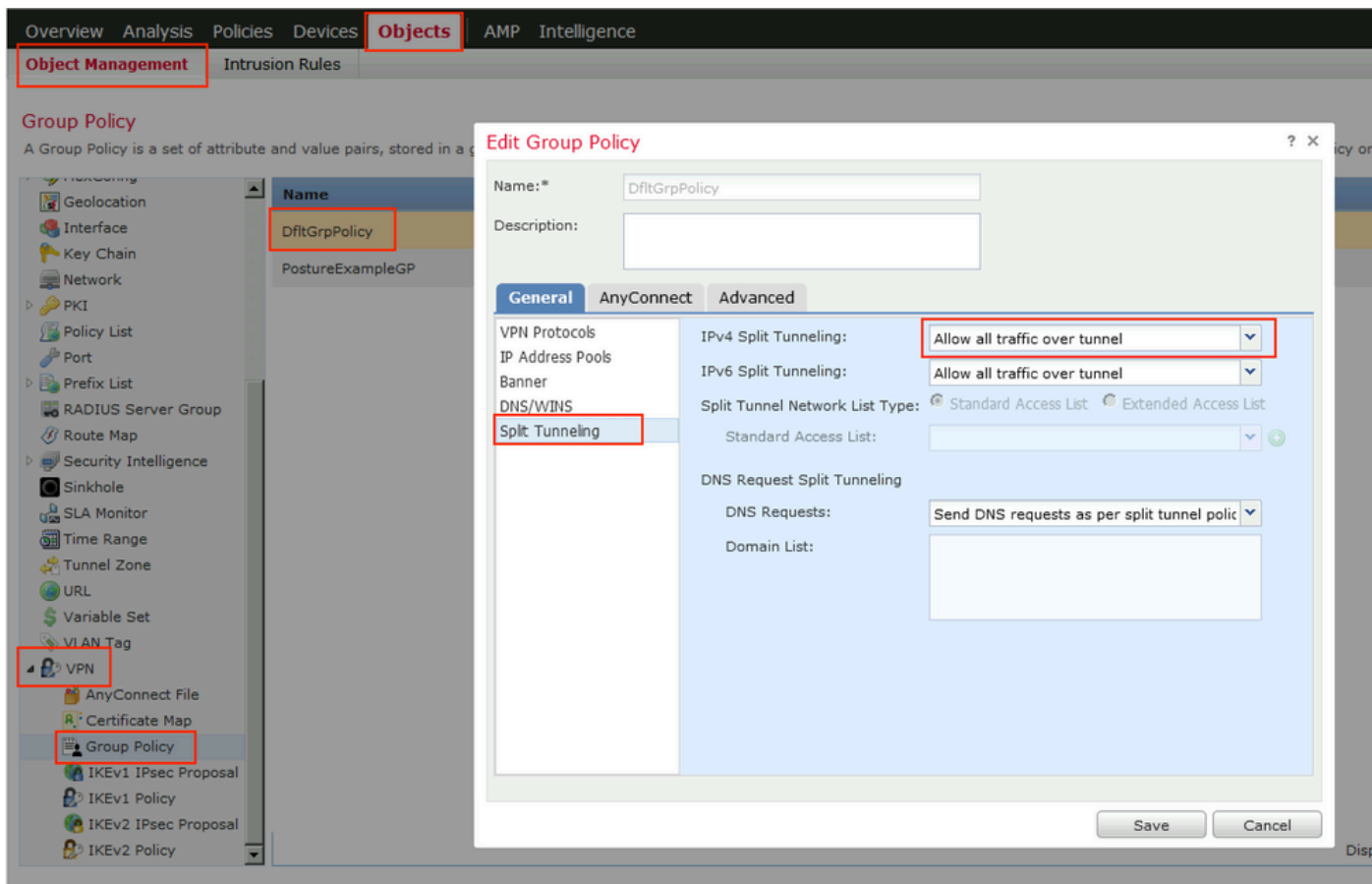
- こぼれたトンネル

スプリットトンネルが設定されている場合の一般的な問題の1つです。この例では、すべてのトラフィックをトンネリングするデフォルトのグループポリシーが使用されます。特定のトラフィックだけがトンネル化される場合は、ISEおよびその他の内部リソースへのトラフィックに加えて、AnyConnectプロンプト(enroll.cisco.comおよび検出ホスト)もトンネルを通過する必要があります。

FMCのトンネルポリシーを確認するには、まず、VPN接続に使用されているグループポリシーを確認します。Devices > VPN Remote Accessの順に移動します。

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
EmployeeVPN	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: ISE (RADIUS)	DfltGrpPolicy

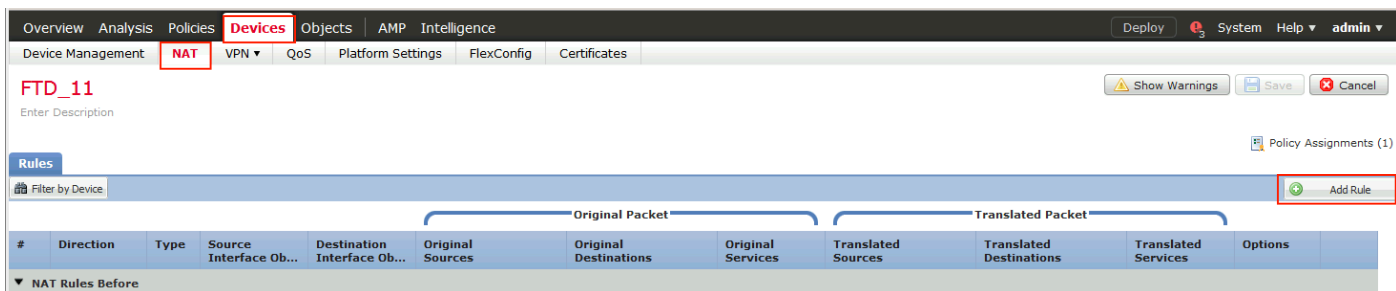
次に、Objects > Object Management > VPN > Group Policyの順に移動し、VPN用に設定されたGroup Policyをクリックします。



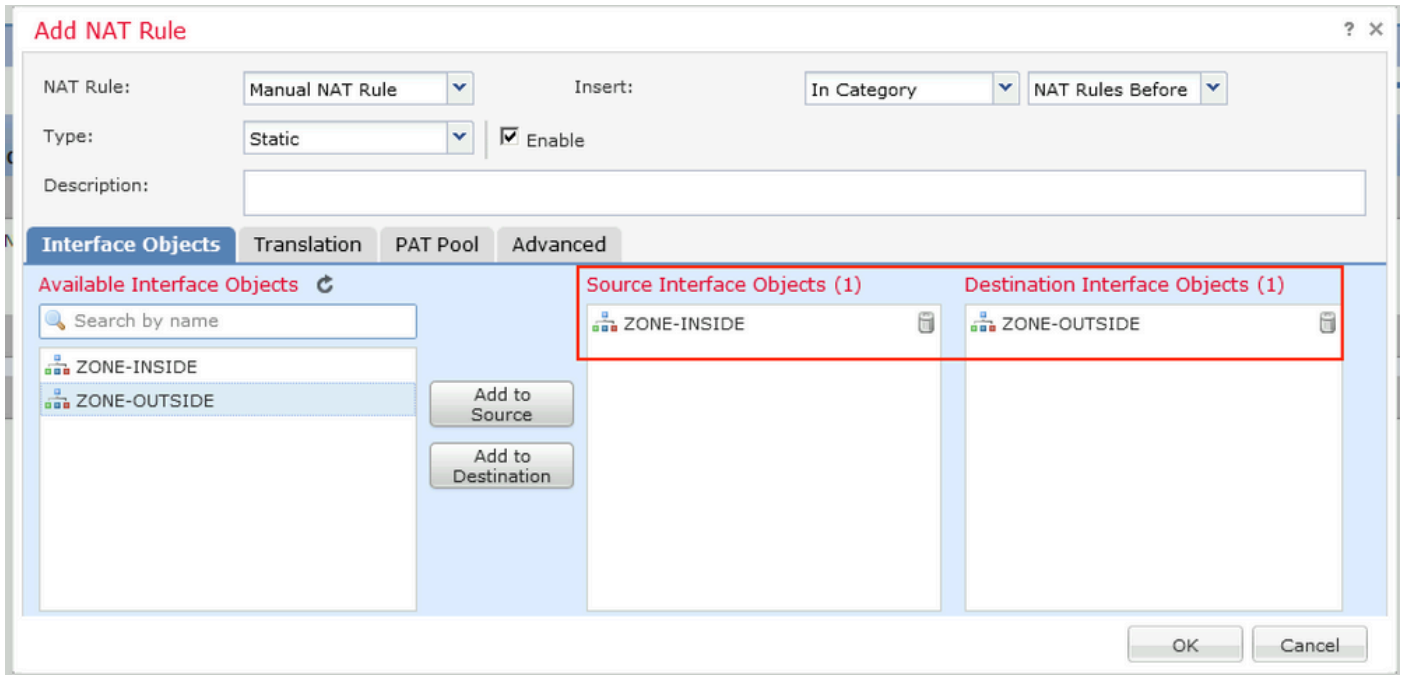
- アイデンティティ NAT

もう1つの一般的な問題は、VPNユーザのリターントラフィックが誤ったNATエントリを使用して変換されることです。この問題を解決するには、アイデンティティ NATを適切な順序で作成する必要があります。

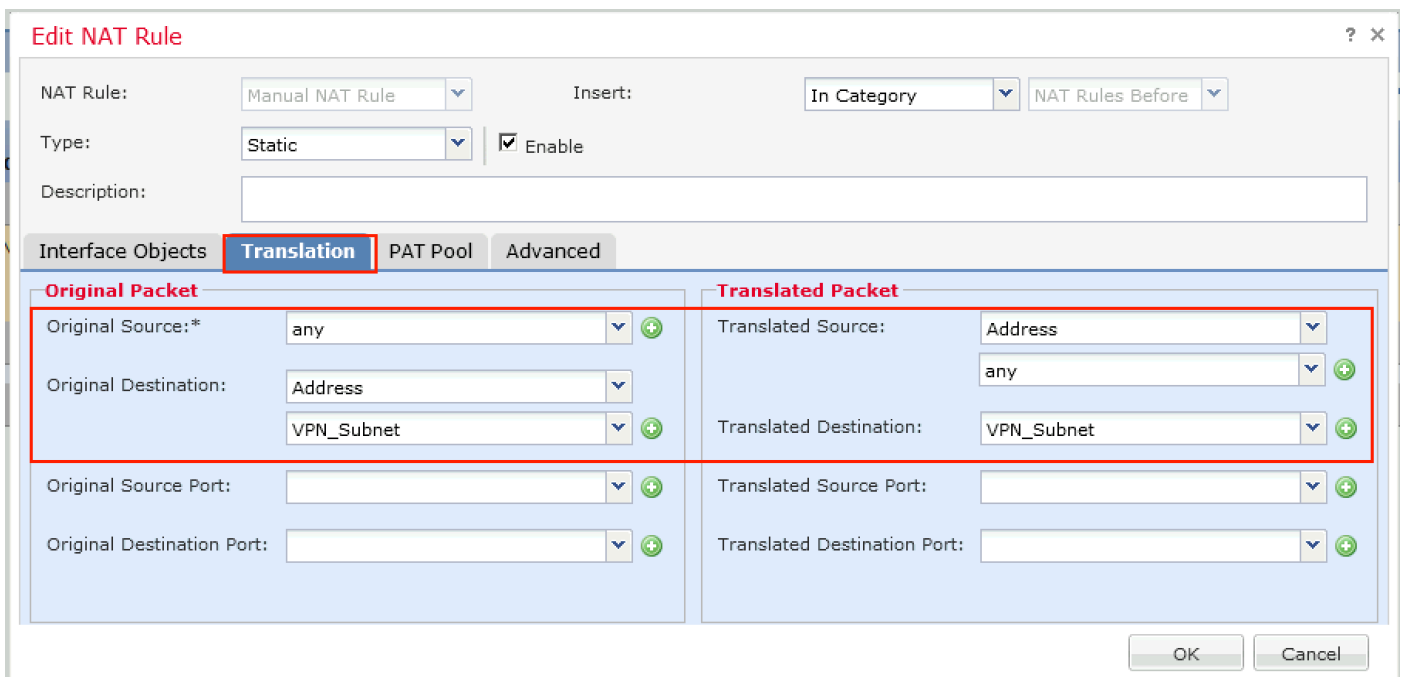
最初に、このデバイスのNATルールを確認します。Devices > NATの順に移動し、Add Ruleをクリックして新しいルールを作成します。



開いているウィンドウのInterface Objectsタブで、Security Zonesを選択します。この例では、NATエントリはZONE-INSIDEからZONE-OUTSIDEに作成されます。



Translationタブで、元の packets と変換された packets の詳細を選択します。アイデンティティ NAT であるため、送信元と宛先は変更されません。



Advancedタブで、次の図に示すようにチェックボックスをオンにします。

Edit NAT Rule

? X

NAT Rule:

Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination Interface
- Unidirectional

OK

Cancel

翻訳について

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