

Configurazione della postura ISE sulla VPN ad accesso remoto AnyConnect su FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete e flusso del traffico](#)

[Configurazioni](#)

[FTD/FMC](#)

[ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive come configurare Firepower Threat Defense (FTD) versione 6.4.0 per posturare gli utenti VPN contro Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AnyConnect VPN ad accesso remoto
- Configurazione VPN di accesso remoto nell'FTD
- Servizi Identity Services Engine e servizi di postura

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

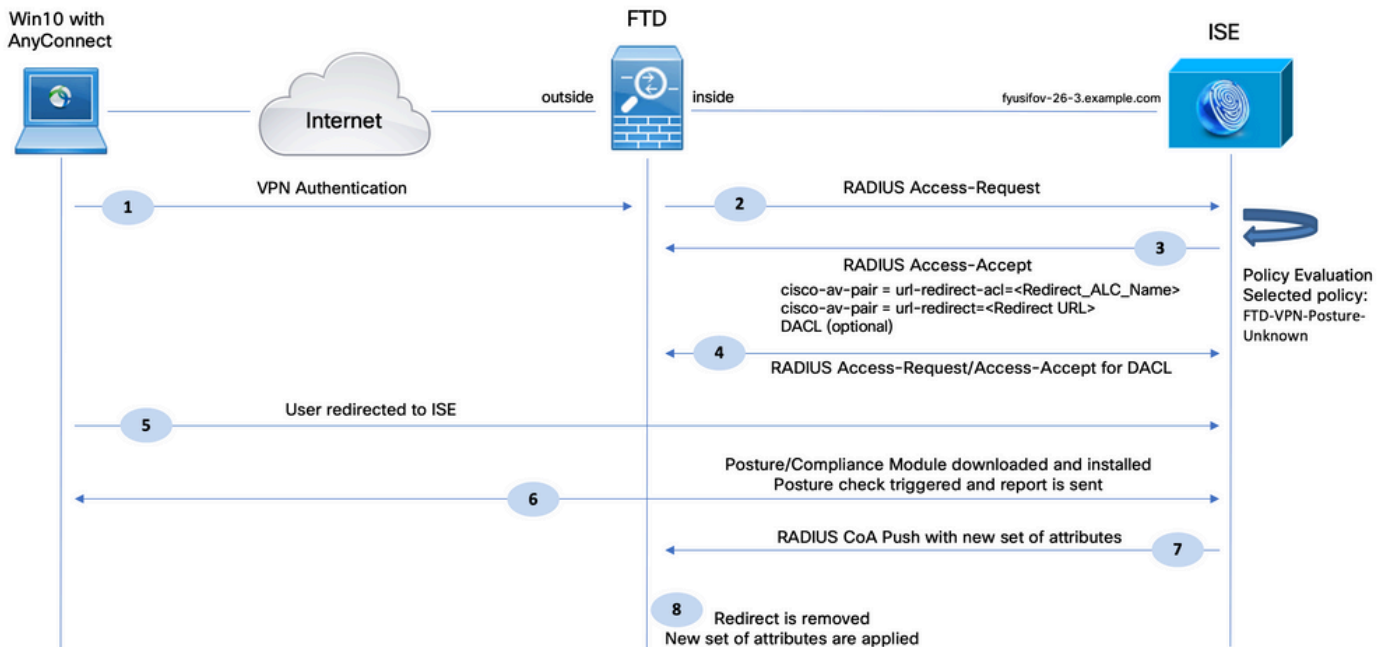
- Software Cisco Firepower Threat Defense (FTD) versioni 6.4.0
- Software Cisco Firepower Management Console (FMC) versione 6.5.0
- Microsoft Windows 10 con Cisco AnyConnect Secure Mobility Client versione 4.7
- Cisco Identity Services Engine (ISE) versione 2.6 con patch 3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete e flusso del traffico



1. L'utente remoto usa Cisco Anyconnect per l'accesso VPN al FTD.

2. L'FTD invia all'ISE una richiesta di accesso RADIUS per tale utente.

3. Tale richiesta è conforme alla policy denominata FTD-VPN-Posture-Unknown sull'ISE. L'ISE invia un messaggio di accesso RADIUS-Accept con tre attributi:

- cisco-av-pair = url-redirect-acl=fyusifovredirect - È il nome dell'elenco di controllo di accesso (ACL) definito localmente sull'FTD, che decide il traffico che viene reindirizzato.
- cisco-av-pair = url-redirect=<https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp> - URL a cui viene reindirizzato l'utente remoto.
- DACL = PERMIT_ALL_IPV4_TRAFFIC - ACL scaricabile. Questo attributo è facoltativo. In questo scenario, tutto il traffico è consentito in DACL)

4. Se viene inviato un DACL, viene scambiato un accesso RADIUS con richiesta/accettazione dell'accesso per scaricare il contenuto del DACL

5. Quando il traffico proveniente dall'utente VPN corrisponde all'ACL definito localmente, viene reindirizzato al portale di provisioning del client ISE. ISE fornisce AnyConnect Posture Module e Compliance Module.

6. Una volta installato sul computer client, l'agente cerca automaticamente l'ISE con le sonde. Quando ISE viene rilevato correttamente, i requisiti di postura vengono controllati sull'endpoint. In questo esempio, l'agente verifica la presenza di software antimalware installato. Infine, invia un report sulla postura all'ISE.

7. Quando ISE riceve il report sulla postura dall'agente, cambia lo stato della postura per questa sessione e attiva il Push del tipo CoA RADIUS con i nuovi attributi. Questa volta, lo stato della postura è noto e viene trovata un'altra regola.

- Se l'utente è conforme, viene inviato un nome DACL che consente l'accesso completo.
- Se l'utente non è conforme, viene inviato un nome DACL che consente l'accesso limitato.

8. L'FTD rimuove il reindirizzamento. L'FTD invia una richiesta di accesso per scaricare il DACL dall'ISE. Il DACL specifico viene collegato alla sessione VPN.

Configurazioni

FTD/FMC

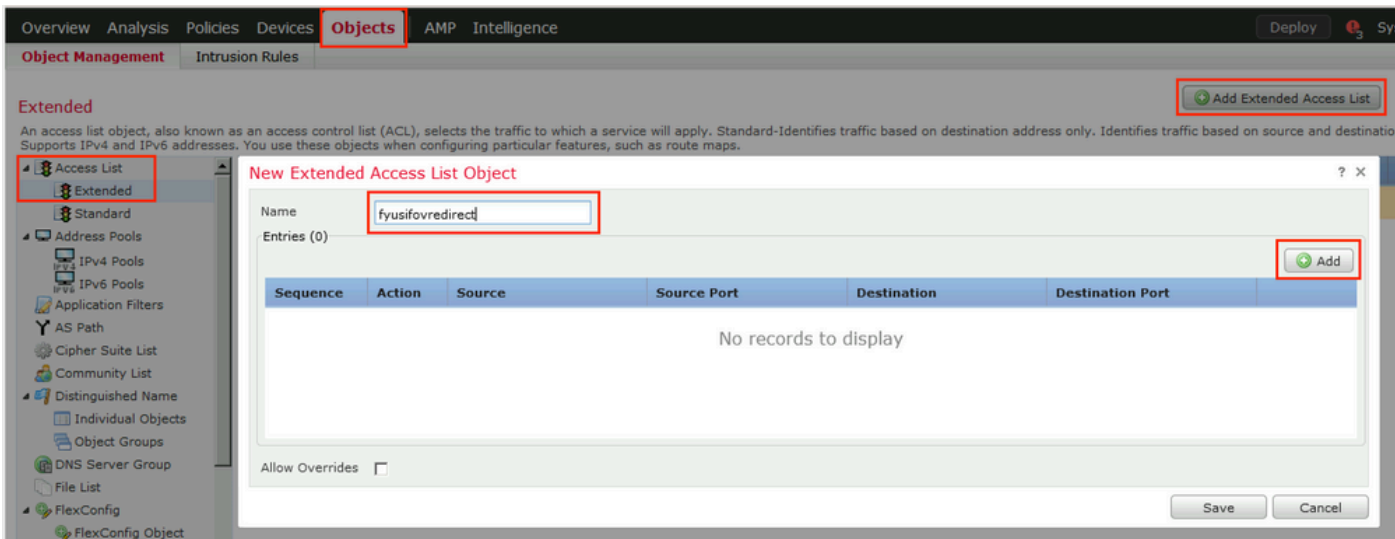
Passaggio 1. Creare un Network Object Group per ISE e gli eventuali server di monitoraggio e aggiornamento. Passare a Oggetti > Gestione oggetti > Rete.

The screenshot shows the Cisco FTD/FMC configuration interface. The 'Objects' tab is selected, and the 'Network' section is visible. A dialog box titled 'Edit Network Object' is open, showing the configuration for a new network object. The 'Name' field is set to 'ISE_PSN', and the 'Network' field is set to '192.168.15.14' with the 'Host' radio button selected. The 'Allow Overrides' checkbox is unchecked. The background shows a table of existing network objects.

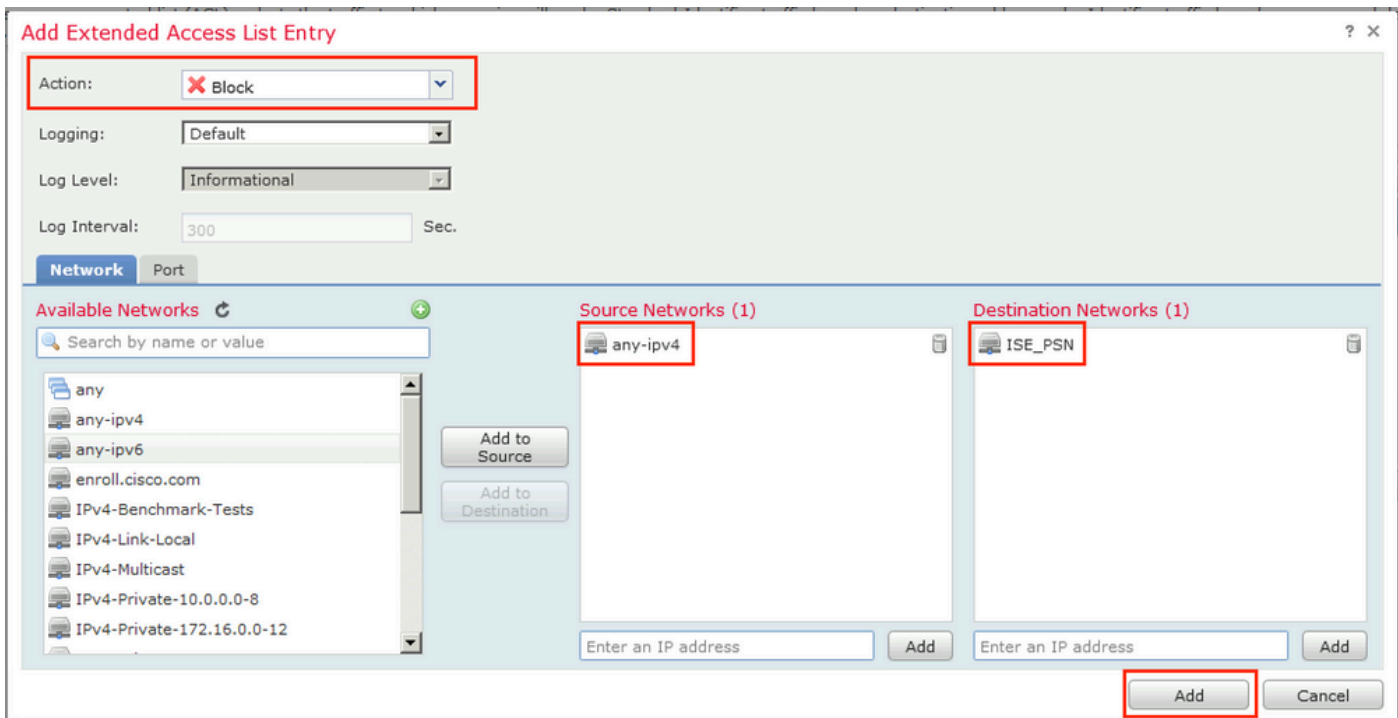
Name	Value
any-ipv4	0.0.0.0/0
any-ipv6	::/0
enroll.cisco.com	72.163.1.80
IPV4-Benchmark-Tests	
IPV4-Link-Local	
IPV4-Multicast	
IPV4-Private-10.0.0.0-8	
IPV4-Private-172.16.0.0-12	
IPV4-Private-192.168.0.0-16	
IPV4-Private-All-RFC1918	
IPV6-IPV4-Mapped	::ffff:0.0.0.0/96
IPV6-Link-Local	fe80::/10
IPV6-Private-Unique-Local-Addresses	fc00::/7
IPV6-to-IPV4-Relay-Anycast	192.88.99.0/24

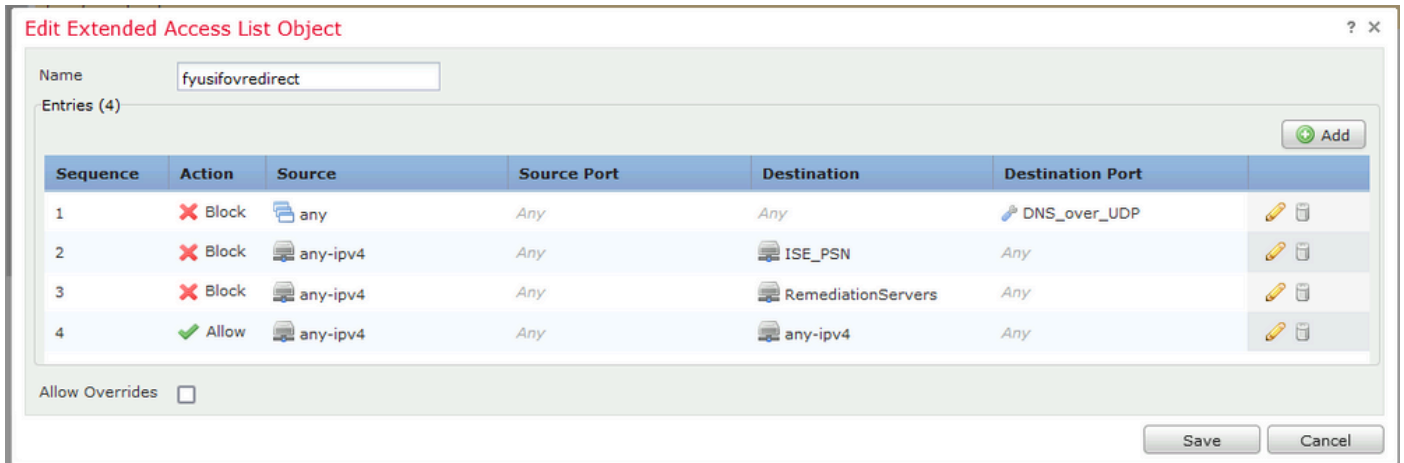
Passaggio 2. Creare un ACL di reindirizzamento. Passare a Oggetti > Gestione oggetti > Elenco accessi > Estesi. Fare clic su Add Extended Access List (Aggiungi elenco accessi esteso) e fornire il nome dell'ACL di reindirizzamento. Questo nome deve coincidere esattamente con quello

restituito dal risultato dell'autorizzazione ISE.



Passaggio 3. Aggiungere voci ACL di reindirizzamento. Fare clic sul pulsante Aggiungi. Bloccare il traffico verso DNS, ISE e verso i server di monitoraggio e aggiornamento per escluderli dal reindirizzamento. Consentire il resto del traffico. Ciò attiva il reindirizzamento (le voci ACL potrebbero essere più specifiche se necessarie).





Passaggio 4. Aggiungere uno o più nodi ISE PSN. Passare a Oggetti > Gestione oggetti > Gruppo server RADIUS. Fare clic su Aggiungi gruppo di server RADIUS, quindi specificare il nome, abilitare e selezionare tutte le caselle di controllo, quindi fare clic sull'icona più.

Edit RADIUS Server Group

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

Passaggio 5. Nella finestra aperta, fornire ISE PSN IP address, RADIUS Key, selezionare Specific Interface (Interfaccia specifica) e selezionare l'interfaccia da cui ISE è raggiungibile (l'interfaccia viene utilizzata come origine del traffico RADIUS), quindi selezionare Redirect ACL, configurato in precedenza.

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

+

Redirect ACL: +

Passaggio 6. Crea pool di indirizzi per utenti VPN. Selezionare Oggetti > Gestione oggetti > Pool di indirizzi > Pool IPv4. Fare clic su Add IPv4 Pools (Aggiungi pool IPv4) e immettere i dettagli.

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

Object Management Intrusion Rules + Add IPv4 Pools

IPv4 Pools IPv4 Pools

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

Name	Value
VPN-172-Pool	172.16.1.10-172.16.1.20

Edit IPv4 Pool

Name*

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

Mask

Description

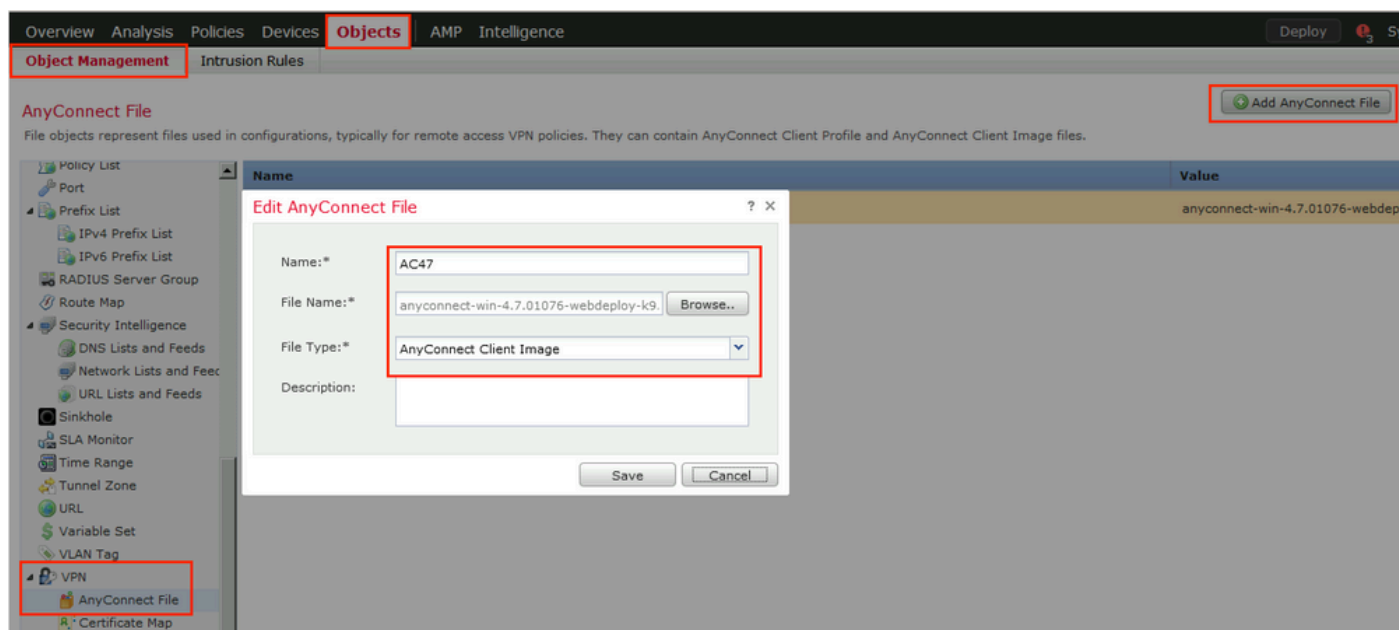
Allow Overrides

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

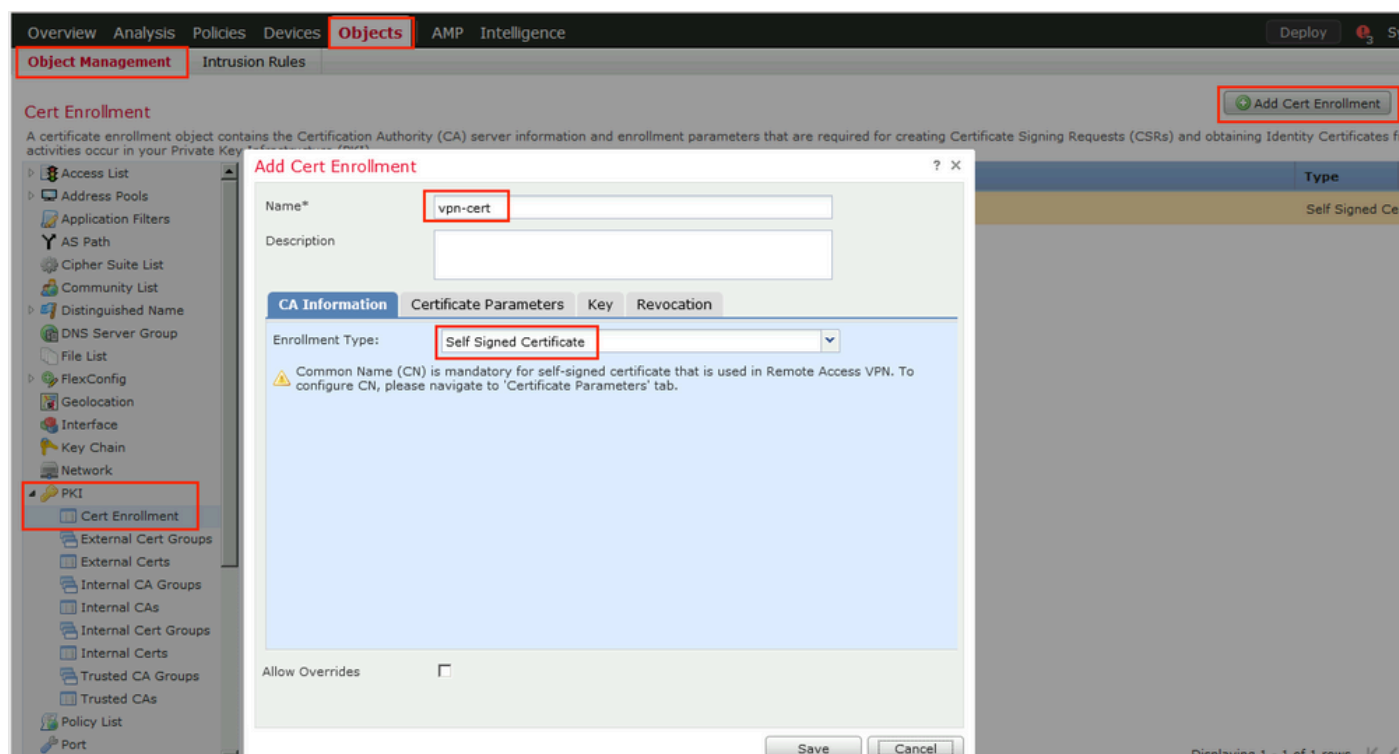
Override (0)

Passaggio 7. Creare il pacchetto AnyConnect. Selezionare Oggetti > Gestione oggetti > VPN > File AnyConnect. Fare clic su Add AnyConnect File (Aggiungi file AnyConnect), fornire il nome del

pacchetto, scaricare il pacchetto da [Cisco Software Download](#) e selezionare Anyconnect Client Image File Type (Tipo di file immagine client Anyconnect).



Passaggio 8. Passare a Oggetti certificato > Gestione oggetti > Infrastruttura a chiave pubblica > Registrazione certificato. Fare clic su Aggiungi registrazione certificato, fornire il nome, scegliere Certificato autofirmato in Tipo di registrazione. Fare clic sulla scheda Parametri certificato e specificare CN.



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):

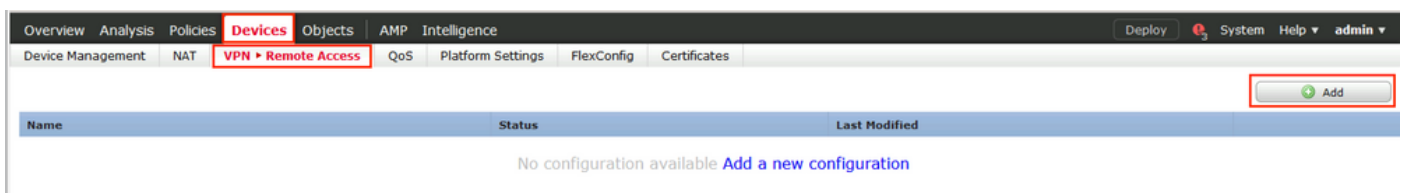
Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

Passaggio 9. Avvia la procedura guidata VPN di Accesso remoto. Selezionare Dispositivi > VPN > Accesso remoto e fare clic su Aggiungi.



Passaggio 10. Fornire il nome, selezionare SSL come protocollo VPN, scegliere FTD che viene utilizzato come concentratore VPN e fare clic su Avanti.

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

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

Passaggio 11. Specificare il nome del profilo di connessione, selezionare Server di autenticazione/accounting, selezionare il pool di indirizzi configurato in precedenza e fare clic su Avanti.

 Nota: non selezionare il server di autorizzazione. e attiva due richieste di accesso per un singolo utente (una volta con la password dell'utente e la seconda volta con la password 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 & 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 Server:* (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:

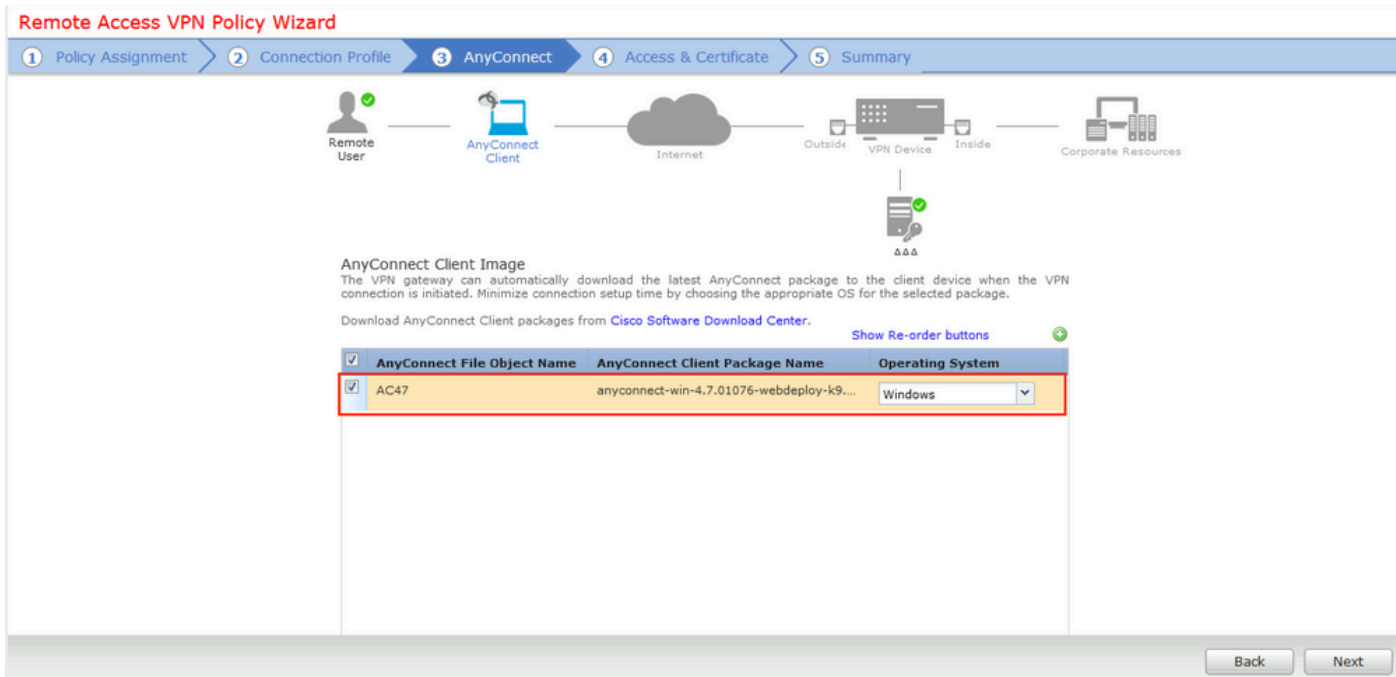
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* ⓘ

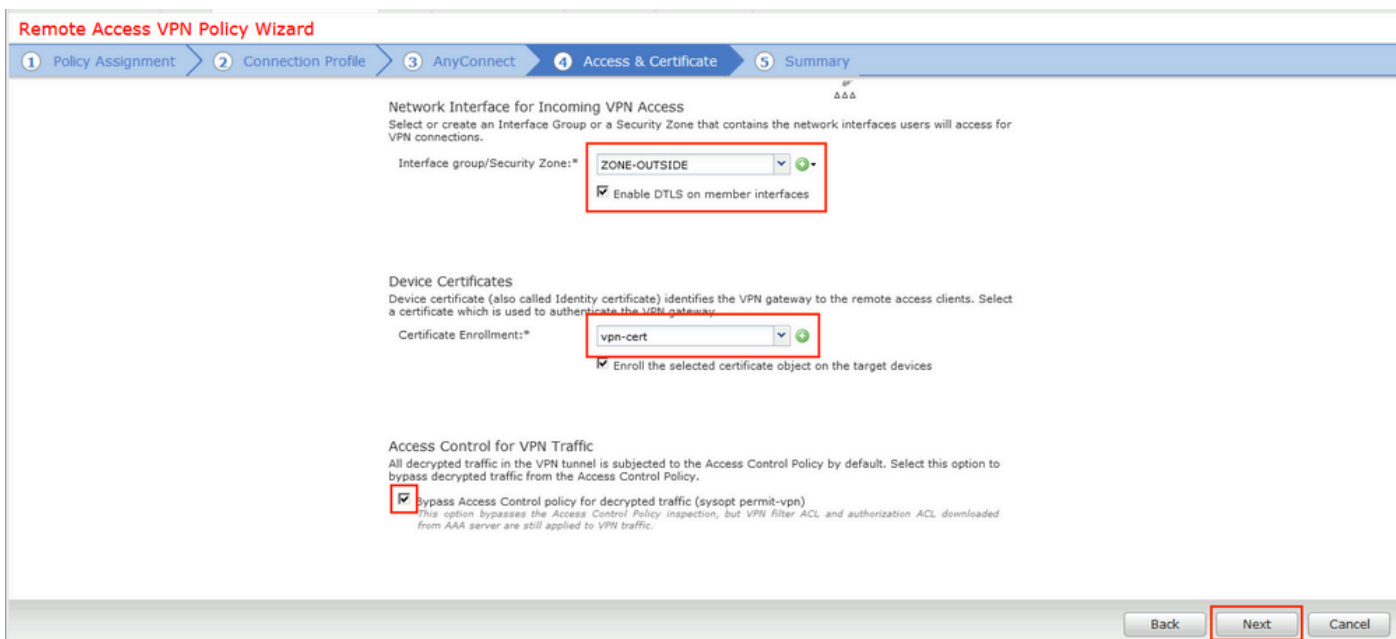
[Edit Group Policy](#)

Back Next Cancel

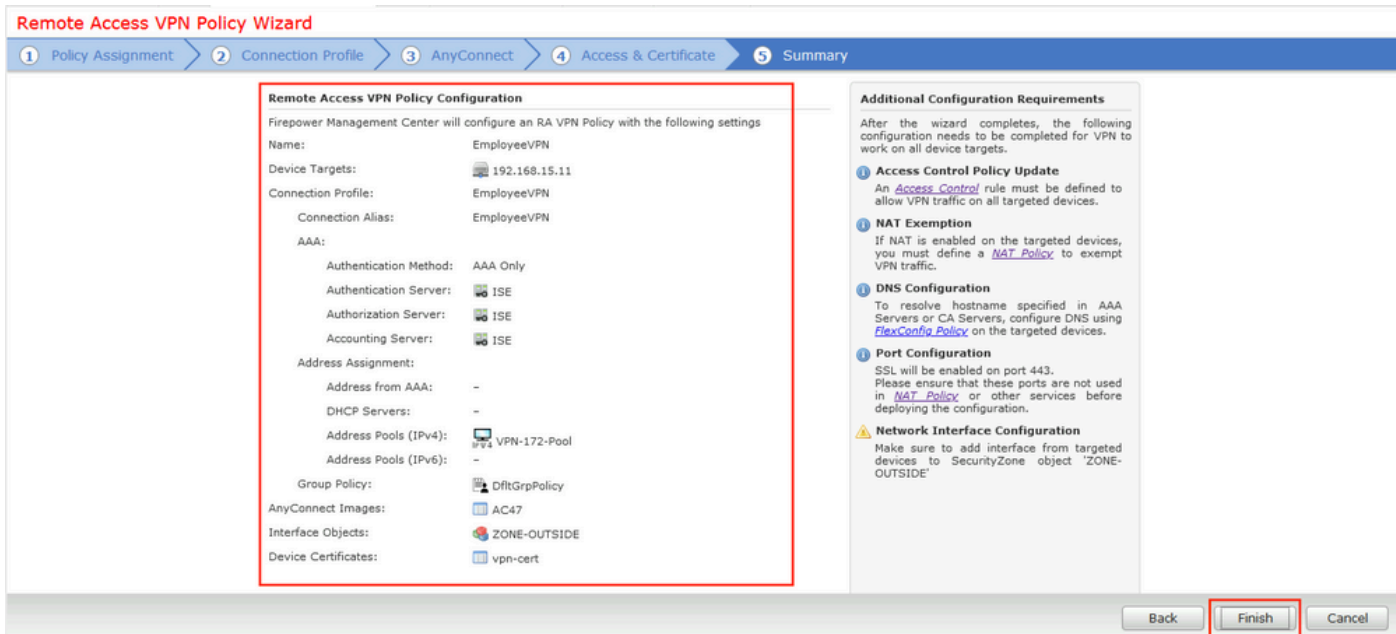
Passaggio 12. Selezionare il pacchetto AnyConnect configurato in precedenza e fare clic su Avanti.



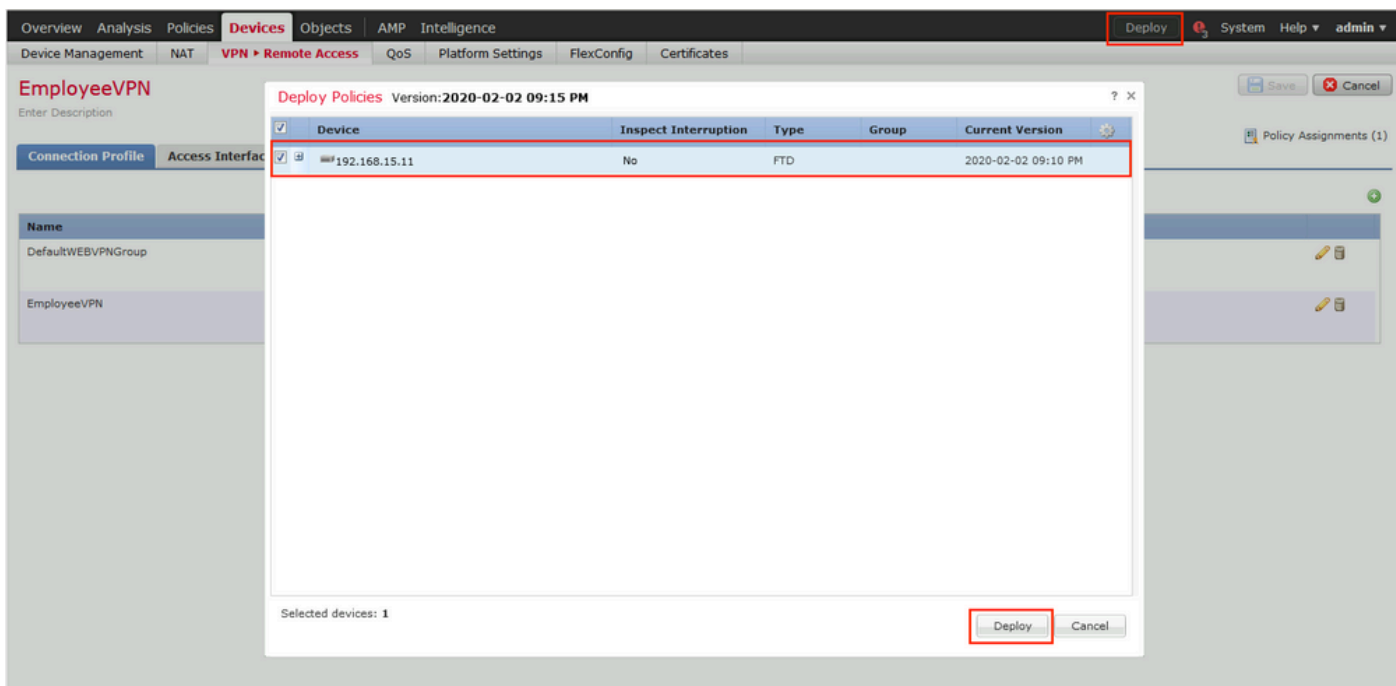
Passaggio 13. Selezionare l'interfaccia da cui è previsto il traffico VPN, selezionare Registrazione certificato configurata in precedenza e fare clic su Avanti.



Passaggio 14. Controllare la pagina di riepilogo e fare clic su Fine.



Passaggio 15. Distribuire la configurazione nel file FTD. Fare clic su Deploy (Distribuisce) e selezionare FTD (FTD) da utilizzare come concentratore VPN.



ISE

Passaggio 1. Eseguire Aggiornamenti Postura. Passare ad Amministrazione > Sistema > Impostazioni > Postura > Aggiornamenti.

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

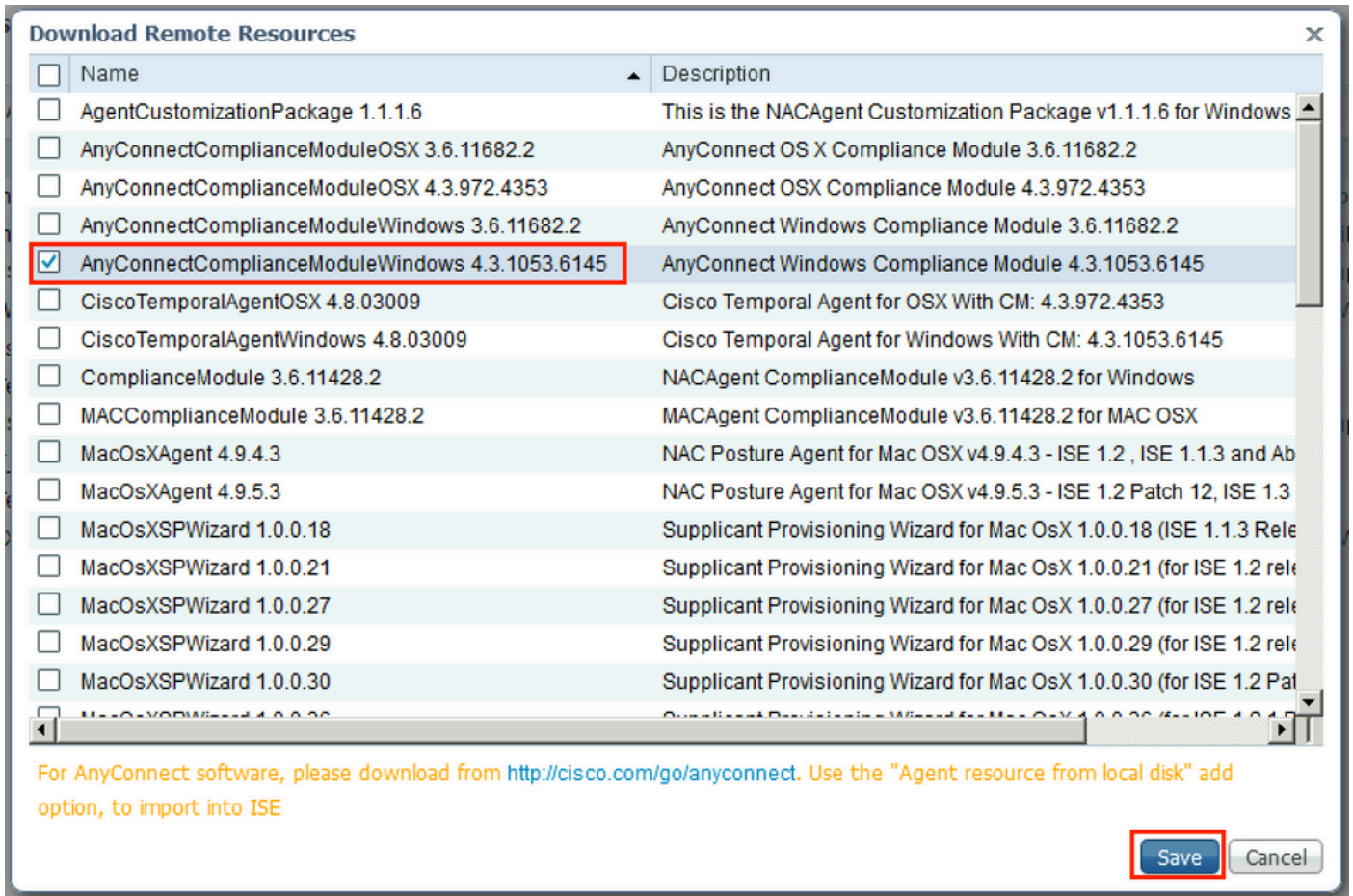
Proxy Port HH MM SS

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

Passaggio 2. Carica il modulo di conformità. Passare a Criteri > Elementi criteri > Risultati > Provisioning client > Risorse. Fare clic su Add (Aggiungi) e selezionare le risorse agente dal sito Cisco



Passaggio 3. Scarica AnyConnect da [Cisco Software Download](http://cisco.com/go/anyconnect), quindi caricalo in ISE. Passare a Criteri > Elementi criteri > Risultati > Provisioning client > Risorse.

Fare clic su Add (Aggiungi) e selezionare Agent Resources From Local Disk. Selezionare Cisco Provided Packages in Category, selezionare AnyConnect package dal disco locale e fare clic su Submit.

Agent Resources From Local Disk > Agent Resources From Local Disk
Agent Resources From Local Disk

Category

▼ AnyConnect Uploaded Resources

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

Submit Cancel

Passaggio 4. Creare un profilo AnyConnect Posture. Passare a Criteri > Elementi criteri > Risultati > Provisioning client > Risorse.

Fare clic su Add (Aggiungi) e selezionare AnyConnect Posture Profile. Inserire il nome e il protocollo di postura.

In *Le regole per i nomi dei server inseriscono * e inseriscono qualsiasi indirizzo IP fittizio in Discovery host.

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 type="text" value="1.2.3.4"/>		The server that the agent should connect to
* Server name rules	<input 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

Passaggio 5. Selezionare Policy > Policy Elements > Results > Client Provisioning > Resources e creare la configurazione AnyConnect. Fare clic su Add (Aggiungi), quindi selezionare AnyConnect Configuration (Configurazione AnyConnect). Selezionare AnyConnect Package, fornire il nome della configurazione, selezionare Compliance Module, selezionare Diagnostic and Reporting Tool, selezionare Posture Profile e fare clic su Save.

* 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

Passaggio 6. Selezionare Policy > Client Provisioning e creare Client Provisioning Policy. Fare clic su Edit, quindi selezionare Insert Rule Above, specificare il nome, selezionare OS, quindi selezionare AnyConnect Configuration (Configurazione di AnyConnect) creata nel passaggio precedente.

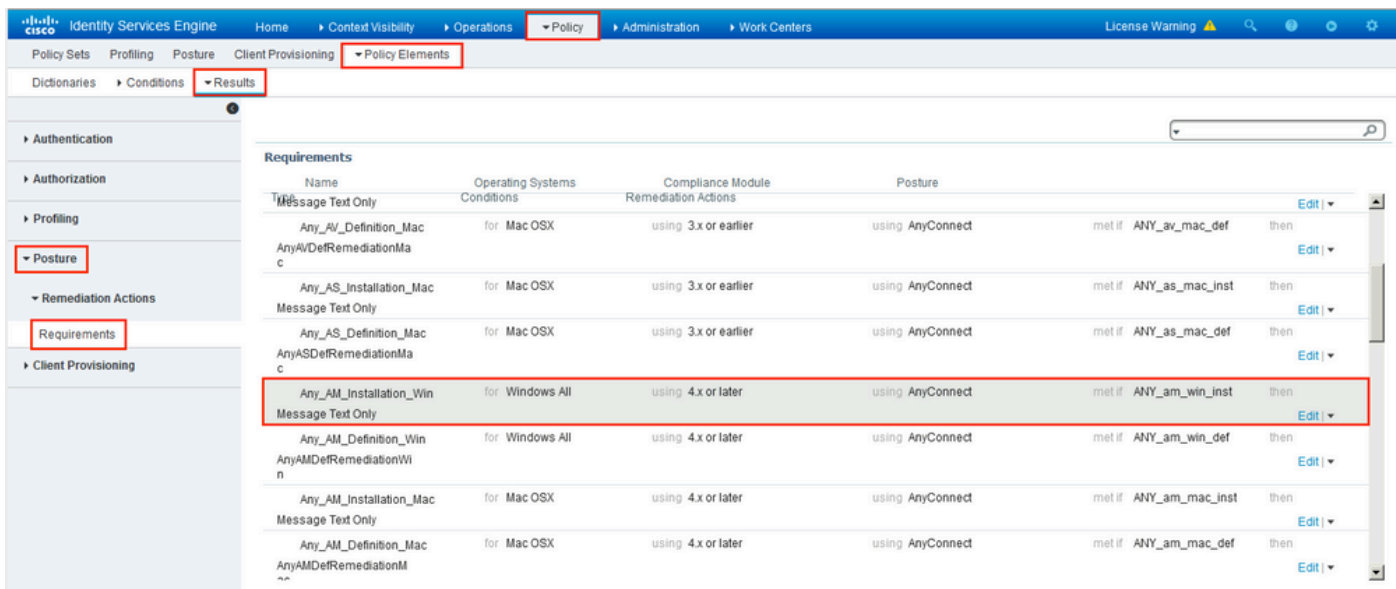
Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AC_47_Win	If Any	and Windows All	and Condition(s)	then AC_CF_47
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	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

Passaggio 7. Crea condizione di postura in Criteri > Elementi criteri > Condizioni > Postura > Condizione antimalware. Nell'esempio viene utilizzato il valore predefinito "ANY_am_win_inst".

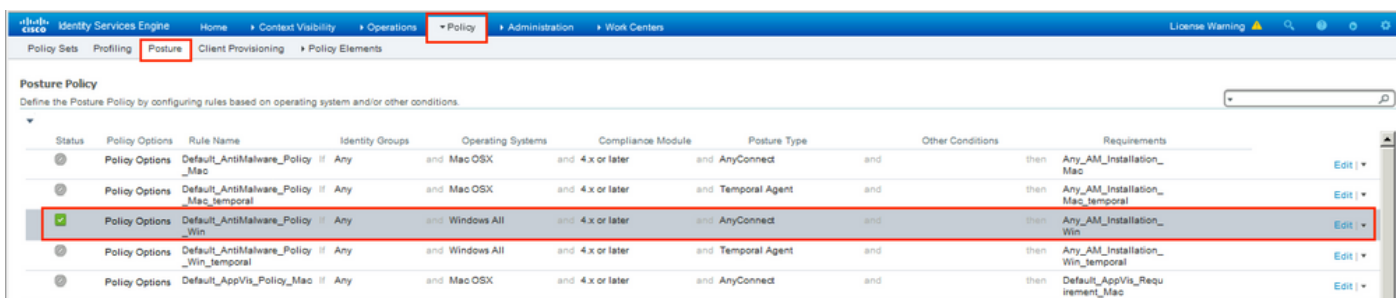
Name	Description
ANY_am_win_inst	Any AM installation check on Wi...
ANY_am_win_def	Any AM definition check on Wind...
ANY_am_mac_inst	Any AM installation check on Mac
ANY_am_mac_def	Any AM definition check on Mac

Passaggio 8. Passare a Criterio > Elementi criteri > Risultati > Postura > Azioni di correzione e creare la correzione della postura. In questo esempio viene ignorato. L'azione di risoluzione può essere un SMS.

Passaggio 9. Passare a Criterio > Elementi criteri > Risultati > Postura > Fabbisogni e creare Fabbisogni postura. Si utilizza il requisito predefinito Any_AM_Installation_Win.



Passaggio 10. Creare i criteri di postura in Criteri > Postura. Viene utilizzato il criterio di postura predefinito per qualsiasi controllo antimalware per il sistema operativo Windows.



Passaggio 11. Passare a Policy > Policy Elements > Results > Authorization > Downloadable ACLS (Criteri > Elementi criteri > Risultati > Autorizzazione > ACL scaricabili) e creare DACL per stati di postura diversi.

In questo esempio:

- DACL con postura sconosciuta: consente il traffico verso DNS, PSN e HTTP e HTTPS.
- DACL postura non conforme - nega l'accesso alle subnet private e consente solo il traffico Internet.
- Permit All DACL - consente tutto il traffico per lo stato di conformità alla postura.

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



conforme e non conforme. A tale scopo, selezionare Criteri > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione. Nel profilo Postura sconosciuta, selezionare DACL postura sconosciuta, selezionare Reindirizzamento Web, selezionare Provisioning client, fornire il nome ACL di reindirizzamento (configurato su FTD) e selezionare il portale.

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

Nel profilo Postura non conforme, selezionare DACL per limitare l'accesso alla rete.

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

Nel profilo Posture Compliant, selezionare DACL per consentire l'accesso completo alla rete.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

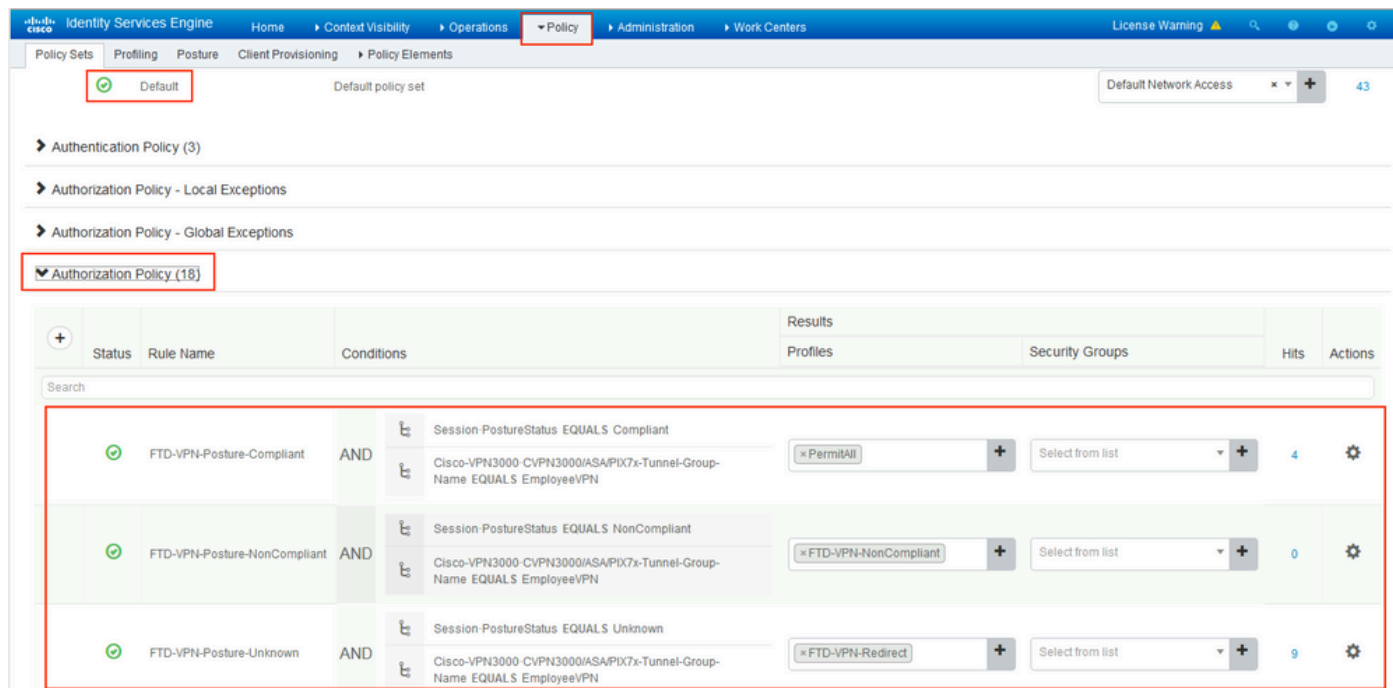
Common Tasks

DACL Name

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PermitAll

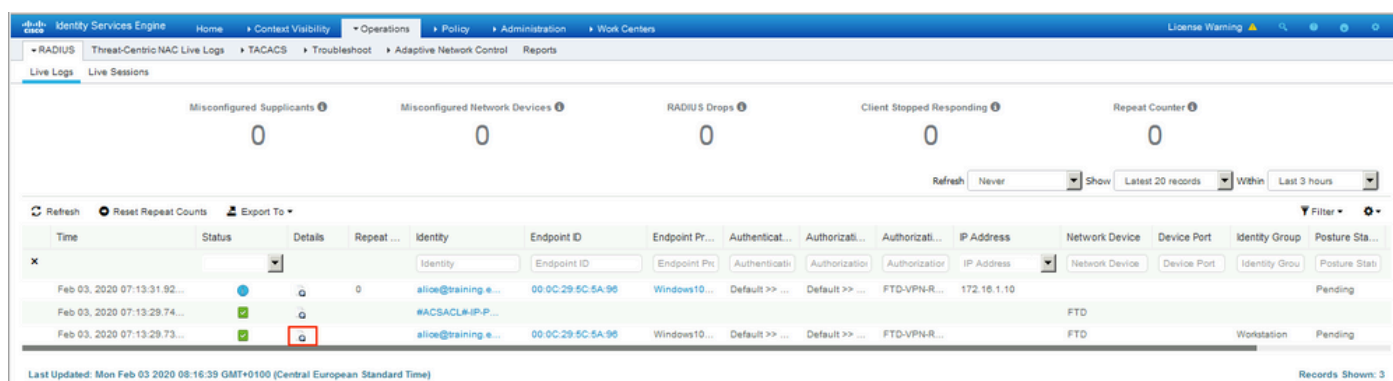
Passaggio 13. Creare i criteri di autorizzazione in Criterio > Set di criteri > Predefinito > Criterio di autorizzazione. Poiché vengono utilizzati lo stato della postura della condizione e il nome del gruppo di tunnel VPN,



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Ad ISE, il primo passaggio della verifica è RADIUS Live Log. Passare a Operazioni > Registro dinamico RADIUS. In questo caso, l'utente Alice è connesso ed è selezionato il criterio di autorizzazione previsto.



Il criterio di autorizzazione FTD-VPN-Posture-Unknown corrisponde e di conseguenza, FTD-VPN-Profile viene inviato a FTD.

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

Stato postura in sospenso.

NAS IPv4 Address 192.168.15.15

NAS Port Type Virtual

Authorization Profile FTD-VPN-Redirect

Posture Status Pending

Response Time 365 milliseconds

La sezione Risultato mostra quali attributi vengono inviati a FTD.

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

Su FTD, per verificare la connessione VPN, eseguire il comando SSH sulla casella, eseguire il supporto di sistema diagnostic-cli e quindi visualizzare i dettagli vpn-sessiondb su anyconnect. Da questo output, verificare che gli attributi inviati da ISE siano applicati per questa sessione VPN.

<#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

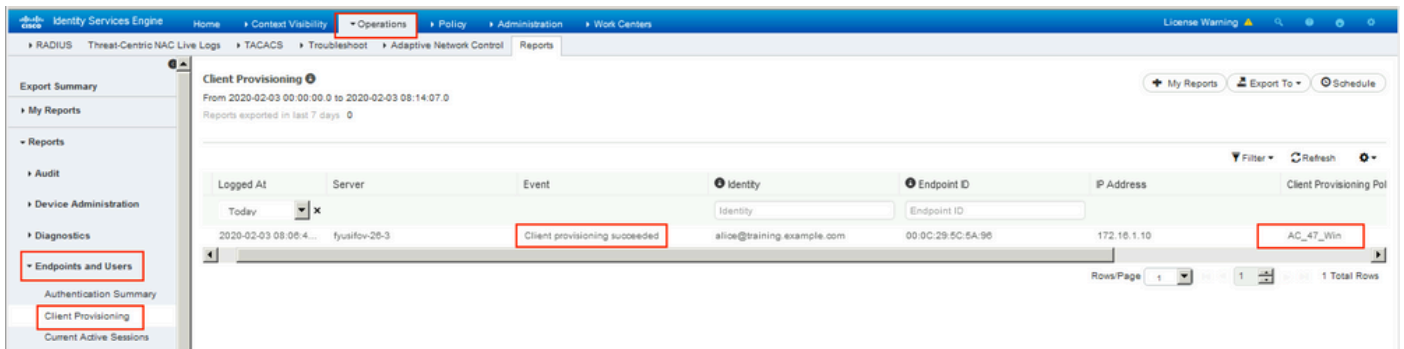
Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

ISE Posture:

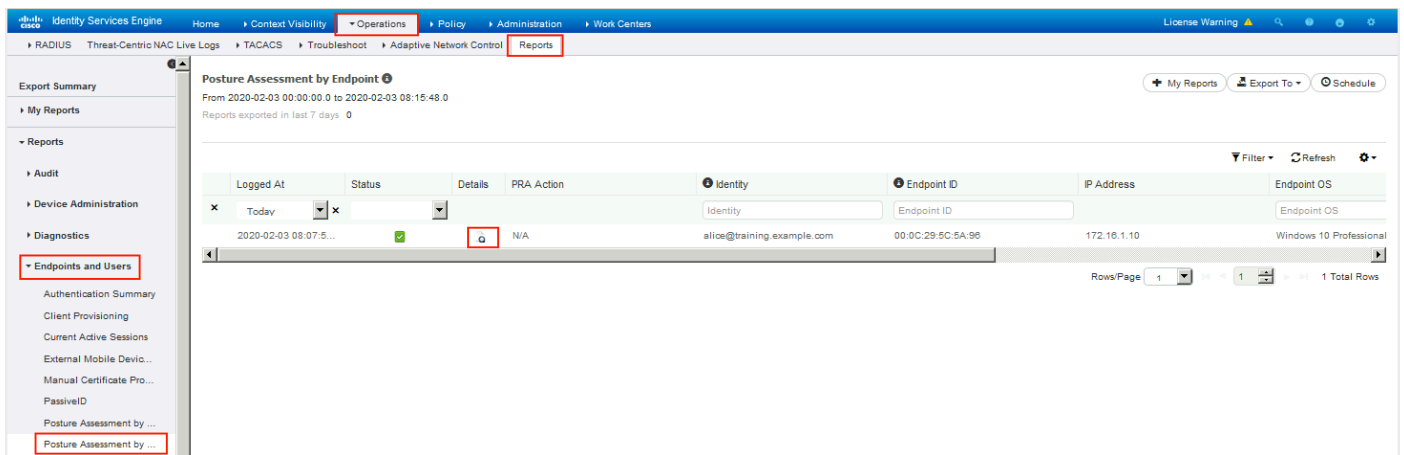
Redirect URL : <https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=00000000000c0005e37c81>
Redirect ACL : fyusifovredirect

fyusifov-ftd-64#

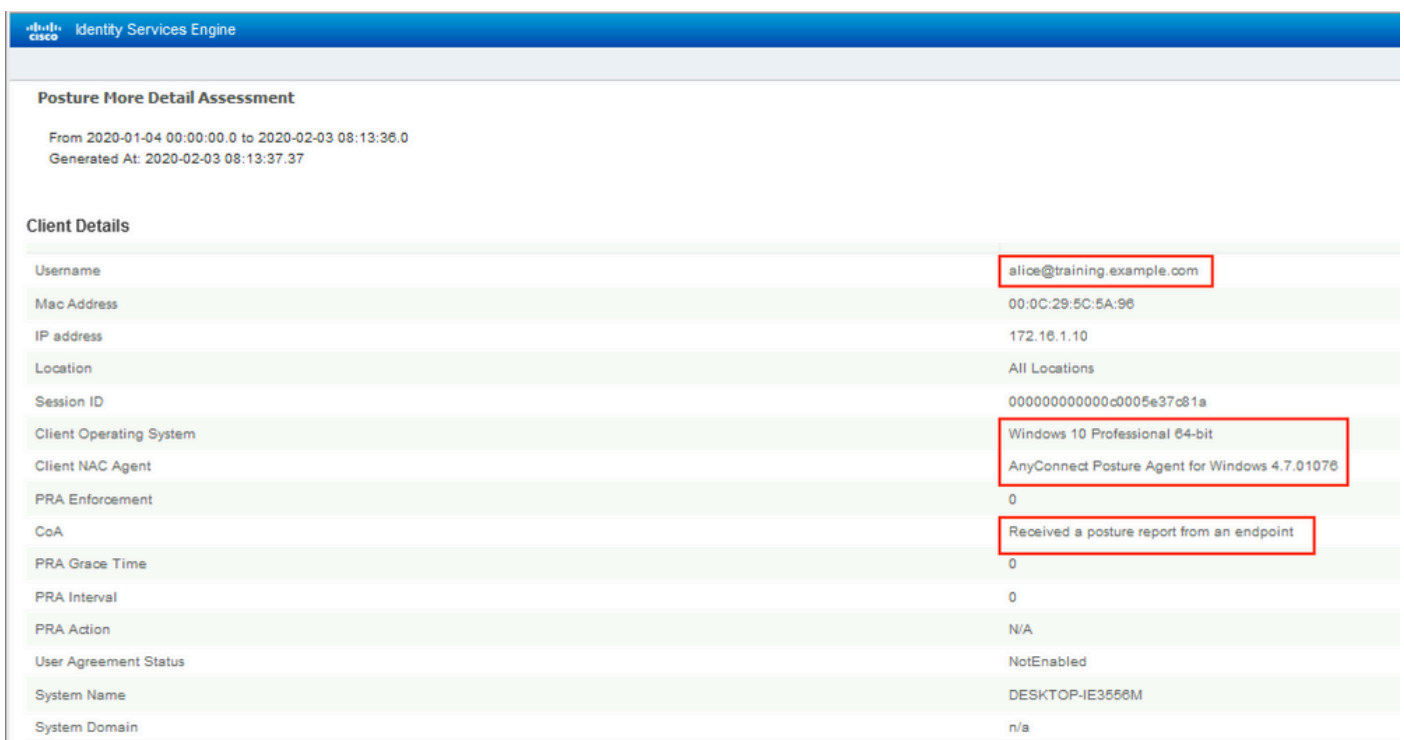
È possibile verificare i criteri di provisioning client. Passare a Operazioni > Report > Endpoint e utenti > Provisioning client.



È possibile controllare il report sulla postura inviato da AnyConnect. Passare a Operazioni > Rapporti > Endpoint e utenti > Valutazione postura per endpoint.



Per visualizzare ulteriori dettagli sul report di postura, fare clic su Dettagli.



Dopo la ricezione del report ad ISE, lo stato della postura viene aggiornato. In questo esempio, lo stato della postura è conforme e il Push CoA viene attivato con una nuova serie di attributi.

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-8753d45bf56c
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

Verificare a FTD che i nuovi ACL di reindirizzamento e URL di reindirizzamento vengano rimossi per la sessione VPN e che venga applicato PermitAll DACL.

```
<#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#

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per un flusso di postura dettagliato e per risolvere i problemi relativi a AnyConnect e ISE, controllare questo collegamento: [Confronto tra gli stili di postura ISE per le versioni precedenti e successive alla 2.2.](#)

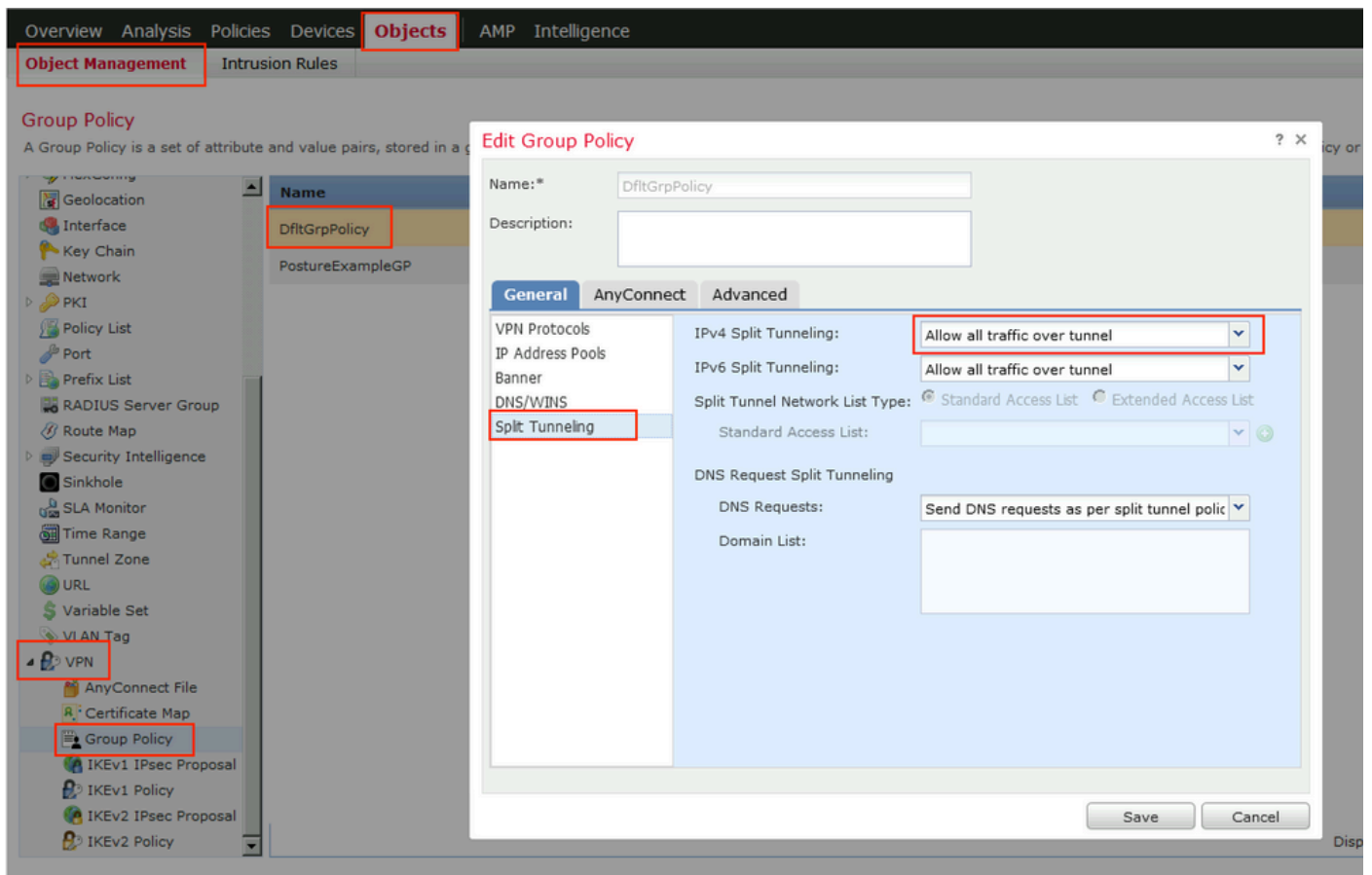
- Spilt Tunnel

Uno dei problemi più comuni, quando è configurato un tunnel di spit. In questo esempio viene utilizzato il criterio di gruppo predefinito, che esegue il tunneling di tutto il traffico. Nel caso in cui venga tunneling solo del traffico specifico, le sonde AnyConnect (enroll.cisco.com e host di rilevamento) devono attraversare il tunnel, oltre al traffico diretto all'ISE e ad altre risorse interne.

Per controllare i criteri del tunnel in FMC, verificare innanzitutto quali criteri di gruppo vengono utilizzati per la connessione VPN. Selezionare Dispositivi > Accesso remoto VPN.

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

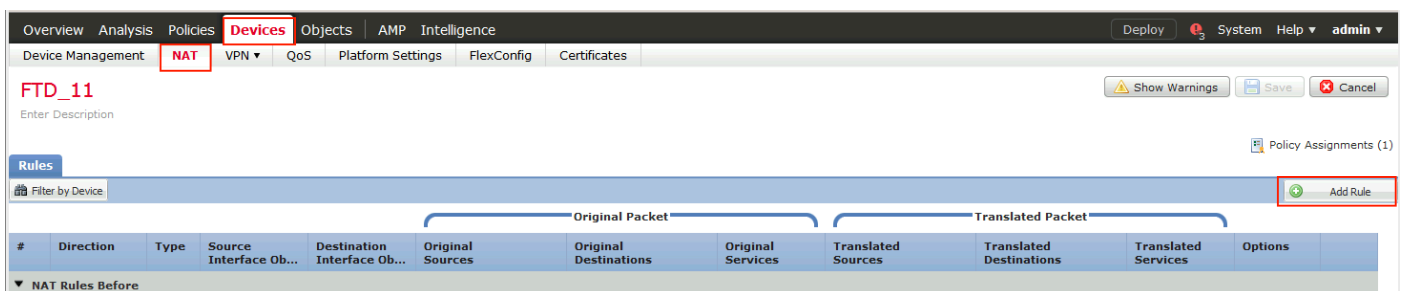
Passare quindi a Oggetti > Gestione oggetti > VPN > Criteri di gruppo e fare clic su Criteri di gruppo configurati per VPN.



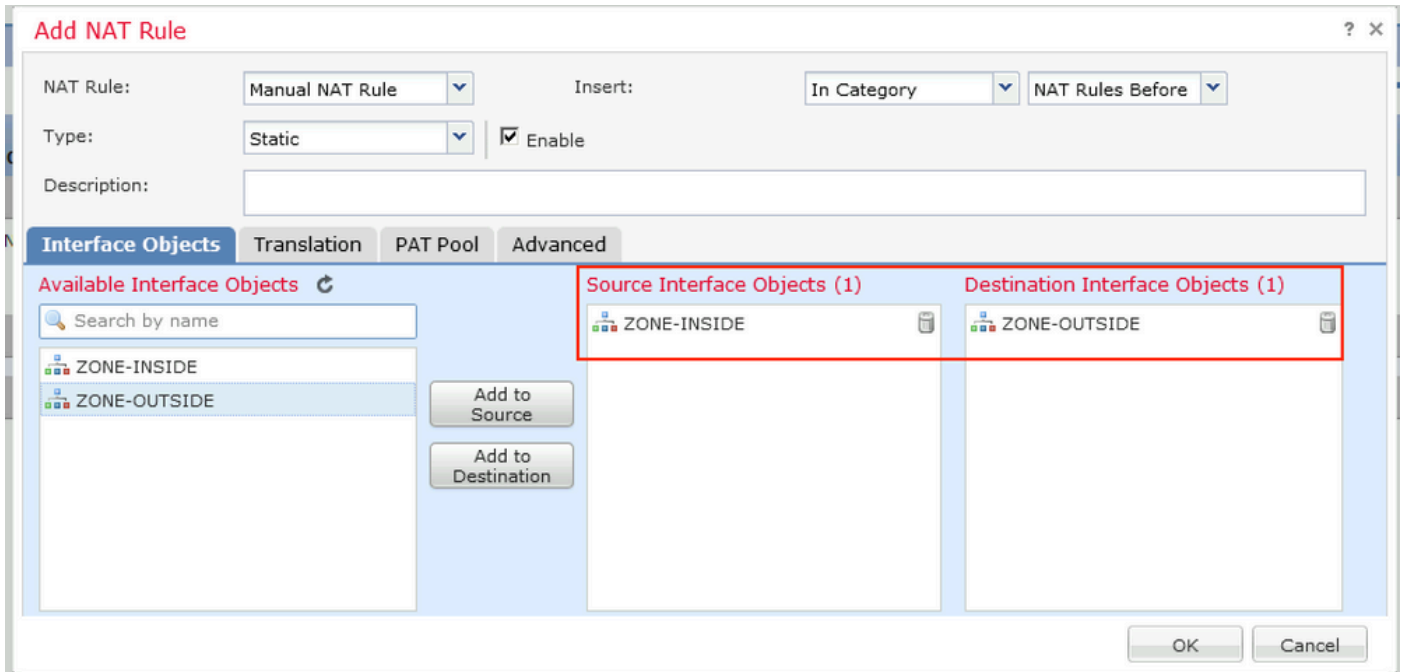
- Identity NAT

Un altro problema comune è quando il traffico di ritorno degli utenti VPN viene tradotto con l'uso di una voce NAT errata. Per risolvere il problema, è necessario creare Identity NAT nell'ordine appropriato.

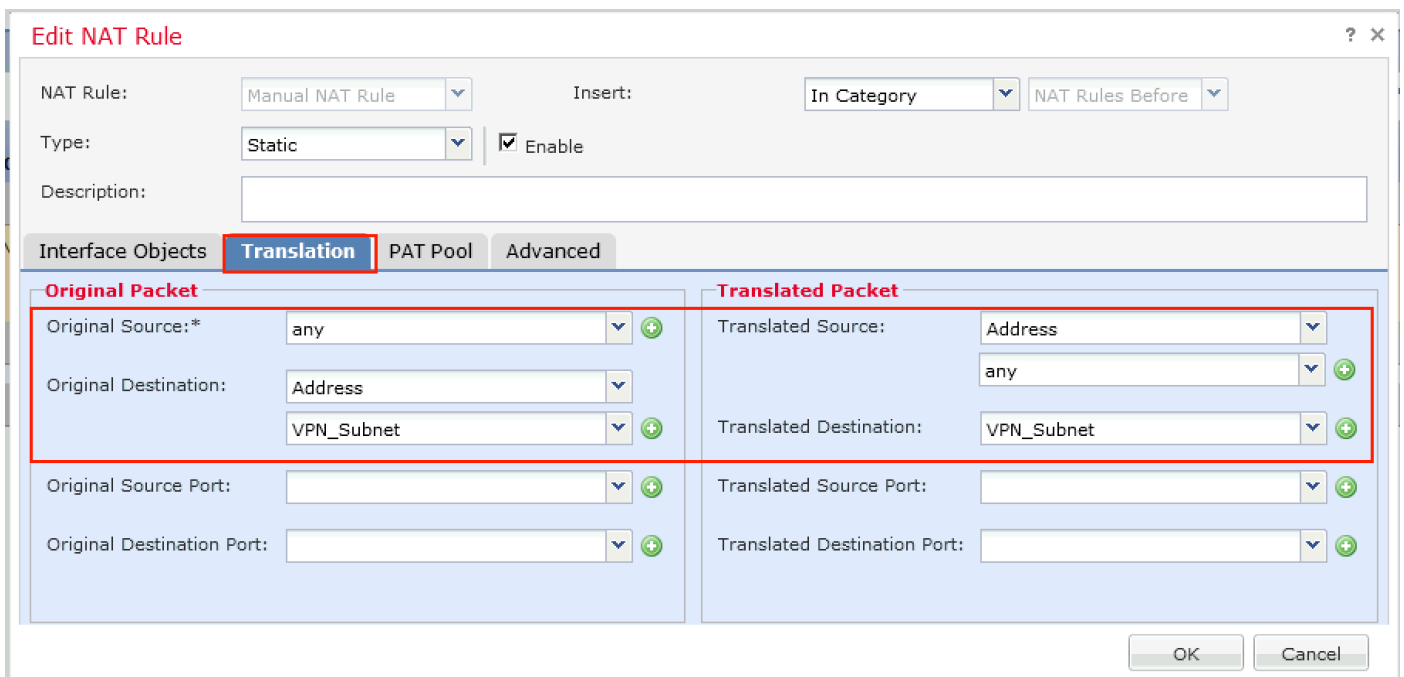
Controllare innanzitutto le regole NAT per il dispositivo. Passare a Dispositivi > NAT e fare clic su Aggiungi regola per creare una nuova regola.



Nella finestra aperta, selezionare Aree di protezione nella scheda Oggetti interfaccia. Nell'esempio, la voce NAT viene creata da ZONE-INSIDE a ZONE-OUTSIDE.



Nella scheda Traduzione, selezionare i dettagli del pacchetto originale e tradotto. Essendo Identity NAT, l'origine e la destinazione rimangono invariate:



Nella scheda Avanzate, selezionare le caselle di controllo come illustrato nell'immagine:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).