

åæ·FTDä, Šé€šé? ŽAnyConnecté? ç«¯è¨ªå•? VPN

ç»®éŒ,,

[ç°jää»<](#)

[å¿...è!æçä»¶](#)

[éœ€æ±,](#)

[æŽ;ç¨ª...fä»¶](#)

[è¨ª®š](#)

[ç¶²è·åœ-èj¨ª'Œæé†æª,³è¼,](#)

[çµæ...<](#)

[FTD/FMC](#)

[ISE](#)

[é©—è%o](#)

[ç-‘é:fxæŽ’èšf](#)

ç°jää»<

æœ-æªªæj^ä»ç¹å!,å½•è¨ª®šFirepowerå»è,...é²ç!|(FTD)ç%o^æœ-6.4.0ä»¥é†æª°è°«å^tè¨ª^¥æœæªª

[å¿...è!æçä»¶](#)

éœ€æ±,

æœçš'å»è°æ,¨çžèšfä»¥ä,ä,»éjŒi¼š

- AnyConnecté ç«¯åª-VPN
- FTDä, Šçš,é ç«¯åª-VPNçµ,æ...<
- è°«å»½æœæªªª¼æŽŽå'Œç€æ...æœæªªª

[æŽ;ç¨ª...fä»¶](#)

æœ-æªªæj^ä,çš,,è³†è¨ªšæ¨ª¹æ¨ªš«¥ä,«è»Ýé«¨ç%o^æœ-i¼š

- Cisco Firepowerå»è,...é²ç!|(FTD)è»Ýé«¨ç%o^æœ-6.4.0
- Cisco Firepowerç°jç†æŽšå^¶æª(FMC)è»Ýé«¨ç%o^æœ-6.5.0
- æè¼%oCisco AnyConnectå®%oå...¨èjŒåªåŒ-å½ç¨¨è€...ç«¯ç%o^æœ-4.7çš,,Microsoft Windows 10
- æœçš'è°«å^tè¨ª^¥æœæªªª¼æŽŽ(ISE)ç%o^æœ-2.6i¼Œå,¶èfœä,³

æœ-æ-†ä,çš,,è³†è¨ªšæ¨ª¹æ¨ªš«šç%o¹å®šå¹é©—å®çç'°åçfå...šçš,,èfç½®æ%o€å»°ç««ã€æ-†ä,å½ç¨¨å^°çš,,æ

è¨ª®š

[ç¶²è·åœ-èj¨ª'Œæé†æª,³è¼,](#)

Win10 with AnyConnect



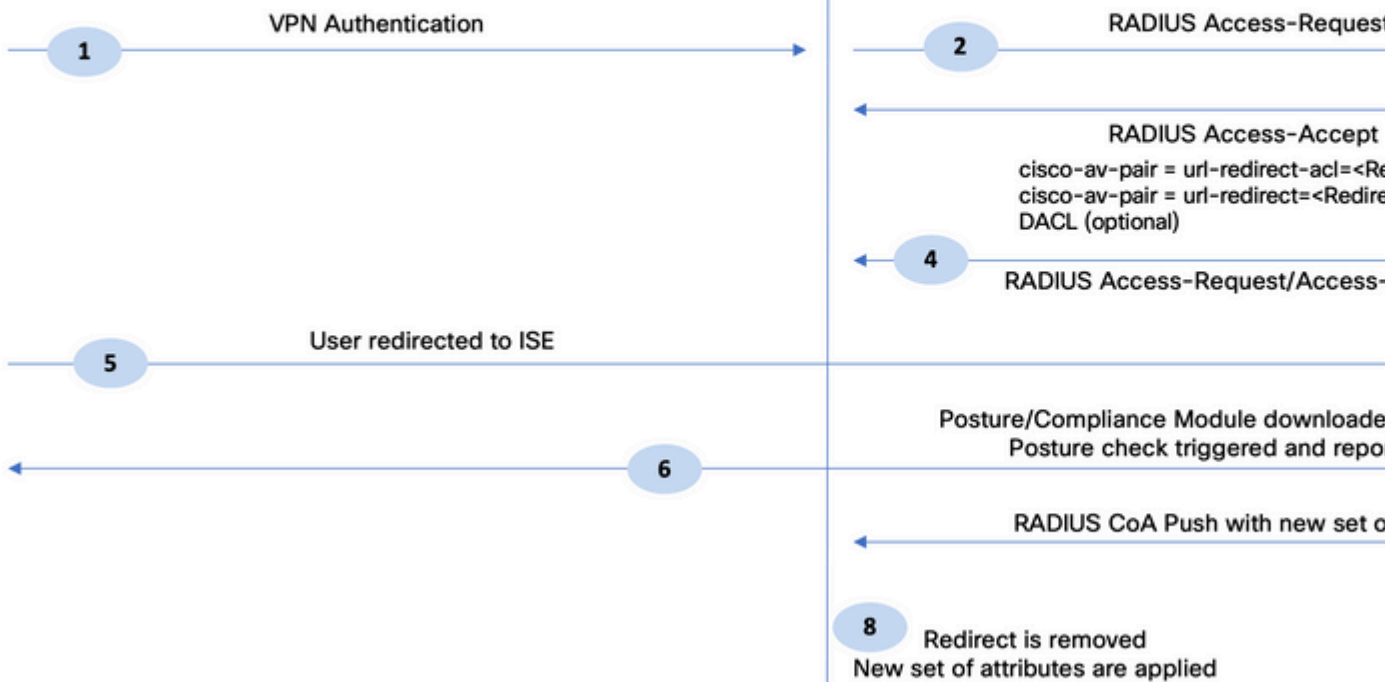
FTD



outside

inside

fyusif



1. é ç « ä ½ ç ” è € ... ä ½ ç ” Cisco Anyconnect é € ? è ; Ç FTD ç š „ VPN è ° ä • ä € ,

2. FTD ä • ISE ä , ³ é € è © ä ½ ç ” è € ... ç š „ RADIUS ä ~ ä • - è | • æ ± , ä € ,

3. è © ² è « æ ± , ä œ ” ISE ä , Š ä ^ ° é • ” ä • • ç , ° FTD - VPN - Posture - Unknown ç š „ ç - ç • ¥ ä € , ISE ä , ³ é € ä , ¶ æ œ % ö ä , % ö ä € ç ä ± - æ € Š ç š „ RADIUS Access - Accept :

- **cisco-av-pair = url-redirect-acl=fyusifovredirect** â € ” é €™ æ ~ ä œ ” FTD æ œ - æ © Ÿ ä , Š ä @ š ç ¾ © ç š „ ä ~ ä • - æ Ž š ä ^ ¶ æ „ ... ä - @ (ACL) ä • • ç ” ± i ¼ Ç æ ± ä @ š é † • æ - ° ä ° Ž ä
- **cisco-av-pair = url-redirect=**<https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp> â € ” é €™ æ ~ • ç « ä ½ ç ” è € ... é † • ä @ š ä • ä ^ ° ç š „ URL ä € ,
- **DACL = PERMIT_ALL_IPV4_TRAFFIC** â € ” ä • ä , < è ¼ % ACL æ ¢ ä ± - æ € § æ ~ ä • - é • ç š „ ä € , ä œ ” æ ¢ æ j ^ ä ¾ ä , i ¼ Ç æ % ö æ œ % ö æ µ • é † • é f ½ ä ... è ” ± ä

4. ä , æ ž œ ä , ³ é € ä ° † DACL i ¼ Ç ä % ö † æ œ f ä ° ¢ æ • RADIUS Access - Request / Access - Accept i ¼ Ç ä » ¥ ä ¾ ä , è ¼ % DACL ç š „ ä ... Š ä @ ¹

5. ç • ¶ ä ¾ † è † a VPN ä ½ ç ” è € ... ç š „ æ • é † • è ^ † æ œ - ä œ ° ä @ š ç ¾ © ç š „ ACL ä Ç ¹ é ... æ™ , i ¼ Ç æ µ • é † • ä ° † é † • ä

6. ä œ ” ä @ ç æ ^ ¶ ç « - é » è ... ! ä , Š ä @ % è f • ä » £ ç • † ä ¾ Ç ä i ¼ Ç ä @ f æ œ f ä ½ ç ” æ Ž ç æ , - ä Š Ÿ è f ½ è † a ä • æ • œ ä ° < ISE ä €

7. ç • ¶ ISE æ ” ¶ ä ^ ° ä ¾ † è † a » £ ç

◆†çš,,ç<€æ...<â ±âŠæ™,i¼CEISEæ'æ"¹æææææfè©±çš,,ç<€æ...<ä,|èš,ç™¼ä...·ææ%æ-°â±-æ€šçš,,RADIU
CoAž<â^¥Pushã€€,é™ä,€æ-ij¼CEç<€æ...<ç,°â²çŸ¥i¼CEâ◆|ä,€ã€<è|◆â%ø†èç<«â'½ä,ã€,

- â!,æžæä½ç™"è€...ç-|â◆^è|◆æ±,ij¼CEâ%ø†ææfâ,³é€◆â...◆è"±â@CEâ...è"ªâ•◆çš,,DACLâ◆◆ç"±
- â!,æžæä½ç™"è€...ä,◆ç>,â@¹i¼CEâ%ø†ææfâ,³é€◆â...◆è"±ææ%é™◆è"ªâ•◆çš,,DACLâ◆◆ç"±ã€,

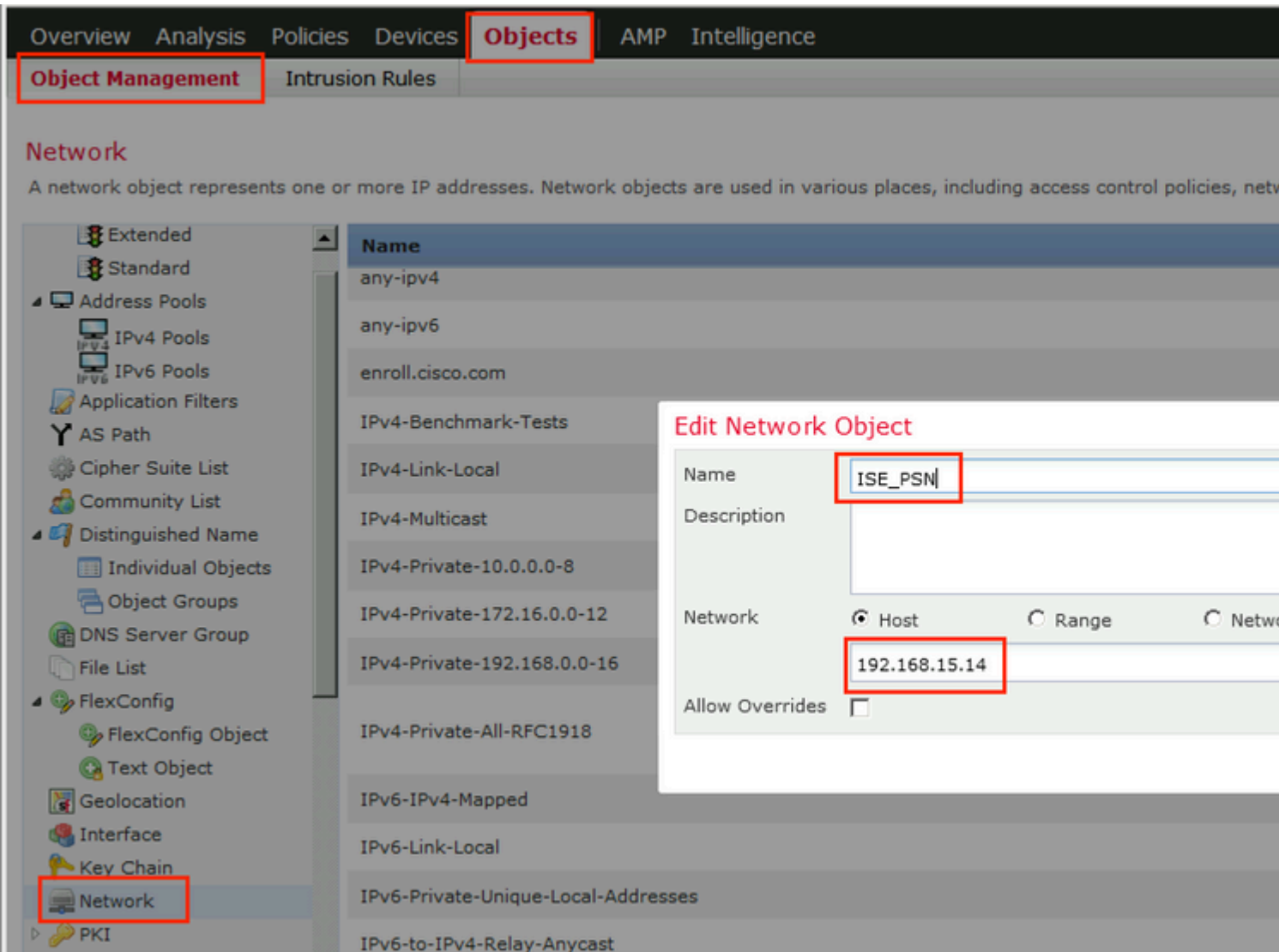
8.

FTDææfçš»é™æé†◆æ-°âžâ◆'ã€,FTDææfâ,³é€◆â~â◆-è|◆æ±,ij¼CEâ»¥ã¼ç¼¼žISEä,è¼%æDACLã€,ç>

çµæ...<

FTD/FMC

æ¥é©Ÿ1.ç,°ISEâ'CEä;@æfä¼°ææ◆â™"i¼^â|,æžæææ%øi¼%æ»ç<<ç¶²è·°◆è±jçµ,,ã€,â°žè^ª^ª°◆è±j;



æ¥é©Ÿ2.â»°ç<<é†◆æ-°âžâ◆'ACLã€,â°žè^ª^ª°◆è±j>â°◆è±jçµ;ç>†>è"ªâ•◆æ,...â-@>æ"ª±ã€,æD
Extended Access

Listã€i¼CEâ,|æ◆◆ã¼é†◆æ-°âžâ◆'ACLçš,,â◆◆ç"±ã€,æªâ◆◆ç"±âž...é^è†ISEæž^æ-šçµ◆æžç

Overview Analysis Policies Devices **Objects** AMP Intelligence

Object Management Intrusion Rules

Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

- Access List
 - Extended
 - 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

New Extended Access List Object

Name:

Entries (0)

Sequence	Action	Source	Source Port	Destination
No records to display				

Allow Overrides

æ¥é©ÿ3.æ-°åçžé† ◆å®šå ◆'ACLæç ◆ç>®ã€ ,æŒ%0ä, €ä, <AddæŒ%0é^•ã€ ,é~»æçç™¹¼å³⁄4€DNSã ◆ISEå'Œèè€

Add Extended Access List Entry

Action: ⌵

Logging: ⌵

Log Level: ⌵

Log Interval: Sec.

Network Port

Available Networks ↻ +

Search by name or value

- any
- any-ipv4
- any-ipv6
- enroll.cisco.com
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

Source Networks (1)

- any-ipv4

Destination Networks

- ISE_PSN

Edit Extended Access List Object

Name

Entries (4)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	any	Any	Any	DN
2	Block	any-ipv4	Any	ISE_PSN	Any
3	Block	any-ipv4	Any	RemediationServers	Any
4	Allow	any-ipv4	Any	any-ipv4	Any

Allow Overrides

æ¥€©Ÿ4.æ-°âçŽISE PSNç-€é»žã€,,â°Žè^ââ° è±;â° è±;ç@;ç†>

RADIUSä¼°æœ°â™™ çµ,,â€,,æ€%œä, €ä,Add RADIUS Server

Groupi¼€ç,,¶â¾€æ°° ä¾°â°° ç° ±i¼€â°Ÿç°° é° ,ä,æ%œæœ%œè|^â° -æ-¹â;šä,|é»žé° ,plusâœ-çœ°â€

Edit RADIUS Server Group

Name:*

ISE

Description:

Group Accounting Mode:

Single

Retry Interval:*

10

(1-10)

Realms:

Enable authorize only

Enable interim account update

Interval:*

24

(1-12)

Enable dynamic authorization

Port:*

1700

(1024)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname

No records to display

Interface, ISE, RADIUS, ACL

New RADIUS Server

IP Address/Hostname: * 192.168.15.13

Authentication Port: * 1812

Key: * [Redacted]

Confirm Key: * [Redacted]

Accounting Port: 1813

Timeout: 10

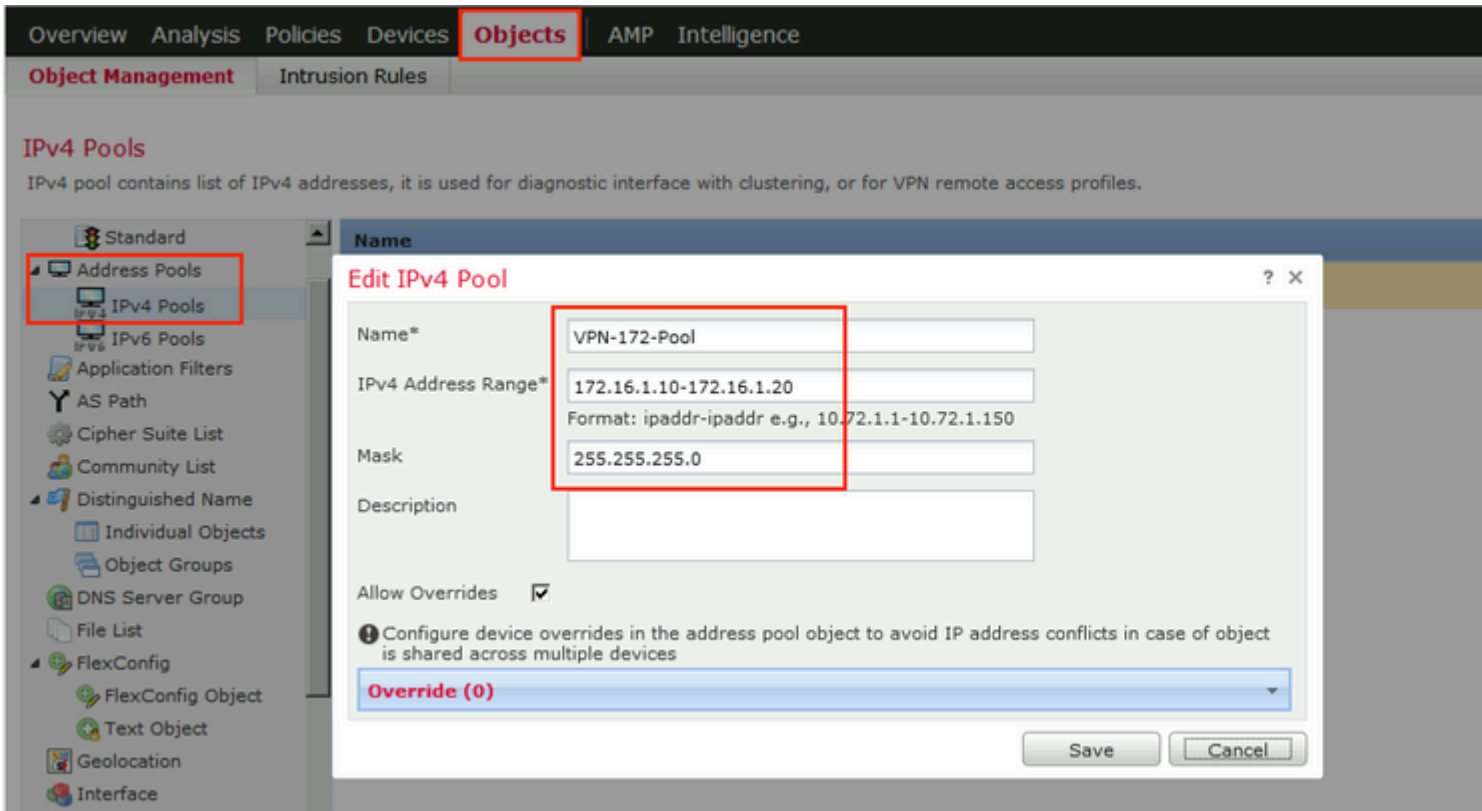
Connect using: Routing Specific Interface *i*

ZONE-INSIDE

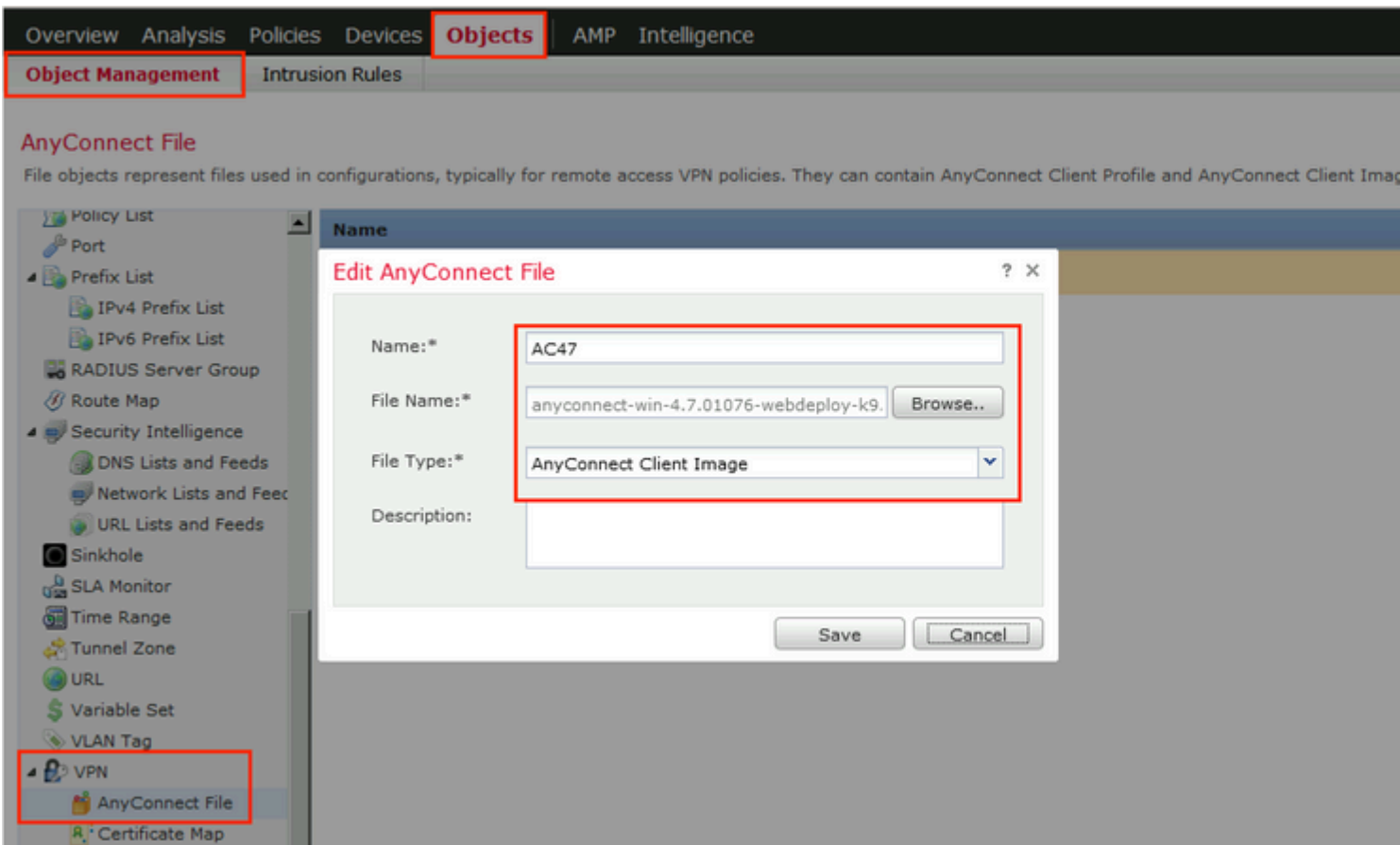
Redirect ACL: fyusifovredirect

Save

VPN, Add IPv4 Pools



AnyConnect » Objects > Object Management > VPN > Add AnyConnect File » Cisco Software Download » Anyconnect Client Image File Type



æ¥é©ÿ8.â°žè^â° Certificate Objects > Object Management > PKI > Cert

Enrollment, æE%öä, €ä, Add Cert Enrollment, ä¼Eæ, ä¼, ç, ±i¼Eâö, Enrollment

Type, é, æ, Self Signed Certificate, é, žé, Certificate Parameters, ç±, ä, æ, ä¼, CN, ä, €,

The screenshot displays the Fortinet FortiGate web interface. At the top, the navigation menu includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' tab is active, and the 'Object Management' sub-tab is selected. The main content area shows the 'Cert Enrollment' section. A dialog box titled 'Add Cert Enrollment' is open, showing the following fields and options:

- Name***: vpn-cert
- Description**: (empty text box)
- CA Information** (selected tab):
 - Enrollment Type**: Self Signed Certificate
 - Warning**: Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.
- Allow Overrides**:

The left sidebar contains a tree view of configuration objects. The 'PKI' folder is expanded, and the 'Cert Enrollment' item is highlighted with a red box. At the bottom right of the dialog, there are 'Save' and 'Cancel' buttons.

Add Cert Enrollment

Name*

vpn-cert

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN:

Use Device Hostname as FQDN

Include Device's IP Address:

10.48.26.99

Common Name (CN):

vpn-cert.example.com

Organization Unit (OU):

Organization (O):

example

Locality (L):

State (ST):

Krakow

Country Code (C):

PL

Email (E):

Include Device's Serial Number

Allow Overrides

Access > VPN > Remote

Overview Analysis Policies **Devices** Objects AMP Intelligence

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

Name	Status	Last Modified
No configuration available Add a new configuration		

æ¥é©ÿ10.æ...ä³¼>â...ç...±i¼Ææªçæÿ¥SSLä½œç,°VPNâ...â®š¼Æé...æ"†ç"...ä½œVPNé>†ä,â™...çš,,F

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

Search:

192.168.15.11

Selected Devices

192.168.15.11

Add

Before You Start

Before you start, ensure that the required configuration elements are in place to complete Remote Access VPN configuration.

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

AnyConnect Client Package
Make sure you have the AnyConnect Client package for VPN Clients. If you do not have it, you have the relevant download link to download it during the configuration process.

Device Interface
Interfaces should be assigned to the targeted devices so that they can be used as a security zone. You can also assign a security zone to enable VPN access.

æ¥é©ÿ11.æ...ä³¼>é€ç:šé...ç½®æ"æj^â...ç...±i¼Æé...æ"†è°«ä»½é©—è%ø/è™...â,³ä¼°æœ...â™...i¼Æé

æ³"æ,,i¼šè«<â<jé...æ"†æŽ^æ-šä¼°æœ...â™...ã€â®fèš,ç™¼â-®â€<ä½ç"...è€...çš,,â...©æ-j

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: * (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](#)

æ¥é©Ÿ12.é,æ“#ä»¥å%é...ç½@çš,,AnyConnectè»Ÿé«”åĈ...ï¼Ĉç,,¶å¼ĈæĈ%oä,€ä,ĸNextã€,

Remote Access VPN Policy Wizard

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

AnyConnect Client Image
The VPN gateway can automatically download the latest AnyConnect package to the client device when the 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"/>	AC47	anyconnect-win-4.7.01076-webdeploy-k9....	Windows

æ¥é©ÿ13.é,æ"†â,Ææœ>â¼žä,æŽ¥æ"¶VPNæµé†çš,,ä»éçï¼Æé,æ"†Certificate Enrollmenti¼^ä»¥â%é...ç½®çš,,è%œ>è" »â†šï¼%oi¼Æç,,¶â¼ÆæÆ%öä,€ä,«Nextã€,

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: *

Enroll the selected certificate object 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.

æ¥é©ÿ14.æªçæÿ¥æ"~è!é éçï¼Æç,,¶â¼ÆæÆ%öä,€ä,«â®Ææ^ã€,

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:	EmployeeVPN
Device Targets:	192.168.15.11
Connection Profile:	EmployeeVPN
Connection Alias:	EmployeeVPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE
Authorization Server:	ISE
Accounting Server:	ISE
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	VPN-172-Pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
AnyConnect Images:	AC47
Interface Objects:	ZONE-OUTSIDE
Device Certificates:	vpn-cert

- ### Additional Configuration Required
- After the wizard completes, configuration needs to be completed on all device targets.
- 1 Access Control Policy Update**
An [Access Control](#) rule must be configured to allow VPN traffic on all targeted devices.
 - 1 NAT Exemption**
If NAT is enabled on the target device, you must define a [NAT Policy](#) to exempt VPN traffic.
 - 1 DNS Configuration**
To resolve hostname specifications on target devices or CA Servers, configure a [FlexConfig Policy](#) on the target devices.
 - 1 Port Configuration**
SSL will be enabled on port 443. Please ensure that these ports are open on the target devices in [NAT Policy](#) or other security policies when deploying the configuration.
 - 1 Network Interface Configuration**
Make sure to add interface configuration for target devices to SecurityZone of 'OUTSIDE'.

æ¥é©ÿ15.å°‡çµæ...<éf`ç½2â°FTDã€æCE%öä,€ä,ã€Deployã€ï¼CEç,,¶å¾CEé,æ“†ç”” ä½œVPNé›tä,å™”

Overview Analysis Policies **Devices** Objects AMP Intelligence

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

EmployeeVPN

Enter Description

Connection Profile Access Interface

Name

DefaultWEBVPNGroup

EmployeeVPN

Deploy Policies Version: 2020-02-02 09:15 PM

<input checked="" type="checkbox"/>	Device	Inspect Interruption	Type	Group	Current Versi
<input checked="" type="checkbox"/>	192.168.15.11	No	FTD		2020-02-02 09:15 PM

Selected devices: 1

ISE

Administration > System > Settings > Posture > Updates

Posture Updates

Web Offline

* Update Feed URL

Proxy Address ⓘ

Proxy Port HH MM SS

Automatically check for updates starting from initial delay every

Save

Update Now

Reset

▼ 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:
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

Policy > Policy Elements > Results > Client Provisioning > Resources > Add Agent resources from Cisco site

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.972.4353	AnyConnect OSX Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance M
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.1053.6145	AnyConnect Windows Compliance M
<input type="checkbox"/>	CiscoTemporalAgentOSX 4.8.03009	Cisco Temporal Agent for OSX With C
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.8.03009	Cisco Temporal Agent for Windows V
<input type="checkbox"/>	ComplianceModule 3.6.11428.2	NACAgent ComplianceModule v3.6.1
<input type="checkbox"/>	MACComplianceModule 3.6.11428.2	MACAgent ComplianceModule v3.6.1
<input type="checkbox"/>	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9
<input type="checkbox"/>	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for M
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for M

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource" option, to import into ISE

© 2013 Cisco Software

[Download](#) > AnyConnect > Policy > Policy Elements > Results > Client Provisioning > Resources

Add Agent Resources From Local

Disk Category

Packages

Submit

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

Category

Cisco Provided Packages ⓘ

Browse... anyconnect-win-4.7.01076-webdeploy-k9.pkg

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.10...	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secu

Submit Cancel

Policy > Policy Elements > Results > Client Provisioning > Resources

Add AnyConnect Posture Profile

Server name rules put Discovery host

ISE Posture Agent Profile Settings > AC_Posture_Profile

* Name: AC Posture Profile
Description

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if 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 server names that the agent can connect to. E.g. *.ci
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 the agent will try to connect to if the PSN is unreachable 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 continue to connect to targets and previously connected targets until max time limit is reached

Policy > Policy Elements > Results > Client Provisioning > Resources > AnyConnect Configuration > Add AnyConnect Configuration > AnyConnect Package > Compliance Module > Diagnostic and Reporting Tool > Posture Profile > Save

* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.1076.0

* Configuration Name: AC CF 47

Description:

Description Value

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1012

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

Policy > Client Provisioning > Client Provisioning

Policy > Edit > Insert Rule

Above > OS > AnyConnect Configuration >

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

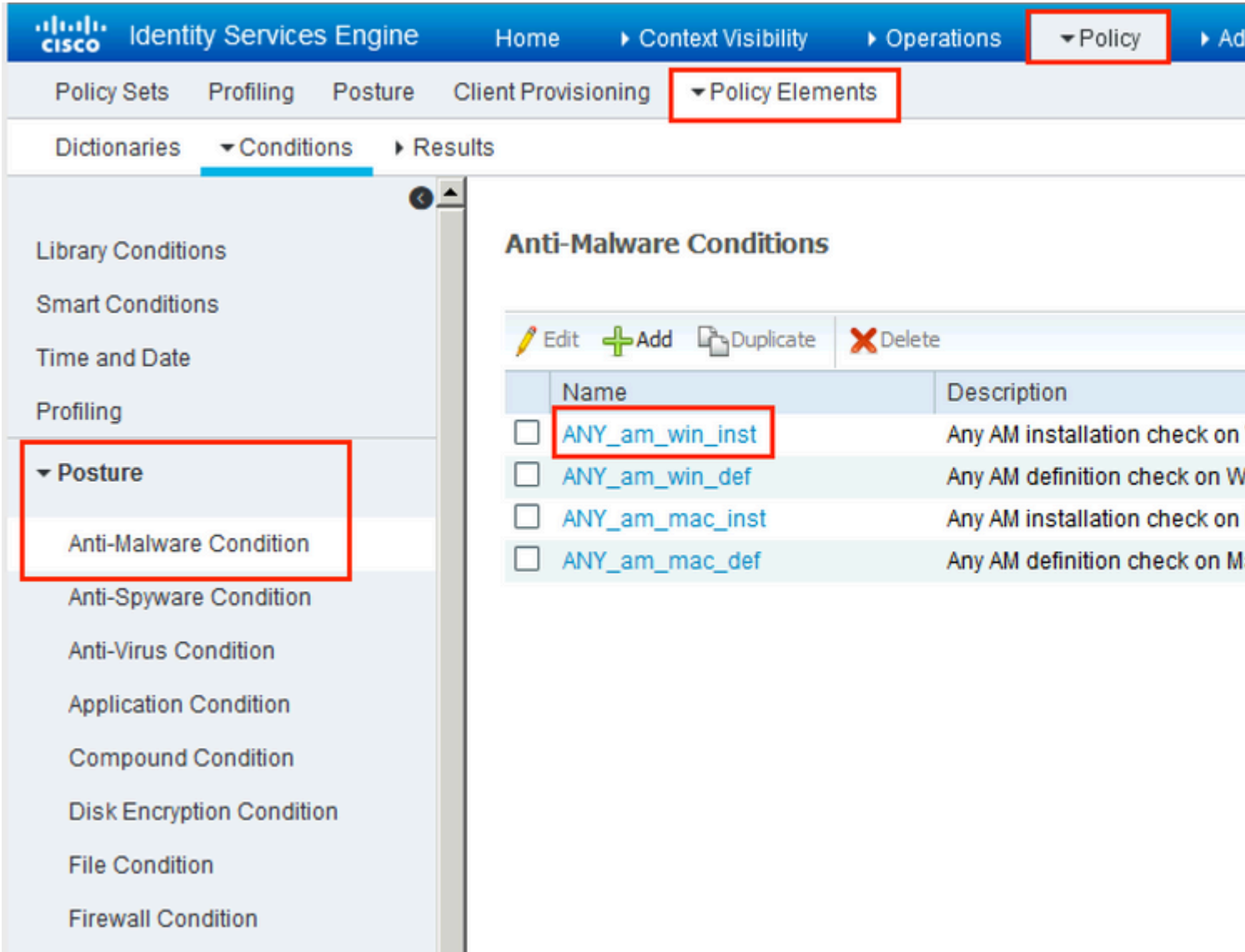
Client Provisioning Policy

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

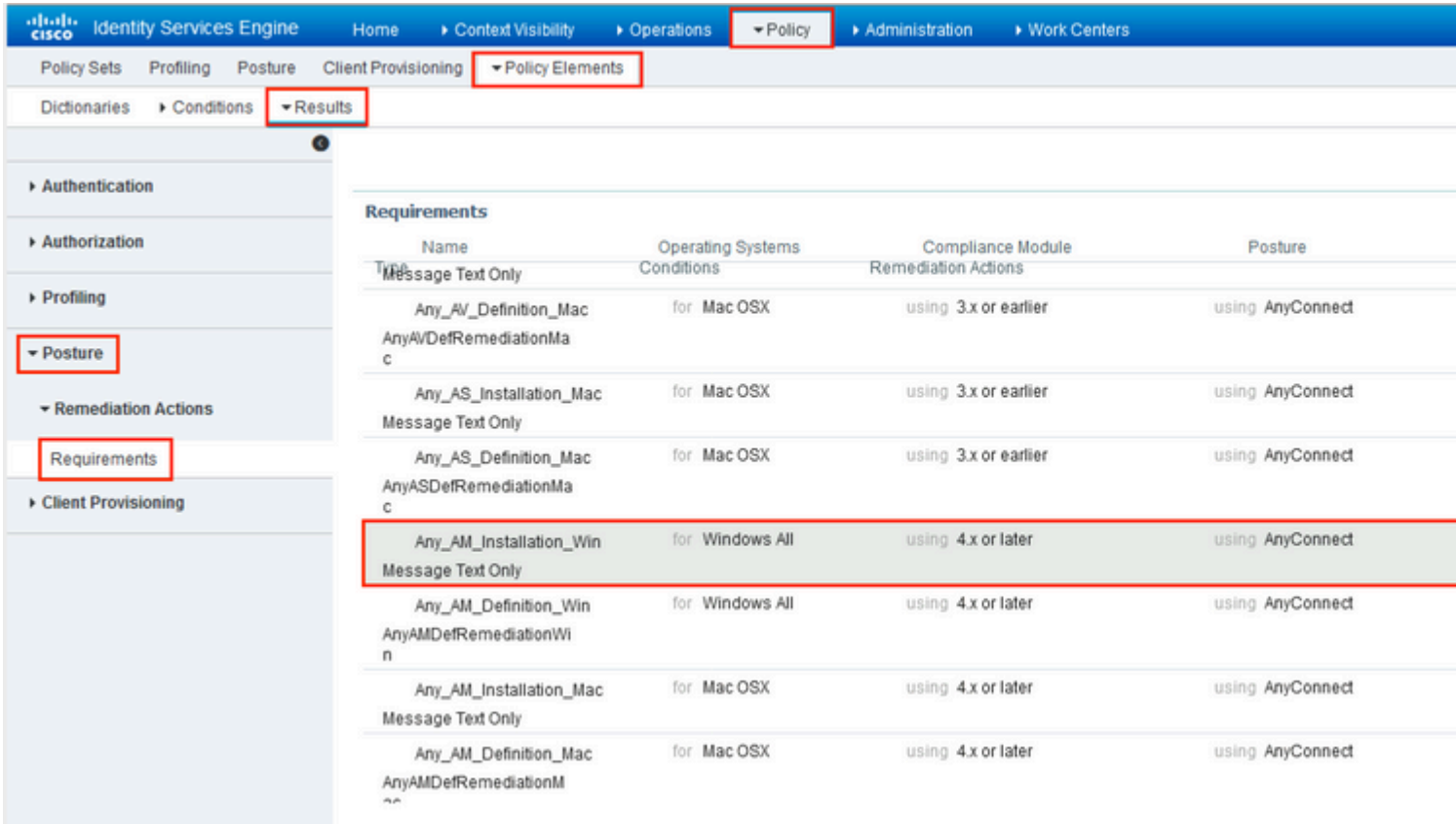
Policy > Policy Elements > Conditions > Posture > Anti-Malware

Condition ANY_am_win_in



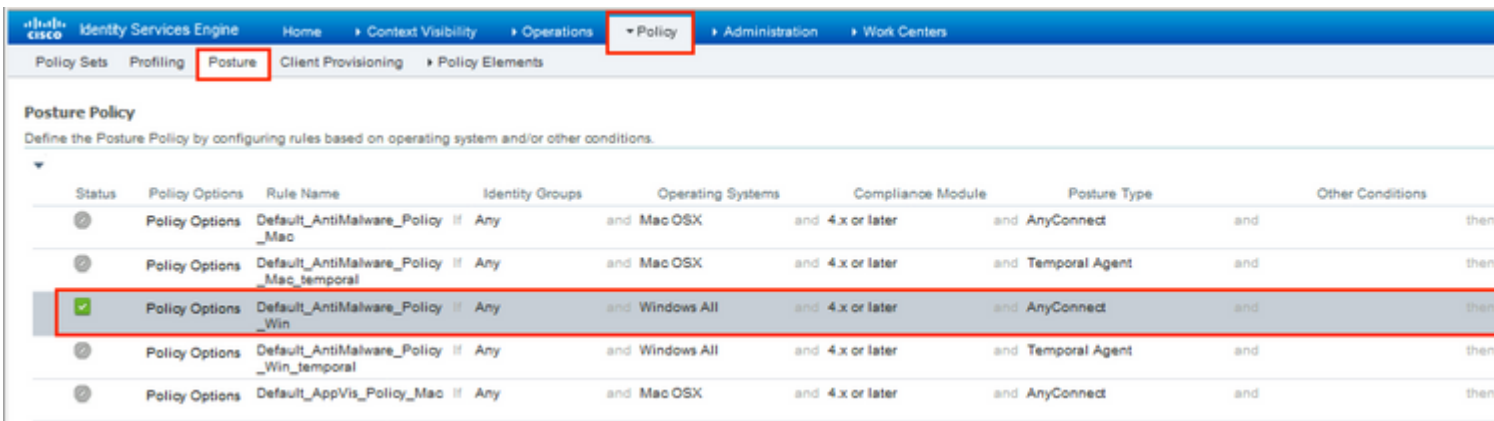
Policy > Policy Elements > Results > Posture > Remediation Actions > Posture Remediation > ANY_AM_Installation_Win

Policy > Policy Elements > Results > Posture > Requirements > Posture Requirements > ANY_AM_Installation_Win



æŸé©Ÿ10.âœ`Policies >

Postureä, <â>°ç<<ç<€æ...<ç-ç•Ÿã€,,ä1/2ç””é#â°â°Windowsä1/2œæŸç³»çµ±çš,,ä»»ä1/2•é~2æfjæ,,â»è»Ÿé«”æªCa



æŸé©Ÿ11.â°Žè^â°Policy > Policy Elements > Results > Authorization > Downloadable

ACLi1/4(€ç,,¶â3/4(€ç,°ä,â°â°(€çš,,ç<€æ...<â>°ç<<DACLã€,

âœ`æŸç”,,ä3/4<ä,i1/4š

- ç<€æ...<æªçŸŸDACL â€”
â...â°è”±æµâ°é†â°éâ°”DNSã€â°PSNä»Ÿâ°šHTTPâ°(€HTTPSæµâ°é†â°ã€,
- â@%â...”ç<€æ...<ä,â°ç-!â°^DACL â€”
æ’çµ•è”â°â°â°ç””â°ç¶²ä,|â°f...â...â°è”±ç¶²és>ç¶²è-æµâ°é†â°ã€,
- Permit All DACL â€”
â...

[Downloadable ACL List > PostureNonCompliant1](#)

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic [i](#)

* 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 List > New Downloadable ACL](#)

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic [i](#)

* 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

æ¥©Ÿ12.ç,°Posture Unknownã€Posture NonCompliantã'ÆPosture
Compliantç«æ...<ã»°ç««ä,‰ã€<æŽ^æ-Šé... ç½®æ"æj^ã€,ç,°æπ¼Æè«<ã°Žè^èè#³Policy >
Policy Elements > Results > Authorization > Authorization Profilesã€,ãæPosture
Unknownè"ã@šæ"ä,¼Æé,æ"†Posture Unknown DACLi¼ÆæªçæŸ¥Web
Redirectioni¼Æé,æ"†Client
Provisioningi¼Ææ,ä¾æ†æ-°ãŽã'ACLãç"±i¼^ãœ"FTDä,Šè"ã@š¼‰ä,|é,æ"†ã...¥ã£ç

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&acti

Posture

NonComplianté... ç½@æ"æj^ä,j¼Œé,æ"‡DACLä»¥é™ä^¶å°ç¶²è·çš,,è"å•ã€,

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... ç½@æ"æj^ä,ï¼Éé,æ"†DACLä»¥å... è±å° ç¶²è-çš,,å@Æå... è"å•ã€,

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

Policy > Policy Sets > Default > Authorization

Policy, <â>°ç<<æŽ^æ-šç-ç•¥ã€„Asæçä»¶||ä½¿ç'''ç<€æ...<ç<€æ...<â'CEVNPéššé"çμ,,âç"±ã€„

Identity Services Engine Home Context Visibility Operations **Policy** Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Default Default policy set

Authentication Policy (3)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (18)

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

é©—è%

äl½ç”æ¬ç¬€â...šâ@i¼Eçç°èæ, çš,,çµ,,æ...æ¬âæ | æ£â,,éæ½œæ€,

âœISEä,š¼Eç¬¬ä, €â€é©—è%æ¥é©ÿæ¬RADIUSæ™,æ¬¥èªEã€‚â°žè½è³ **Operations > RADIUS Live**

Logã€‚âœ¬é€™è£;¼¼Eä½½ç”è€... Aliceâ²é€£ç¬š¼¼Eä¼ä,¼,¼”âæ¬æ”éæœÿçš,,æž^æ¬šç¬ç¥ã€,

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0

Refresh Reset Repeat Counts Export To

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

Last Updated: Mon Feb 03 2020 08:16:39 GMT+0100 (Central European Standard Time)

æž^æ¬šç¬ç¥FTD-VPN-Posture-

Unknown... FTD-VPN-Profile, FTD,

Overview

Event	5200 Authentication succeeded
Username	alice@training.example.com
Endpoint Id	00:0C:29:5C:5A:98
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	fyusifov-26-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

...@,

NAS IPv4 Address	192.168.15.15
NAS Port Type	Virtual
Authorization Profile	FTD-VPN-Redirect
Posture Status	Pending
Response Time	365 milliseconds

... 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=0d90f1cdf40e83039a7ad6a228603112
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

System support diagnostic-cli show vpn-sessiondb detail anyconnect

<#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#

å♦-ä»¥é©—è%å®¢æ^¶ç«-è³¿é...♦ç-ç•¥ã€‚å°žè^å^æ“♦ä½œ>å±åš>ç«-é»žå'œä½¿ç"'è€...>å®¢

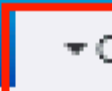
Client Provisioning

From 2020-02-03 00:00:00.0 to 2020-02-03 08:14:07.0

Reports exported in last 7 days: 0

Logged At	Server	Event	Identity	Endpoint ID
Today			Identity	Endpoint ID
2020-02-03 08:06:4...	fyusifov-26-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:96

å♦-ä»¥æª¢æÿ¥å³¼žAnyConnectå,³é€♦çš,,ç«œ³♦å±åšš€‚å°žè^å^æ“♦ä½œ>å±åš>ç«-é»žå'œä½¿ç"'è€...>å®¢



Export Summary

My Reports

Reports

Audit

Device Administration

Diagnostics

Endpoints and Users

Authentication Summary

Client Provisioning

Current Active Sessions

External Mobile Device...

Manual Certificate Pro...

PassiveID

Posture Assessment by ...

Posture Assessment by ...

Posture Assessment by Endpo

From 2020-02-03 00:00:00.0 to 202

Reports exported in last 7 days 0

	Logged At	St
--	-----------	----



Today



2020-02-03 08:07:5...



Posture More Detail Assessment

From 2020-01-04 00:00:00.0 to 2020-02-03 08:13:36.0
 Generated At: 2020-02-03 08:13:37.37

Client Details

Username	alice@
Mac Address	00:0C
IP address	172.1
Location	All Lo
Session ID	00000
Client Operating System	Windo
Client NAC Agent	AnyCo
PRA Enforcement	0
CoA	Recei
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEn
System Name	DESK
System Domain	n/a

System User	admin
User Domain	DESKTOP-I
AV Installed	
AS Installed	
AM Installed	Windows De

Posture Report

Posture Status	Compliant
Logged At	2020-02-03 08:07:50.03

Posture Policy Details

Policy	Name	Enforcement Type	Status	Passed Conditions
Default_AntiMalware_Policy_Win	Any_AM_Installation_Win	Mandatory	Passed	am_inst_v4_ANY_vendor

Push



Refresh



Reset Repeat Counts



Export To ▾

	Time	Status	Details	Rep
✕		<input type="text"/>	▼	
	Feb 03, 2020 08:07:52.05...	✓		
	Feb 03, 2020 08:07:50.03...	ⓘ		0
	Feb 03, 2020 07:13:29.74...	✓		
	Feb 03, 2020 07:13:29.73...	✓		

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

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

ACL URL
DAACL

<#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#

ç-‘é>£æŽ’èš£

ææ-ç-€æ ä¾çš,,è³†è Šå ç æ-¼å çµ,,æ...<é€²è;CEç-‘é>£æŽ’èš£ã€,

ææ%œ—œè©³ç´°çš,,çµç«-å@%å...“è©•ä¼°æ ç <ä»¥å Šå AnyConnectå’CEISEé€²è;CEæ...ésœæŽ’é™ªĩ
ISEçµç«-å@%å...“è©•ä¼°æ“£å¼°æ-“è¼fi¼CEç” æ-¼å%œæœÿå’CEå¼CEæœÿ2.2ã€,

- æ°çä½ éššé

ä, €å€<å, è<å é;CEi¼CEç•¶é... ç½®ä°†å,™ç” éššé æ™,ã€,åœ æçç°ä¾<ä,ĩ¼CEä½ç” é è çµ,,ç-ç-¥

ç, °ä°†æªçæÿ¥FMCä, Šçš,,ésšé ç-ç-¥i¼CEé |-å...^æªçæÿ¥åªªå€<çµ,,ç-ç-¥ç” æ-¼VPNé€£ç.šã€,å°Žè |½è†³
> VPN Remote Accessã€,

Overview Analysis Policies **Devices** Objects AMP Intelligence

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

EmployeeVPN

Enter Description

Connection Profile Access Interfaces Advanced

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

ç,,¶â¼Æî¼Æâ°Žè^â^° **Objects > Object Management > VPN > Group Policy**¼¼Æç,,¶â¼Æé»žé◆,ç,°VPNé...◆ç½®çš„Group Policyã€,

Overview Analysis Policies Devices **Objects** AMP Intelligence

Object Management Intrusion Rules

Group Policy

A Group Policy is a set of attribute and value pairs, stored in a

- Geolocation
- Interface
- Key Chain
- Network
- PKI
- Policy List
- Port
- Prefix List
- RADIUS Server Group
- Route Map
- Security Intelligence
- Sinkhole
- SLA Monitor
- Time Range
- Tunnel Zone
- URL
- Variable Set
- VLAN Tag
- VPN**
- AnyConnect File
- Certificate Map
- Group Policy**
- IKEv1 IPsec Proposal
- IKEv1 Policy
- IKEv2 IPsec Proposal
- IKEv2 Policy

Edit Group Policy

Name:* DfltGrpPolicy

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling: **Allow all traffic**

IPv6 Split Tunneling: **Allow all traffic**

Split Tunnel Network List Type: Standard Access List

Standard Access List:

DNS Request Split Tunneling

DNS Requests: **Send DNS requests**

Domain List:

- è°«ä»½NAT

å◆|ä,€â€<â„è|<â•◆é;Ĉæ~ĩ¼Ĉç•¶VPNä½¿ç””è€...çš,,è¿”â>žæµ◆é‡◆ä½¿ç””éĈè°æçš,,NATæç◆ç>®è
 é|–â...~ĩ¼Ĉæ°çæÿ¥è©²è£◆ç½®çš,,NATè|◆â%#ã€,,â°Žè^â^°Devices >
 NATĩ¼Ĉç,,¶â¼Ĉé»žé◆,Add Ruleä»¥â»°ç««æ–°è|◆â%#ã€,,

The screenshot shows a web-based network management interface. At the top, there is a navigation bar with tabs: Overview, Analysis, Policies, **Devices** (highlighted with a red box), and Objects. Below this is a sub-menu with options: Device Management, **NAT** (highlighted with a red box), VPN, QoS, and Platform. The main content area displays the configuration for a device named **FTD_11**. Underneath the device name, there is a text input field labeled 'Enter Description'. A blue 'Rules' button is visible on the left. Below the button is a 'Filter by Device' dropdown menu. At the bottom, a table header is partially visible with columns: #, Direction, Type, Source Interface Ob..., and Destination Interface. A dropdown arrow is shown next to the text 'NAT Rules Before'.

âœ`é–<â•ÿçš,,è|–çª—ä,ĩ¼Ĉæ°`Interface Objectsé◆ç±ªä,ĩ¼Ĉé◆,æ”#Security
 Zonesã€,,âœ`æœ–ç°ª¼<ä,ĩ¼ĈENATæ◆ç>®æ~â¼žZONE-INSIDEâ°ZONE-OUTSIDEâ»°ç««çš,,ã€,,

Add NAT Rule

NAT Rule:

Insert:

Type:

Enable

Description:

Interface Objects

Translation

PAT Pool

Advanced

Available Interface Objects

- ZONE-INSIDE
- ZONE-OUTSIDE

Add to Source









































Add to Destination

Source Interface Objects (1)

ZONE-INSIDE 

Destination

ZONE-INSIDE

Translation                                        

Edit NAT Rule

NAT Rule:

Manual NAT Rule

Type:

Static

Enabled

Description:

Interface Objects

Translation

PAT Pool

Advanced

Original Packet

Original Source:*

any

Original Destination:

Address

VPN_Subnet

Original Source Port:

Original Destination Port:

Edit NAT Rule

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。