

Konfigurieren des ISE-Status über AnyConnect Remote Access VPN auf FTD

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Konfigurieren](#)
- [Netzwerkdiagramm und Datenverkehrsfluss](#)
- [Konfigurationen](#)
- [FTD/FMC](#)
- [ISE](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie Firepower Threat Defense (FTD) Version 6.4.0 so konfigurieren, dass VPN-Benutzer den Status der Identity Services Engine (ISE) erhalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- AnyConnect Remote Access-VPN
- Konfiguration des Remote Access VPN auf dem FTD
- Identity Services Engine und Statusservices

Verwendete Komponenten

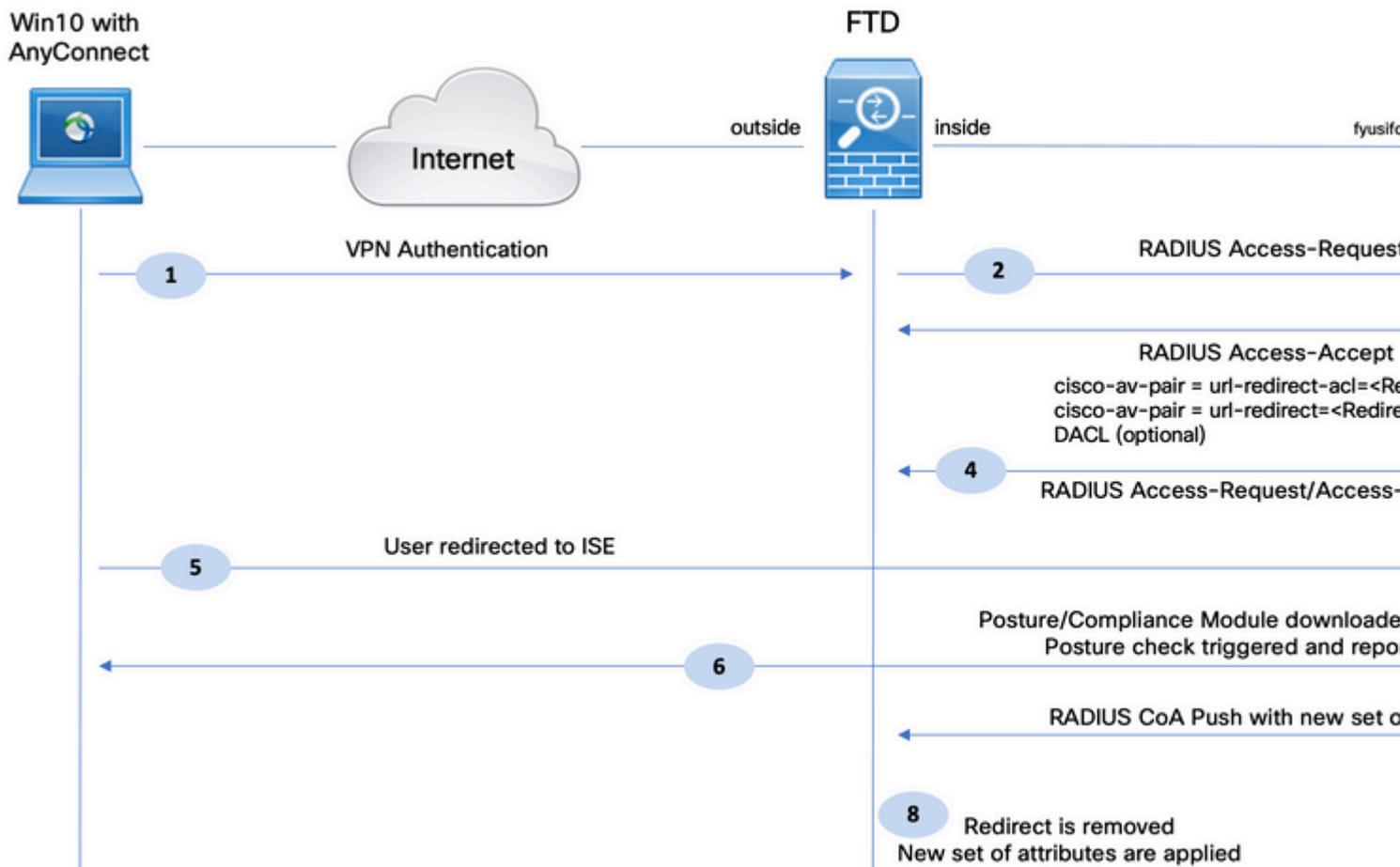
Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco Firepower Threat Defense (FTD) Softwareversion 6.4.0
- Cisco FirePOWER Management Console (FMC) Softwareversion 6.5.0
- Microsoft Windows 10 mit Cisco AnyConnect Secure Mobility Client Version 4.7
- Cisco Identity Services Engine (ISE) Version 2.6 mit Patch 3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm und Datenverkehrsfluss



1. Der Remote-Benutzer verwendet Cisco AnyConnect für den VPN-Zugriff auf den FTD.
2. Der FTD sendet eine RADIUS-Zugriffsanforderung für diesen Benutzer an die ISE.
3. Diese Anforderung erreicht die Richtlinie **FTD-VPN-Posture-Unknown** auf der ISE. Die ISE sendet ein RADIUS Access-Accept mit drei Attributen:
 - **cisco-av-pair = url-redirect-acl=fyusifovredirect** - Dies ist der Name der Zugriffskontrollliste (ACL), der lokal auf dem FTD definiert wird und über den umgeleiteten Datenverkehr entscheidet.
 - **cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp** - Dies ist die URL, zu der der Remote-Benutzer umgeleitet wird.
 - **DACL = PERMIT_ALL_IPV4_TRAFFIC** - herunterladbare ACL Dieses Attribut ist optional. In diesem Szenario ist der gesamte Datenverkehr in DACL zulässig)
4. Wenn DACL gesendet wird, wird RADIUS Access-Request/Access-Accept ausgetauscht, um den Inhalt der DACL herunterzuladen
5. Wenn der Datenverkehr vom VPN-Benutzer mit der lokal definierten ACL übereinstimmt, wird er zum ISE-Client-Bereitstellungsportal umgeleitet. Die ISE stellt das AnyConnect Posture Module und das Compliance Module bereit.
6. Nachdem der Agent auf dem Client-Computer installiert wurde, sucht er automatisch mithilfe von Tests

nach ISE. Wenn die ISE erfolgreich erkannt wurde, werden die Statusanforderungen am Endpunkt überprüft. In diesem Beispiel sucht der Agent nach installierter Anti-Malware-Software. Anschließend wird ein Statusbericht an die ISE gesendet.

7. Wenn die ISE den Statusbericht vom Agenten empfängt, ändert die ISE den Status für diese Sitzung und löst den RADIUS CoA-Typ "Push" mit neuen Attributen aus. Dieses Mal ist der Status bekannt und eine weitere Regel wird getroffen.

- Wenn der Benutzer die Richtlinien erfüllt, wird ein DACL-Name gesendet, der den vollständigen Zugriff ermöglicht.
- Wenn der Benutzer nicht konform ist, wird ein DACL-Name gesendet, der den eingeschränkten Zugriff zulässt.

8. Die FTD entfernt die Umleitung. FTD sendet Access-Request, um DACL von der ISE herunterzuladen. Die jeweilige DACL ist mit der VPN-Sitzung verbunden.

Konfigurationen

FTD/FMC

Schritt 1: Erstellen Sie eine Netzwerkobjektgruppe für ISE- und Problembehebungsserver (falls vorhanden). Navigieren Sie zu **Objekte > Objektverwaltung > Netzwerk**.

The screenshot shows the Cisco ASA configuration interface. The top navigation bar 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 is titled 'Network' and contains a list of network objects. A modal dialog titled 'Edit Network Object' is open, showing the configuration for a new network object. The 'Name' field is set to 'ISE_PSN|', the 'Network' type is 'Host', and the IP address is '192.168.15.14'. The 'Allow Overrides' checkbox is unchecked.

Name
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
IPv4-Private-192.168.0.0-16
IPv4-Private-All-RFC1918
IPv6-IPv4-Mapped
IPv6-Link-Local
IPv6-Private-Unique-Local-Addresses
IPv6-to-IPv4-Relay-Anycast

Edit Network Object

Name: ISE_PSN|

Description:

Network: Host Range Network

192.168.15.14

Allow Overrides:

Schritt 2: Umleitungs-ACL erstellen. Navigieren Sie zu **Objekte > Objektverwaltung > Zugriffstabelle > Erweitert**. Klicken Sie auf **Add Extended Access List (Erweiterte Zugriffstabelle hinzufügen)**, und geben Sie den Namen der Umleitungszugriffskontrollliste an. Dieser Name muss mit dem ISE-Autorisierungsergebnis übereinstimmen.

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

Schritt 3: ACL-Umleitungseinträge hinzufügen. Klicken Sie auf die Schaltfläche **Hinzufügen**. Blockieren Sie den Datenverkehr zu DNS, ISE und zu den Wiederherstellungsservern, um diese von der Umleitung auszuschließen. Lässt den restlichen Verkehr zu, löst dies eine Umleitung aus (ACL-Einträge können bei Bedarf spezifischer sein).

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

Add to Source

Add to Destination

Source Networks (1)

any-ipv4

Destination

ISE_

Enter an IP address

Add

Enter an

Edit Extended Access List Object

Name

Entries (4)

Sequence	Action	Source	Source Port	Destination	Desti
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

Schritt 4: ISE PSN-Knoten hinzufügen Navigieren Sie zu **Objekte > Objektverwaltung > RADIUS-Servergruppe**. Klicken Sie auf **RADIUS-Servergruppe hinzufügen**, geben Sie den Namen ein, aktivieren Sie die Kontrollkästchen, und klicken Sie auf das **Pluszeichen**.

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

Schritt 5: Geben Sie im geöffneten Fenster ISE PSN IP address (ISE-PSN-IP-Adresse), RADIUS Key (RADIUS-Schlüssel) ein, wählen Sie **Specific Interface (Spezifische Schnittstelle)** und dann eine Schnittstelle aus, von der ISE erreichbar ist (diese Schnittstelle wird als Quelle für RADIUS-Datenverkehr

verwendet), und wählen Sie dann **Redirect ACL (ACL umleiten)** aus.

New RADIUS Server

IP Address/Hostname:* 192.168.15.13

Authentication Port:* 1812

Key:*

Confirm Key:*

Accounting Port: 1813

Timeout: 10

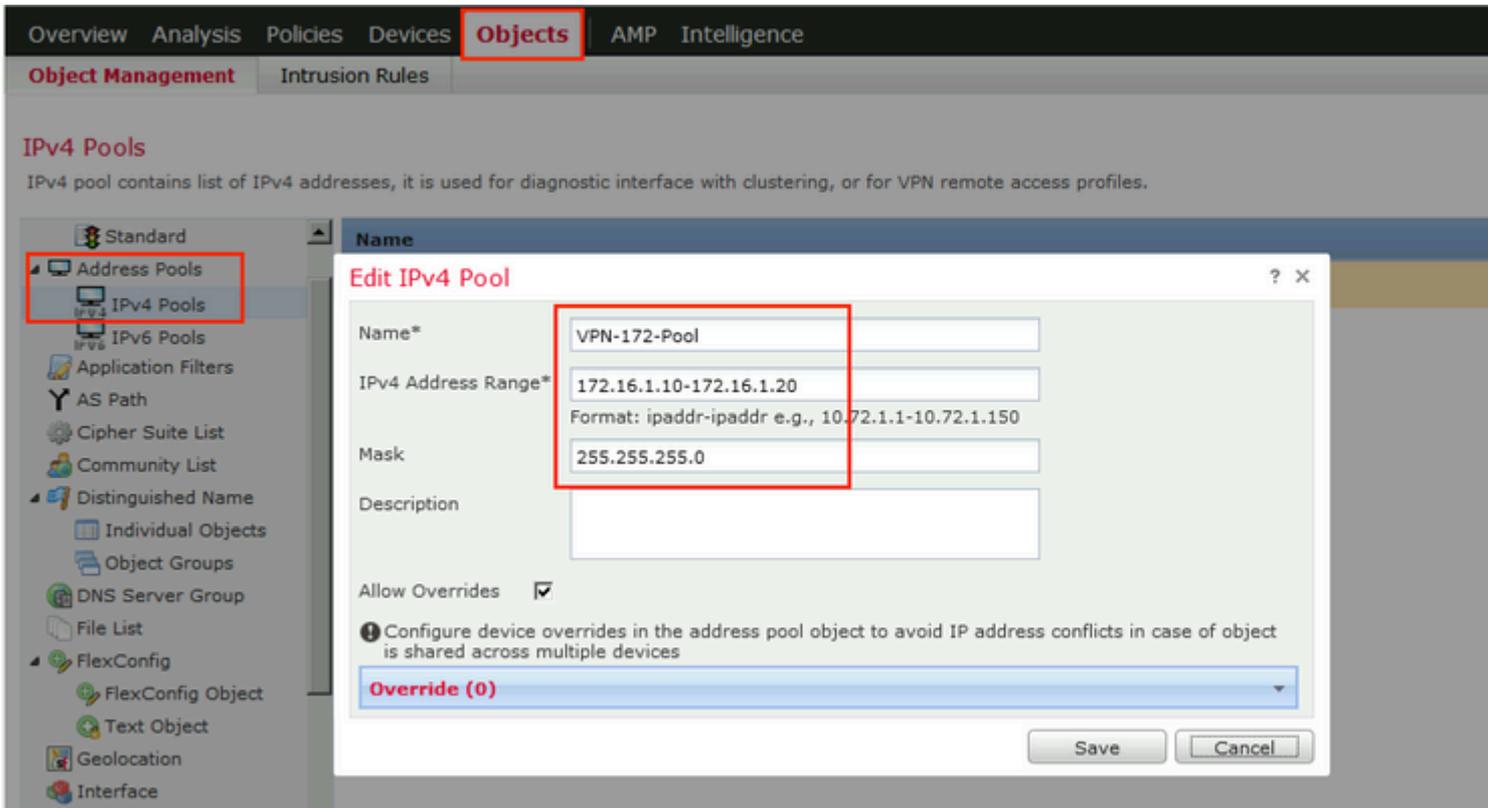
Connect using: Routing Specific Interface ⓘ

ZONE-INSIDE

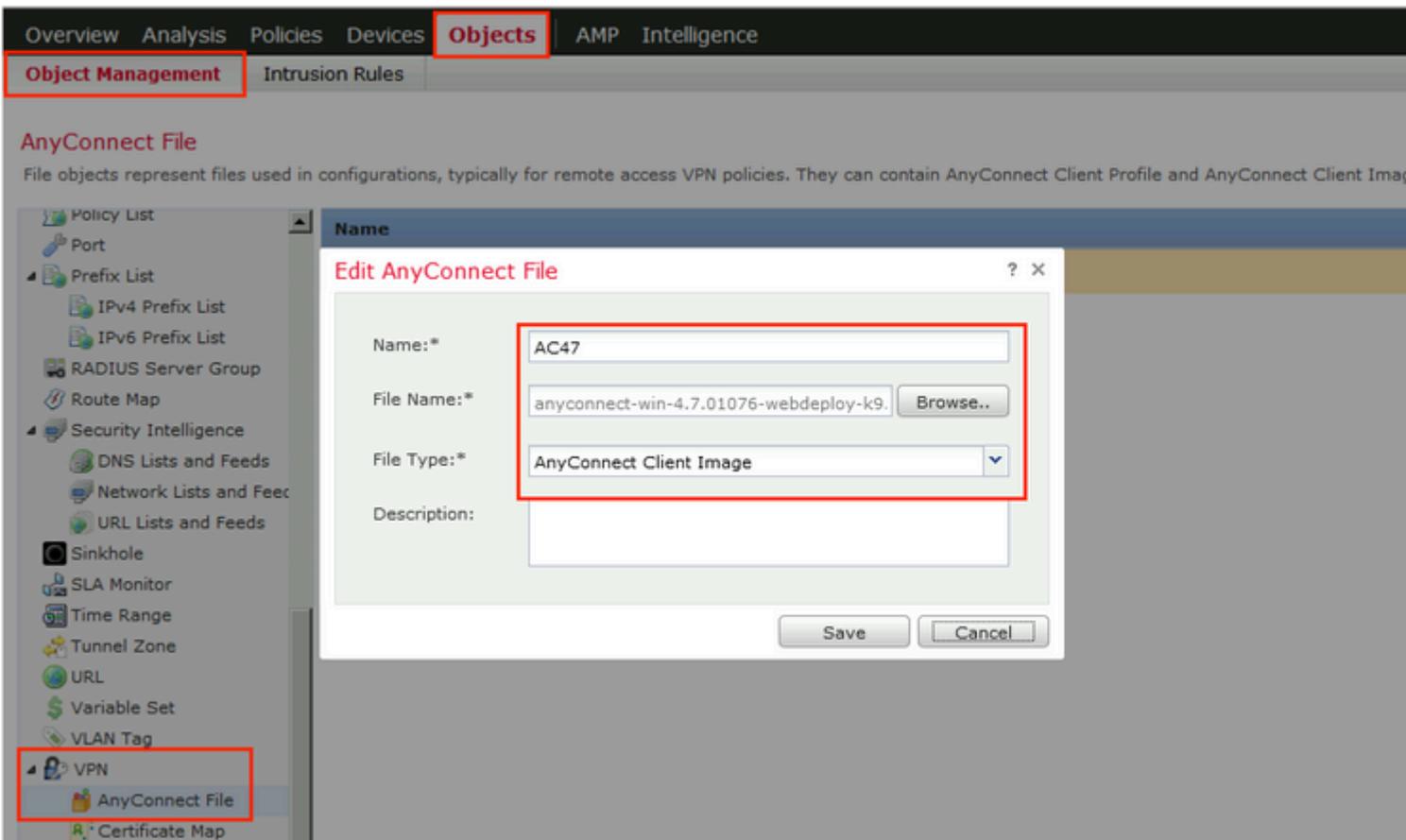
Redirect ACL: fyusifovredirect

Save

Schritt 6: Erstellen eines Adresspools für VPN-Benutzer Navigieren Sie zu **Objekte > Objektverwaltung > Adresspools > IPv4-Pools**. Klicken Sie auf **Add IPv4 Pools** (IPv4-Pools hinzufügen), und geben Sie die Details ein.



Schritt 7. AnyConnect-Paket erstellen. Navigieren Sie zu **Objects > Object Management > VPN > AnyConnect File**. Klicken Sie auf **AnyConnect-Datei hinzufügen**, geben Sie den Paketnamen an, laden Sie das Paket von [Cisco Software Download](#) herunter, und wählen Sie **AnyConnect Client Image** File Type aus.



Schritt 8: Navigieren Sie zu **Zertifikatobjekte > Objektverwaltung > PKI > Zertifikatregistrierung**. Klicken Sie auf **Add Certificate Enrollment (Zertifikatregistrierung hinzufügen)**, geben Sie einen Namen ein, und wählen Sie in Enrollment Type (Registrierungstyp) die Option **Self Signed Certificate (Selbstsigniertes Zertifikat)** aus. Klicken Sie auf die Registerkarte Zertifikatsparameter, und geben Sie CN an.

The screenshot displays the Fortinet management interface. At the top, the navigation menu includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' tab is active, and 'Object Management' is highlighted. Below this, the 'Cert Enrollment' section is visible, with a description: 'A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing activities occur in your Private Key Infrastructure (PKI)'. The left sidebar shows a tree view of configuration objects, with 'PKI' and 'Cert Enrollment' highlighted. The main window shows the 'Add Cert Enrollment' dialog box. The 'Name*' field is filled with 'vpn-cert'. The 'Enrollment Type' dropdown is set to 'Self Signed Certificate'. A warning message is displayed: '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.' The 'Certificate Parameters' tab is selected. At the bottom of the dialog, there is an 'Allow Overrides' checkbox which is unchecked. 'Save' and 'Cancel' buttons are at the bottom right.

Add Cert Enrollment

Name*

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN:

Use Device Hostname as FQDN

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

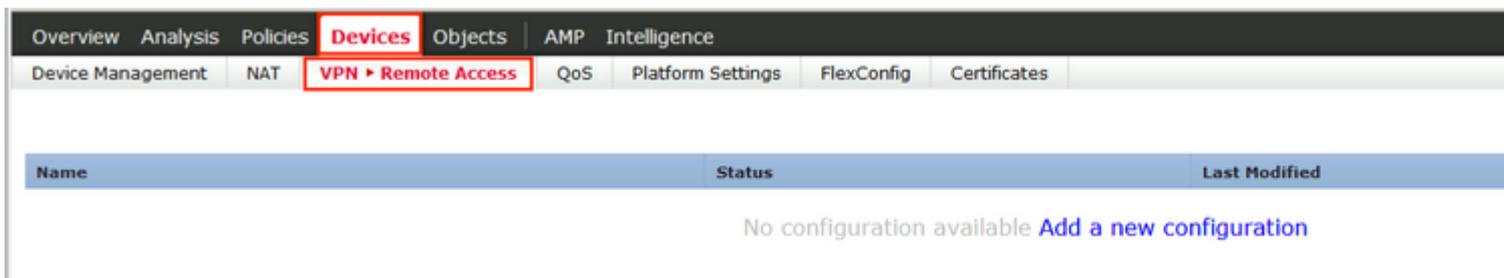
Country Code (C):

Email (E):

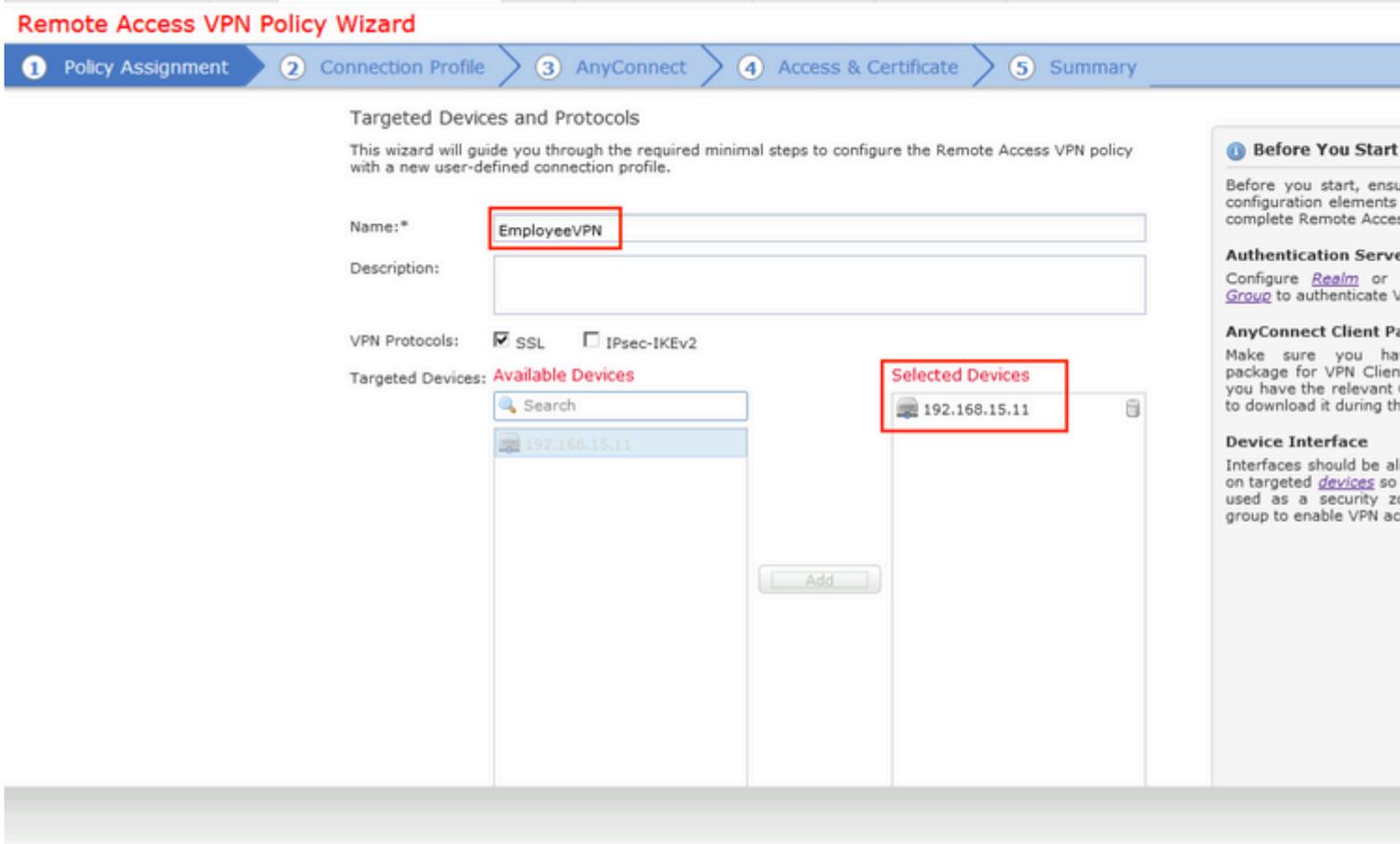
Include Device's Serial Number

Allow Overrides

Schritt 9. Starten des VPN-Assistenten für Remote-Zugriff Navigieren Sie zu **Geräte > VPN > Remotezugriff**, und klicken Sie auf **Hinzufügen**.



Schritt 10. Geben Sie den Namen an, aktivieren Sie SSL als VPN-Protokoll, wählen Sie FTD aus, das als VPN-Konzentrator verwendet wird, und klicken Sie auf **Weiter**.



Schritt 11. Geben Sie den Namen des **Verbindungsprofils** an, wählen Sie **Authentication/Accounting Servers** aus, wählen Sie den zuvor konfigurierten Adresspool aus, und klicken Sie auf **Next (Weiter)**.

Hinweis: Wählen Sie nicht den Autorisierungsserver aus. Es löst zwei Zugriffsanfragen für einen einzelnen Benutzer aus (einmal mit dem Benutzerkennwort und das zweite Mal mit dem Kennwort *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: (Realm or RADIUS)
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](#)

Schritt 12: Wählen Sie das zuvor konfigurierte AnyConnect-Paket aus, und klicken Sie auf **Weiter**.

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

Schritt 13: Wählen Sie die Schnittstelle aus, von der der VPN-Datenverkehr erwartet wird, wählen Sie die zuvor konfigurierte **Zertifikatregistrierung aus**, und klicken Sie auf **Weiter**.

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.

Schritt 14: Überprüfen Sie die Übersichtsseite, und klicken Sie auf **Fertig stellen**.

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 allow VPN traffic on all targeted

1 **NAT Exemption**
If NAT is enabled on the target, you must define a [NAT Policy](#) for VPN traffic.

1 **DNS Configuration**
To resolve hostname special characters, configure DNS Servers or CA Servers, configure a [FlexConfig Policy](#) on the target.

1 **Port Configuration**
SSL will be enabled on port 443. Please ensure that these ports are open in [NAT Policy](#) or other security policies when deploying the configuration.

⚠ **Network Interface Configuration**
Make sure to add interface for devices to SecurityZone of 'OUTSIDE'

Schritt 15: Konfiguration in FTD bereitstellen. Klicken Sie auf **Deploy (Bereitstellen)**, und wählen Sie **FTD aus**, das als VPN-Konzentrator verwendet wird.

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

Selected devices: 1

Deploy

ISE

Schritt 1: Ausführen von Statusaktualisierungen. Navigieren Sie zu **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

▼ 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

Schritt 2: Compliance-Modul hochladen. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Clientbereitstellung > Ressourcen**. Klicken Sie auf **Hinzufügen**, und wählen Sie **Agenten-Ressourcen von der Cisco Website** aus.

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

Schritt 3: Laden Sie AnyConnect über [Cisco Software Download herunter](http://cisco.com/go/anyconnect), und laden Sie es dann auf die ISE hoch. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Clientbereitstellung > Ressourcen**.

Klicken Sie auf **Hinzufügen**, und wählen Sie **Agent-Ressourcen von lokalem Datenträger aus**. Wählen Sie **Cisco Provided Packages** unter **Category (Kategorie)** aus, wählen Sie AnyConnect Package von der lokalen Festplatte aus, und klicken Sie auf **Submit (Senden)**.

Agent Resources From Local Disk

Category

 ⓘ

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

Schritt 4: AnyConnect-Statusprofil erstellen. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Clientbereitstellung > Ressourcen**.

Klicken Sie auf **Hinzufügen**, und wählen Sie AnyConnect **Posture Profile** aus. Geben Sie den Namen und das Posture Protocol ein.

Setzen Sie unter ***Server name rules put*** (Servernamensregeln) eine beliebige Dummy-IP-Adresse unter den **Discovery-Host**.

* 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 the max time limit is reached

Schritt 5: Navigieren Sie zu **Policy > Policy Elements > Results > Client Provisioning > Resources**, und erstellen Sie **AnyConnect Configuration**. Klicken Sie auf **Hinzufügen**, und wählen Sie **AnyConnect Configuration aus**. Wählen Sie **AnyConnect-Paket**, geben Sie den Konfigurationsnamen an, wählen Sie **Compliance Module aus**, aktivieren Sie das Diagnose- und Reporting-Tool, wählen Sie **Statusprofil aus**, und klicken Sie auf **Speichern**.

* 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

Schritt 6: Navigieren Sie zu **Policy > Client Provisioning**, und erstellen Sie **Client Provisioning Policy**. Klicken Sie auf **Bearbeiten** und wählen Sie dann **Regel oben einfügen**, geben Sie einen Namen an, wählen Sie Betriebssystem aus, und wählen Sie die AnyConnect-Konfiguration aus, die im vorherigen Schritt erstellt wurde.

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 Supplciant 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

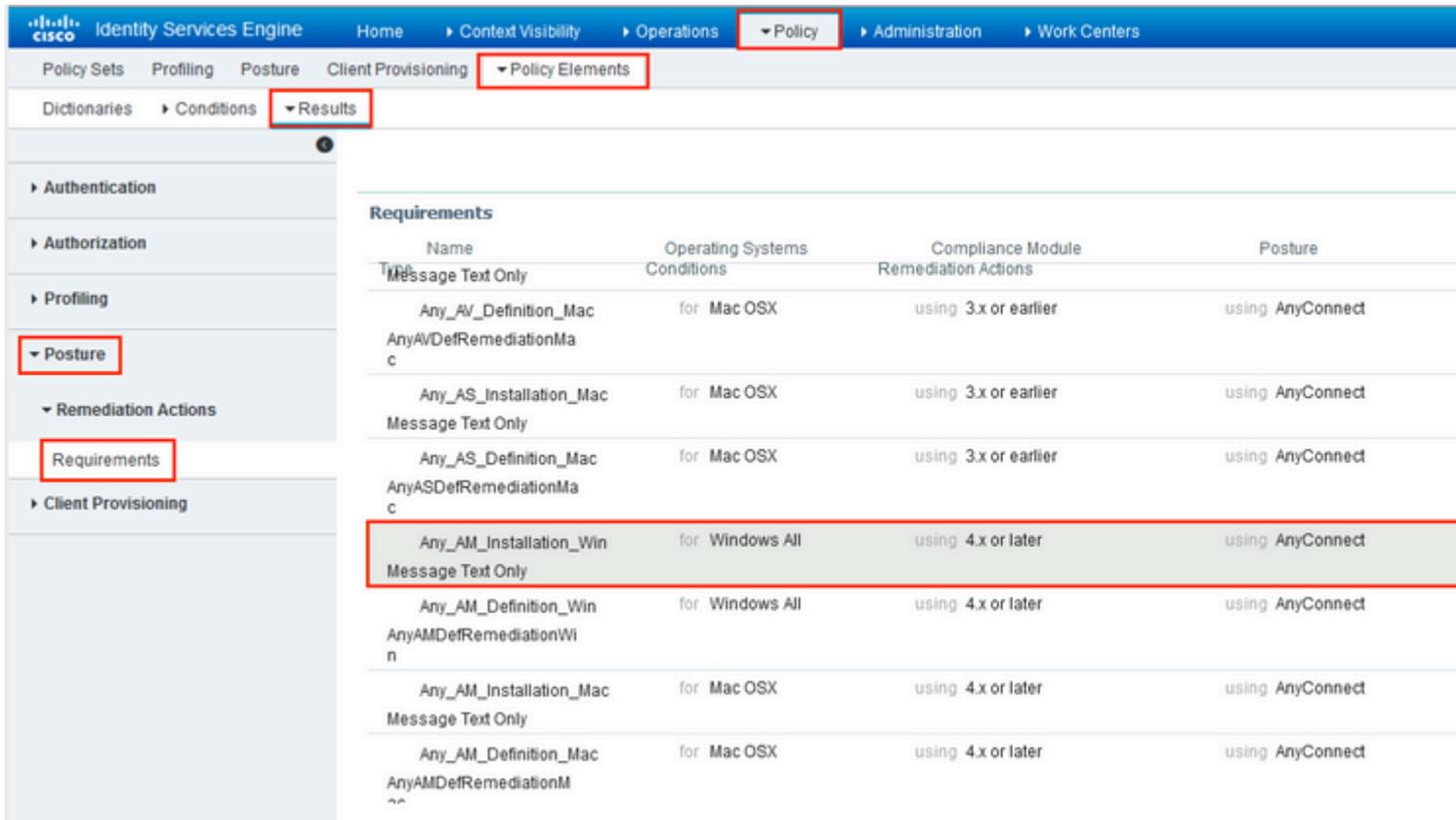
Schritt 7. Erstellen Sie einen Status unter **Richtlinie > Richtlinienelemente > Bedingungen > Status > Anti-Malware-Status**. In diesem Beispiel wird die vordefinierte Option "ANY_am_win_inst" verwendet.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. The 'Policy' menu is expanded to show 'Policy Elements'. Under 'Policy Elements', the 'Posture' sub-menu is expanded to show 'Anti-Malware Condition'. The main content area displays 'Anti-Malware Conditions' with a table of conditions. The table has columns for 'Name' and 'Description'. The first row is 'ANY_am_win_inst' with the description 'Any AM installation check on W'. Other rows include 'ANY_am_win_def', 'ANY_am_mac_inst', and 'ANY_am_mac_def'.

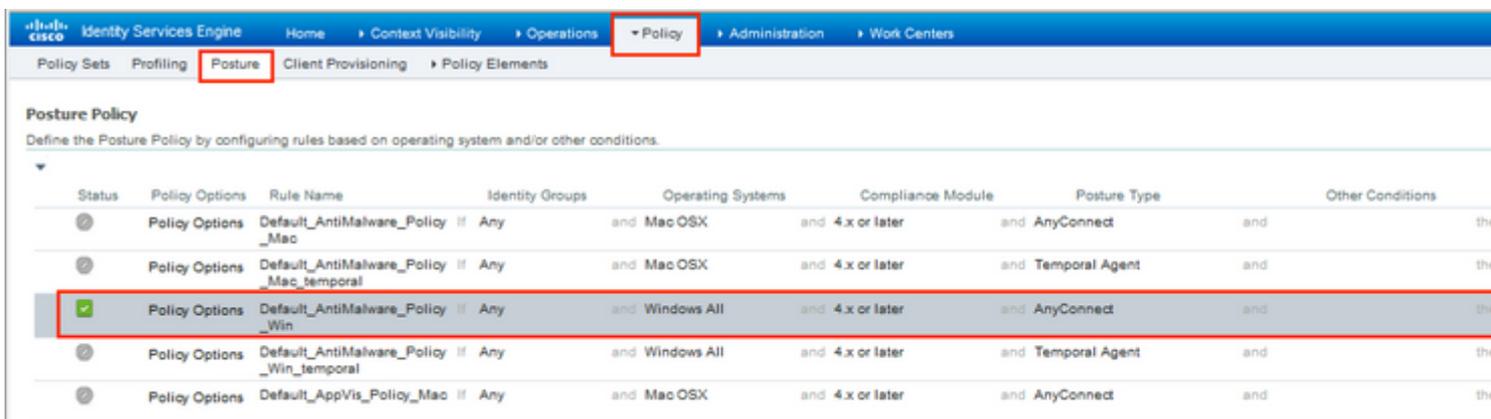
Name	Description
ANY_am_win_inst	Any AM installation check on W
ANY_am_win_def	Any AM definition check on W
ANY_am_mac_inst	Any AM installation check on M
ANY_am_mac_def	Any AM definition check on M

Schritt 8: Navigieren Sie zu **Policy > Policy Elements > Results > Posture > Remediation Actions**, und erstellen Sie **Posture Remediation**. In diesem Beispiel wird sie übersprungen. Die Behebungsaktion kann eine Textnachricht sein.

Schritt 9. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Status > Anforderungen**, und erstellen Sie **Statusanforderungen**. Die vordefinierte Anforderung Any_AM_Installation_Win wird verwendet.



Schritt 10. Erstellen Sie Statusrichtlinien unter **Richtlinien > Status**. Es wird eine Standard-Statusrichtlinie für alle AntiMalware Check for Windows-Betriebssysteme verwendet.



Schritt 11. Navigieren Sie zu **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**, und erstellen Sie DACLs für verschiedene Statusstatus.

In diesem Beispiel:

- Status: Unbekannte DACLs ermöglichen den Datenverkehr zu DNS-, PSN-, HTTP- und HTTPS-Datenverkehr.
- Nicht konforme DACL mit Status - verweigert den Zugriff auf private Subnetze und lässt nur Internetdatenverkehr zu.
- Alle DACLs zulassen: Der gesamte Datenverkehr wird für den Status "Status konform" zugelassen.

[Downloadable ACL List > PostureNonCompliant1](#)

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 List > New Downloadable ACL](#)

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

Schritt 12: Erstellen Sie drei Autorisierungsprofile für den Status "Status unbekannt", "Status nicht konform" und "Status konform". Navigieren Sie dazu zu **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Wählen Sie im Profil **Posture Unknown (Status unbekannt)** die Option **Posture Unknown DACL (Status unbekannt - DACL)**, aktivieren Sie die Option **Web Redirection (Webumleitung)**, wählen Sie **Client Provisioning (Clientbereitstellung)** aus, geben Sie den Namen der Umleitungszugriffskontrollliste (die für FTD konfiguriert ist) an, und wählen Sie das Portal aus.

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

Wählen Sie im Profil **Posture NonCompliant (Status nicht konform)** die Option **DACL** aus, um den Zugriff auf das Netzwerk einzuschränken.

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

Wählen Sie im Profil "**Posture Compliant**" die Option **DACL** aus, um den vollständigen Zugriff auf das Netzwerk zu ermöglichen.

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

Schritt 13: Erstellen Sie Autorisierungsrichtlinien unter **Richtlinie > Richtliniensätze > Standard > Autorisierungsrichtlinie**. Als Bedingung werden Posture Status und VNP TunnelGroup Name verwendet.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The 'Policy' menu is expanded, and the 'Authorization Policy (18)' section is selected. Three authorization rules are visible:

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

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Auf der ISE ist der erste Verifizierungsschritt RADIUS Live Log. Navigieren Sie zu **Operations > RADIUS Live Log (Vorgänge > RADIUS-Live-Protokoll)**. Hier wird der Benutzer Alice verbunden und die erwartete Autorisierungsrichtlinie ausgewählt.

The screenshot shows the RADIUS Live Log page in Cisco ISE. The table below displays the log entries:

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Pr...	Authentica...	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...	

Die Autorisierungsrichtlinie FTD-VPN-Posture-Unknown wird zugeordnet, und das FTD-VPN-Profil wird

an FTD gesendet.

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

Statusstatus ausstehend.

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

Im Ergebnisabschnitt wird angezeigt, welche Attribute an FTD gesendet werden.

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

Auf FTD, um VPN-Verbindung zu überprüfen, SSH auf die Box, führen Sie **System-Support-Diagnose-CLI** und dann **zeigen vpn-sessiondb Detail anyconnect**. Überprüfen Sie anhand dieser Ausgabe, ob die von der ISE gesendeten Attribute für diese VPN-Sitzung angewendet werden.

```
<#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#

Richtlinien für die Client-Bereitstellung können überprüft werden. Navigieren Sie zu **Operations > Reports > Endpoints and Users > Client Provisioning**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Operations' menu is expanded, showing 'RADIUS', 'Threat-Centric NAC Live Logs', 'TACACS', 'Troubleshoot', and 'Adaptive Network Control'. The 'Reports' section is active, displaying 'Client Provisioning' for the period 'From 2020-02-03 00:00:00.0 to 2020-02-03 08:14:07.0'. The left sidebar shows 'Export Summary', 'My Reports', 'Reports', 'Audit', 'Device Administration', 'Diagnostics', 'Endpoints and Users', 'Authentication Summary', 'Client Provisioning', and 'Current Active Sessions'. The main content area shows a table with columns: 'Logged At', 'Server', 'Event', 'Identity', and 'Endpoint ID'. A single row is visible with the following data: '2020-02-03 08:08:4...', 'fysifov-26-3', 'Client provisioning succeeded', 'alice@training.example.com', and '00:0C:29:5C:5A:98'. The 'Event' cell is highlighted with a red box.

Logged At	Server	Event	Identity	Endpoint ID
2020-02-03 08:08:4...	fysifov-26-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:98

Statusbericht, der von AnyConnect gesendet wurde, kann überprüft werden. Navigieren Sie zu **Vorgänge > Berichte > Endpunkte und Benutzer > Statusüberprüfung nach Endpunkt**.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. At the top, the navigation bar includes the Cisco logo, the text 'Identity Services Engine', and links for 'Home', 'Context Visibility', and a dropdown menu. Below this, a secondary navigation bar contains links for 'RADIUS', 'Threat-Centric NAC Live Logs', 'TACACS', and 'Troubleshooting'. On the left side, a vertical navigation menu is displayed with several categories: 'Export Summary', 'My Reports', 'Reports', 'Audit', 'Device Administration', 'Diagnostics', 'Endpoints and Users', and a list of reports including 'Authentication Summary', 'Client Provisioning', 'Current Active Sessions', 'External Mobile Device...', 'Manual Certificate Pro...', 'PassiveID', and 'Posture Assessment by ...'. The 'Endpoints and Users' category and the 'Posture Assessment by ...' report are highlighted with red boxes. The main content area on the right shows the details for the 'Posture Assessment by Endpoints' report, including the date range 'From 2020-02-03 00:00:00.0 to 2020-02-03 00:00:00.0' and the number of reports exported in the last 7 days, which is 0. Below this, a table is partially visible with a header 'Logged At' and a data row showing the timestamp '2020-02-03 08:07:5...'. A horizontal scrollbar is located below the table.

Um weitere Details zum Statusbericht anzuzeigen, klicken Sie auf **Details**.

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

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

Nachdem der Bericht über die ISE eingegangen ist, wird der Status aktualisiert. In diesem Beispiel ist der Status "konform", und der CoA-Push wird mit einer neuen Gruppe von Attributen ausgelöst.



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

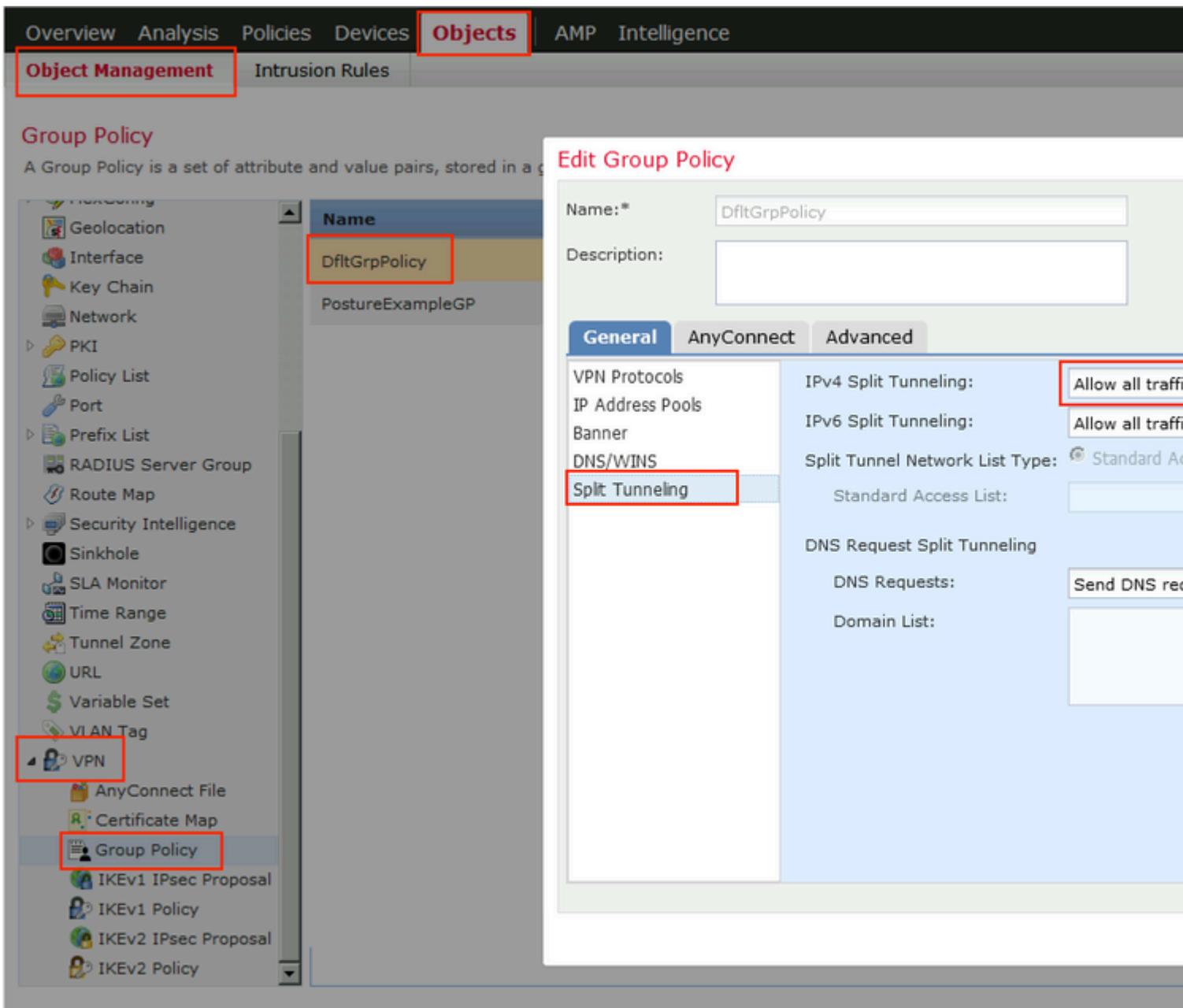
Eines der häufigsten Probleme, wenn es einen Split-Tunnel konfiguriert ist. In diesem Beispiel wird die Standardgruppenrichtlinie verwendet, die den gesamten Datenverkehr tunnelt. Wenn nur bestimmter Datenverkehr getunnelt wird, müssen zusätzlich zum Datenverkehr zur ISE und zu anderen internen Ressourcen auch AnyConnect-Tests (enroll.cisco.com und Discovery Host) durch den Tunnel geleitet werden.

Um die Tunnelrichtlinie auf FMC zu überprüfen, müssen Sie zunächst prüfen, welche Gruppenrichtlinie für die VPN-Verbindung verwendet wird. Navigieren Sie zu **Geräte > VPN-Remotezugriff**.

The screenshot shows the Cisco FMC web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this, there are sub-menus for 'Device Management', 'NAT', 'VPN > Remote Access', 'QoS', 'Platform Settings', 'FlexConfig', and 'Certificates'. The main content area is titled 'EmployeeVPN' and has a sub-header 'Enter Description'. There are three tabs: 'Connection Profile', 'Access Interfaces', and 'Advanced'. Below the tabs is a table with three columns: 'Name', 'AAA', and 'Group Policy'. The table contains two rows: 'DefaultWEBVPNGroup' and 'EmployeeVPN'. The 'EmployeeVPN' row is highlighted with a red box around the name and another red box around the 'DfltGrpPolicy' link in the 'Group Policy' column.

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

Navigieren Sie anschließend zu **Objects > Object Management > VPN > Group Policy**, und klicken Sie auf **Group Policy** configured for VPN (Für VPN konfigurierte **Gruppenrichtlinie**).



- Identitäts-NAT

Ein weiteres häufiges Problem, wenn der Rückverkehr von VPN-Benutzern mithilfe einer falschen NAT-Eingabe umgewandelt wird. Um dieses Problem zu beheben, muss die Identitäts-NAT in der richtigen Reihenfolge erstellt werden.

Überprüfen Sie zunächst die NAT-Regeln für dieses Gerät. Navigieren Sie zu **Devices > NAT**, und klicken Sie dann auf **Add Rule (Regel hinzufügen)**, um eine neue Regel zu erstellen.

Overview Analysis Policies **Devices** Objects

Device Management **NAT** VPN ▼ QoS Plat

FTD_11

Enter Description

Rules

 Filter by Device

#	Direction	Type	Source Interface Ob...	Destina Interfa
▼ NAT Rules Before				

Wählen Sie im geöffneten Fenster auf der Registerkarte **Interface Objects (Schnittstellenobjekte)** die Option **Security Zones (Sicherheitszonen)**. In diesem Beispiel wird der NAT-Eintrag von **ZONE-INSIDE** zu **ZONE-OUTSIDE** erstellt.

Add NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- ZONE-INSIDE
- ZONE-OUTSIDE

Source Interface Objects (1)	Destination
<input checked="" type="checkbox"/> ZONE-INSIDE	<input checked="" type="checkbox"/> ZONE-INSIDE

Wählen Sie auf der Registerkarte **Translation** (Übersetzung) die Originalpaketdetails und die übersetzten Paketdetails aus. Da es sich um Identity NAT handelt, bleiben Quelle und Ziel unverändert:

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:

Aktivieren Sie auf der Registerkarte **Erweitert** die Kontrollkästchen, wie in dieser Abbildung dargestellt:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.