Cisco ISE Posture para VPN de Acceso Remoto con Cisco Secure Client

Comunidad de Cisco

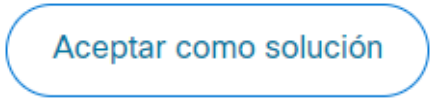
Adrián Lira – Team Captain
Javier Acevedo – Technical Consulting Engineer

Jueves 7 de noviembre de 2024

Conecte, Interactúe, ¡Colabore!

Soluciones

Ayuda a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución” u otórgales un voto de utilidad.



Votos de utilidad

¡Resalta el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios. ¡Reconoce su esfuerzo!

Premios Spotlight Awards

¡Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros!

Los premios Spotlight Awards se otorgan trimestralmente para reconocer a los miembros más destacados.

Conoce a los ganadores de Mayo-Julio 2024

¡Ahora también puedes nominar a un candidato! Haga clic aquí

Nuestros expertos

Adrián Lira

Team Captain

Es Ingeniero egresado del Instituto Politécnico Nacional bajo la especialidad en Comunicaciones y Electrónica impartida en ESIME.

Se unió a Cisco en 2019 al equipo de AAA como TAC Engineer certificado en CCNA y DEVNET ayudando a la resolución de casos de la plataforma ISE (Identity Services Engine) y sus diversas integraciones.

Actualmente se desempeña como capitán del equipo atendiendo casos complejos, escalaciones y documentando artículos de configuración y troubleshooting.

Nuestros expertos

Javier Acevedo

Technical Consulting Engineer

Es Ingeniero en Comunicaciones y Electrónica, egresado del Instituto Politécnico Nacional. Anteriormente trabajó como Ingeniero de soporte en Megacable (MCM Telecom) dentro del Centro de Control de la red.

En 2022 se unió a Cisco como Technical Consulting Engineer, obtuvo las certificaciones de CCNA y DEVNET. A continuación, comenzó a trabajar en el equipo de VPN convirtiéndose en experto en las tecnologías como AnyConnect, DMVPN, GETVPN, FlexVPN, etc.

Actualmente se encuentra trabajando, dando soporte a clientes con problemas en estas tecnologías específicas y apoya a la creación de contenido de calidad para nuestros clientes.

slido

Join at

slido.com

#2535 244

Cisco ISE Posture para VPN de Acceso Remoto con Cisco Secure Client

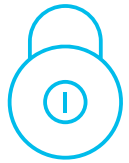
En este webinar...

Exploraremos cómo integrar Cisco Identity Services Engine (ISE) con Cisco Secure Client para planificar y asegurar el cumplimiento de dispositivos mediante un enfoque de postura en conexiones VPN de acceso remoto.

Aprenderán cómo Cisco ISE puede mejorar la seguridad evaluando el estado de los dispositivos que se conectan a la red, asegurando que solo aquellos que cumplan con las políticas establecidas puedan acceder.

También abordaremos técnicas de solución de problemas para optimizar la integración.

Agenda



1. Introducción a Cisco ISE y Cisco Secure Client
2. Descripción y funcionamiento de Posture
3. Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment
4. Configuración básica
   - ISE: Políticas de provisionamiento y autorización
   - VPN: Acceso Remoto con Cisco Secure Client
5. Demo
6. Comprobación: Monitoreo y Reportes
7. Mejores Prácticas y Troubleshooting

Introducción a Cisco ISE y Cisco Secure Client

Introducción a Cisco ISE

Cisco Identity Services Engine (ISE) es una Plataforma centralizada de seguridad diseñada para la implementación de políticas de acceso. Las bases de Cisco ISE son la Autenticación, Autorización y Accounting (AAA).

Entre otras características se tienen:

- Evaluación del estado de Posture
- Segmentación de Red (TrustSec, SGTs)
- Visibilidad y Control (Context Visibility, Profiling)
- Diversidad de integraciones Active Directory, Pxgrid, Passive ID, etc.

Introducción a Cisco Secure Client VPN Acceso Remoto

Cisco Secure Client, antes Cisco AnyConnect, es una solución basada en módulos cuya función principal es garantizar acceso seguro a redes empresariales remotamente con el módulo principal VPN core, o localmente con el módulo NAM (Network Access Manager).

Entre otras características se tienen:

- Evaluación de Posture
- Inclusión de módulos para visibilidad (Secure Endpoint, AMP)
- Autenticación Multifactor

Descripción y funcionamiento de Posture

Active poll

0

Join at

slido.com

#2535 244

¿Cuál es el rol principal de Cisco ISE en un entorno de acceso remoto por VPN?

a) Gestionar conexiones VPN

0%

b) Evaluar la postura de los dispositivos y hacer cumplir las políticas de red

0%

c) Proteger los dispositivos finales mediante firewalls

0%

d) Proporcionar autenticación multifactor para los usuarios de VPN

0%

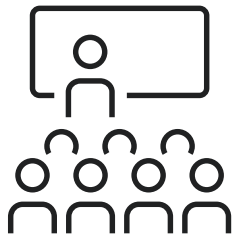
Descripción y funcionamiento de ISE Posture

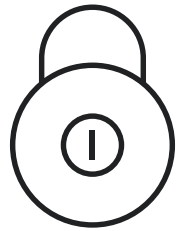
ISE Posture

La "postura" en Cisco ISE se refiere a la evaluación y verificación del estado de seguridad de los dispositivos antes y durante su acceso a la red

Asegurar acceso

Es una funcionalidad para asegurar que solo dispositivos que cumplen con las políticas de seguridad de la organización puedan acceder a los recursos de la red corporativa



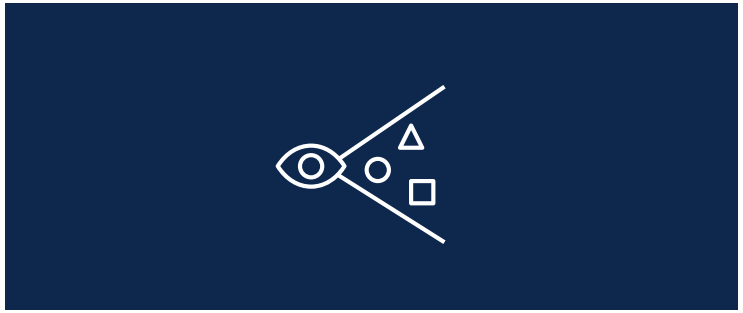


Interacción entre Cisco ISE y Cisco Secure Client para Posture-Assessment

Interacción entre Cisco ISE y Secure Client

Cisco ISE y Secure Client se pueden implementar para la evaluación de Posture, garantizando así:

Conexión remota segura



Escaneo y cumplimiento de políticas de Posture

Acceso a la Red de acuerdo con el estado de Posture

ISE Posture VS Secure Firewall Posture (Hostscan)

Alcance

ISE Posture: Es más amplio y centralizado, puede aplicarse a diferentes tipos de acceso a la red (cableado, inalámbrico, VPN).

Secure Firewall Posture: Está específicamente diseñado para evaluar la postura de dispositivos en conexiones VPN.

Funcionalidad de Remediación

ISE Posture: Capacidades amplias de remediación y puede integrarse con soluciones de gestión de parches y actualizaciones de una amplia variedad de productos.

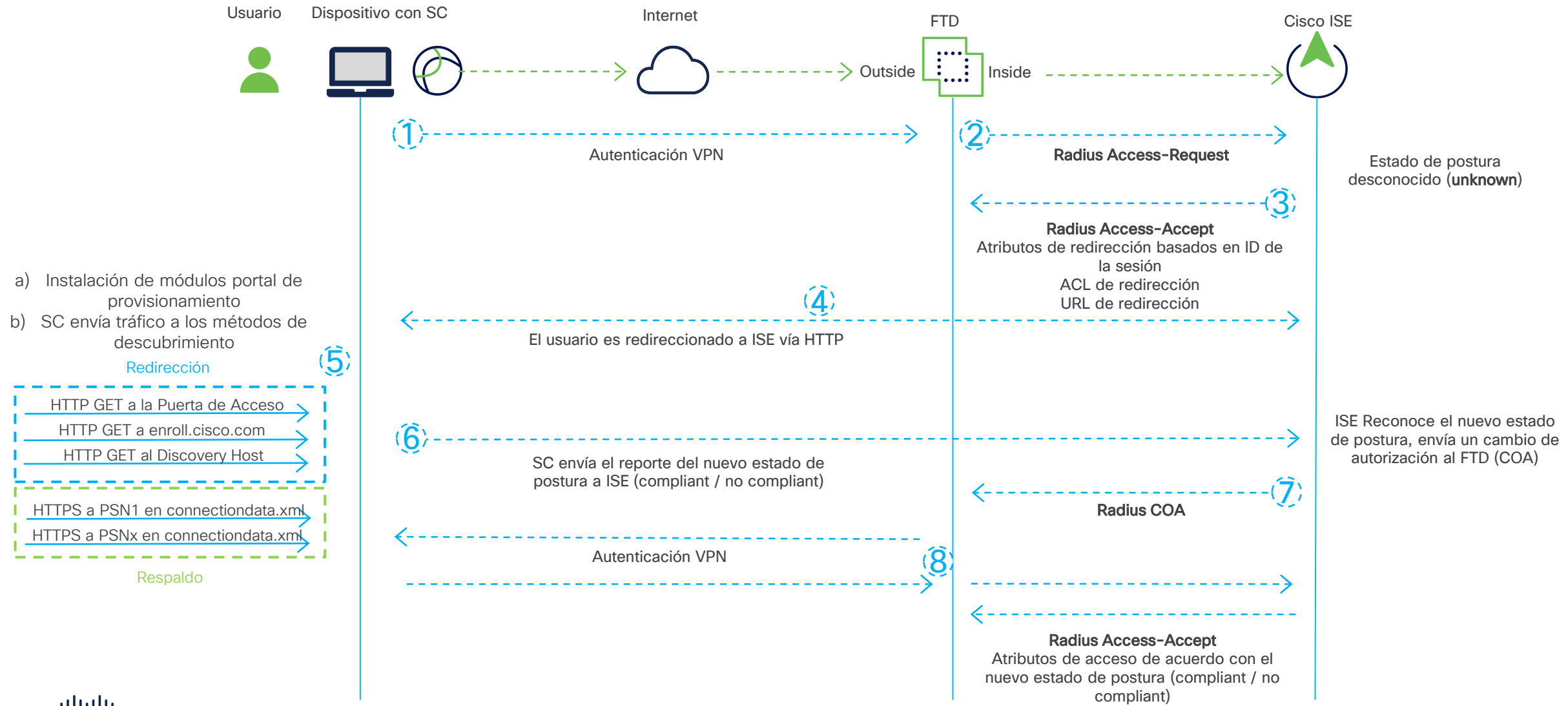
Secure Firewall Posture: Enfocado en permitir o denegar el acceso basado en la evaluación de postura, con opciones limitadas de remediación.

Catálogo

ISE Posture: Incluye una amplia variedad de condiciones de postura como, cifrado de disco, manejo de parches, backup, etc.

Secure Firewall Posture: Tiene condiciones de postura limitadas, antimalware, firewall, ip, certificados.

Flujo de Posture ISE-Secure Client con Redirección



Active poll

0

Join at

slido.com

#2535 244

¿Qué acción se toma si un usuario no cumple con los requisitos de postura en Cisco ISE durante el acceso a la red?

a) Se bloquea el acceso a la red completamente

0%

b) Se aplica una accion de remediación configurada

0%

c) Se le asigna una nueva dirección IP

0%

d) Se le permite el acceso limitado solo a servicios críticos

0%

Configuración básica: ISE y VPN

Configuración Cisco ISE

Configuraciones iniciales de Posture

Actualización de la base de datos de posture

Configuración general de posture

Provisionamiento: Recursos y políticas

Descarga de los módulos

Configuración perfiles de posture y de agente

Configuración de políticas de provisionamiento

Condiciones, Remediación, Requerimientos y Políticas

Configuración de condiciones y acciones de remediación

Configuración de requerimientos

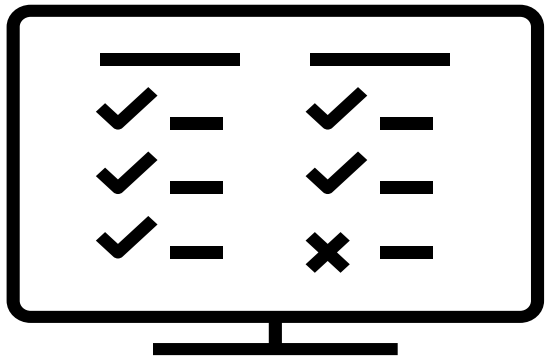
Configuración y activación de políticas de postura

Políticas de Autenticación y Autorización

Configuración de perfiles de autorización para los 3 estados de posture

Configuración del set de políticas de acceso a los estados de posture

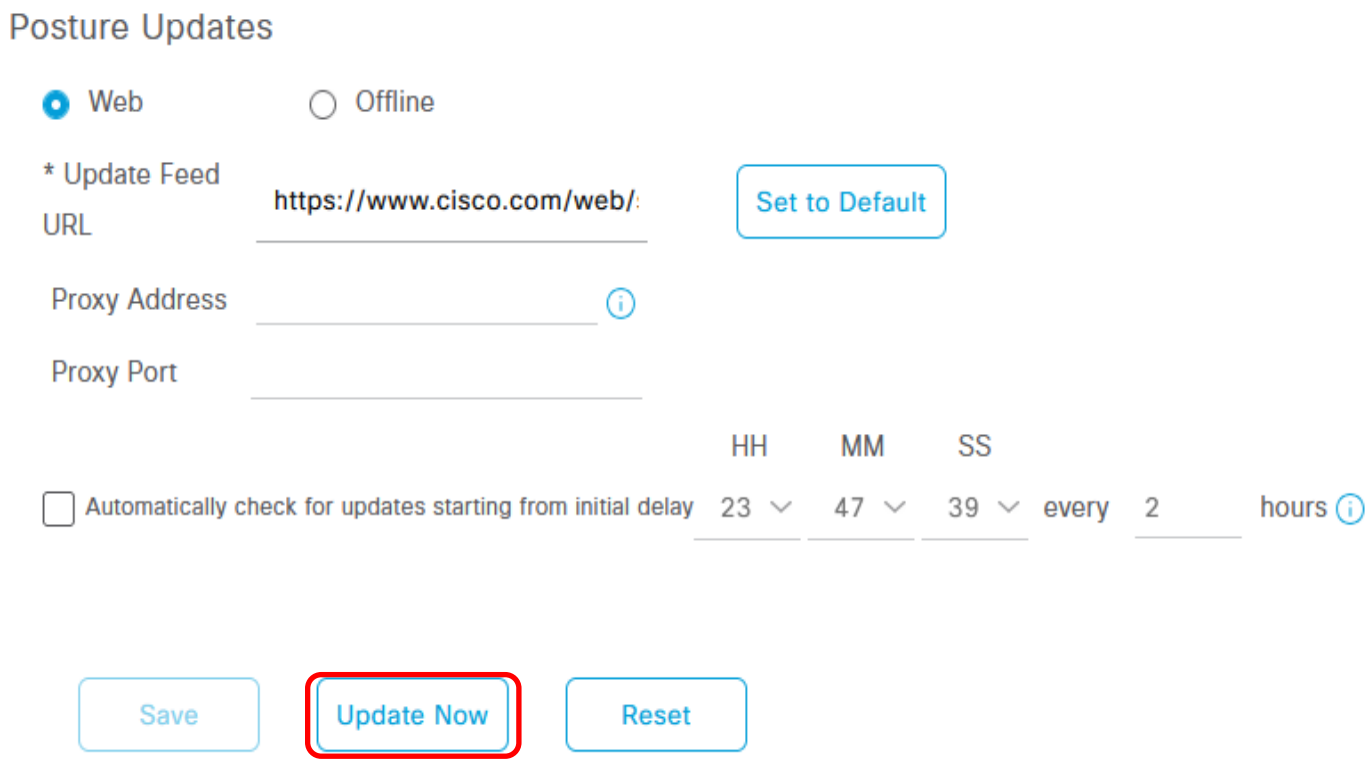
Configuraciones Iniciales de Posture



Configuración Inicial de Posture

Paso 1: Actualización de Base de datos de Posture

Administration > System > Settings > Posture > Updates.



https://www.cisco.com/web/secure/spa/posture-offline.html

Configuración Inicial de Posture

Paso 2: Ajustes Generales

Administration > System > Settings > Posture > General Settings

Posture General Settings

These settings will be used if there is no profile under client provisioning policy.

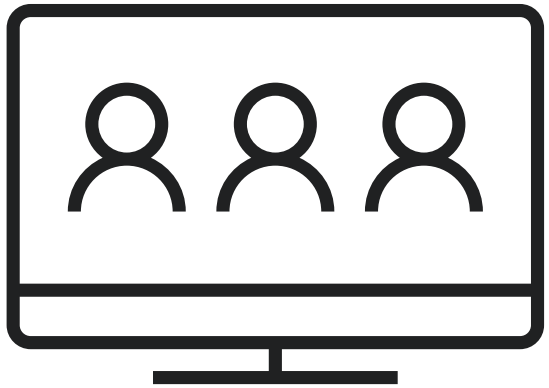
Remediation Timer	10	Minutes
Network Transition Delay	3	Seconds
Acceptable Use Policy in Stealth Mode	Block	
Default Posture Status	NonCompliant	
Automatically Close Login Success Screen After	0	Seconds
Continuous Monitoring Interval	15	Minutes

Posture Lease

- (•) Perform posture assessment every time a user connects to the network
- ( ) Perform posture assessment every 1 Days
- [ ] Cache Last Known Posture Compliant Status

Last Known Posture Compliant State: 0 Minutes

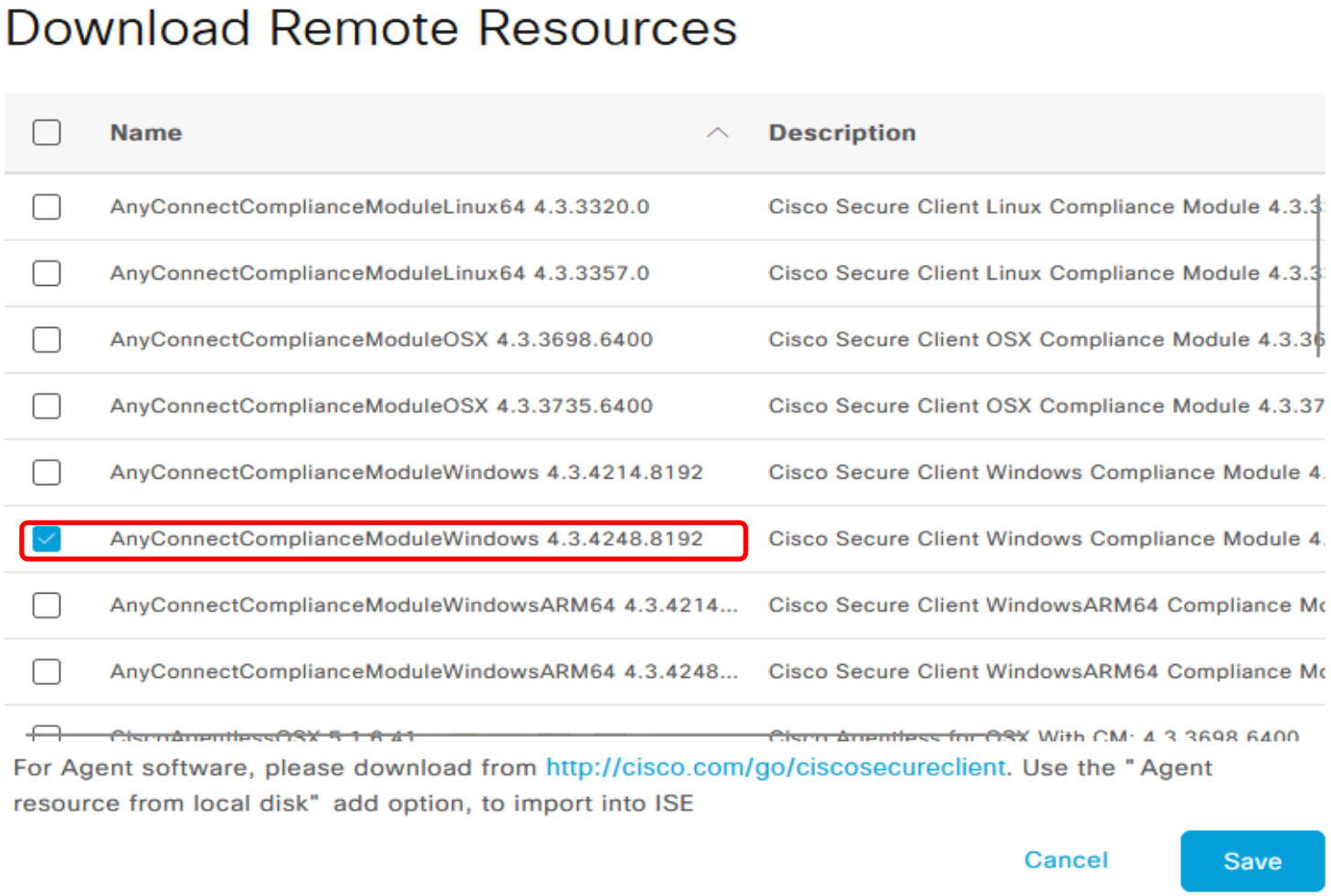
Provisionamiento: Recursos y políticas



Configuración Básica ISE: Provisionamiento

Paso 1: Descargar módulo de Cumplimiento (CM)

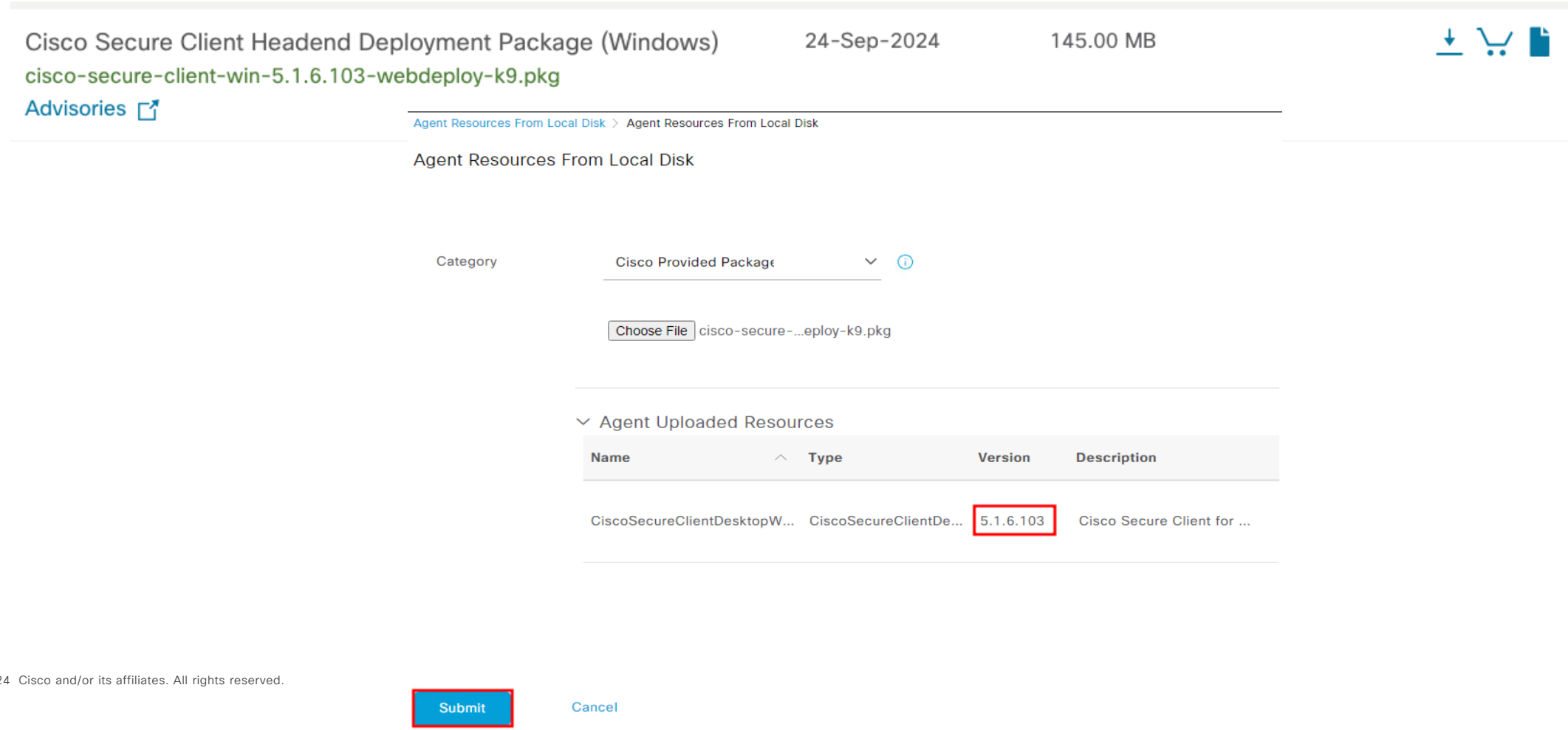
Policy > Policy Elements > Results > Client Provisioning > Resources
Add > Agent Resources From Cisco Site



Configuración Básica ISE: Provisionamiento

Paso 2: Descargar y subir Imagen de Cisco Secure Client

https://software.cisco.com/download/
Policy > Policy Elements > Results > Client Provisioning
Add > Agent Resources From Local Disk

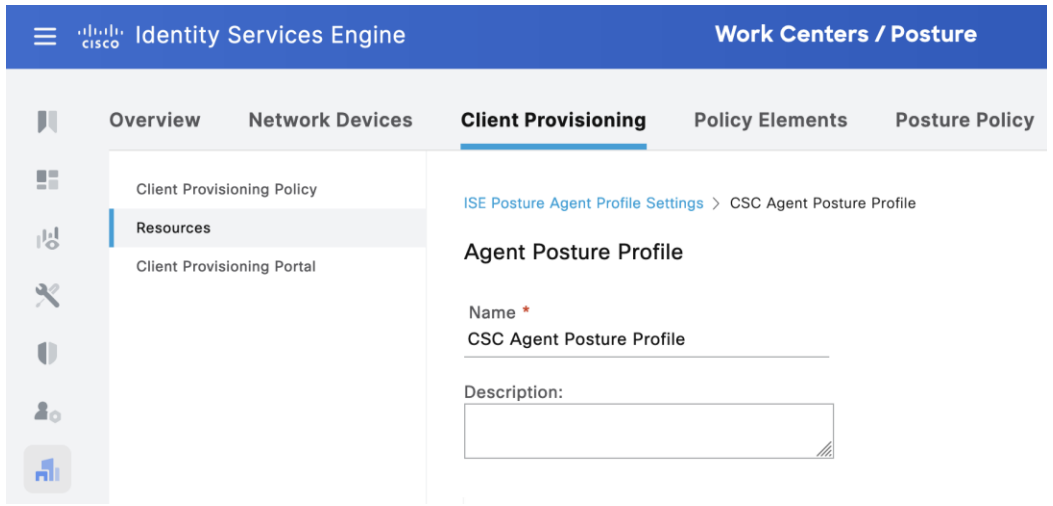


Configuración Básica ISE: Provisionamiento

Paso 3: Configuración del perfil de posture para Secure Client (Agente)

Policy > Policy Elements > Results > Client Provisioning

Add > Agent Configuration



Posture Protocol

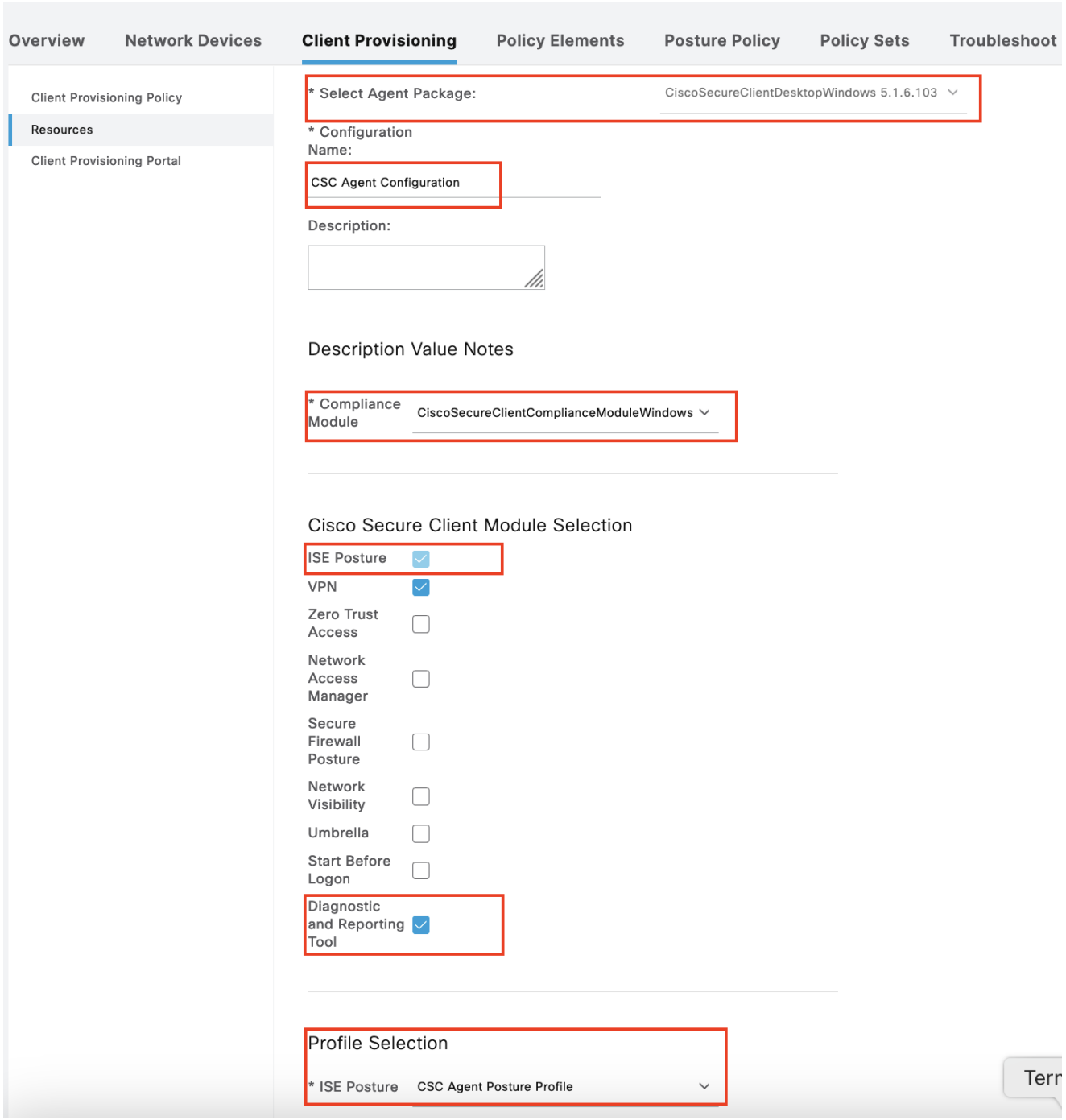
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ	1.2.3.4	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List ⓘ		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.

Configuración Básica ISE: Provisionamiento

Paso 4: Configuración del perfil del Agente SC

Policy > Client Provisioning > Resources

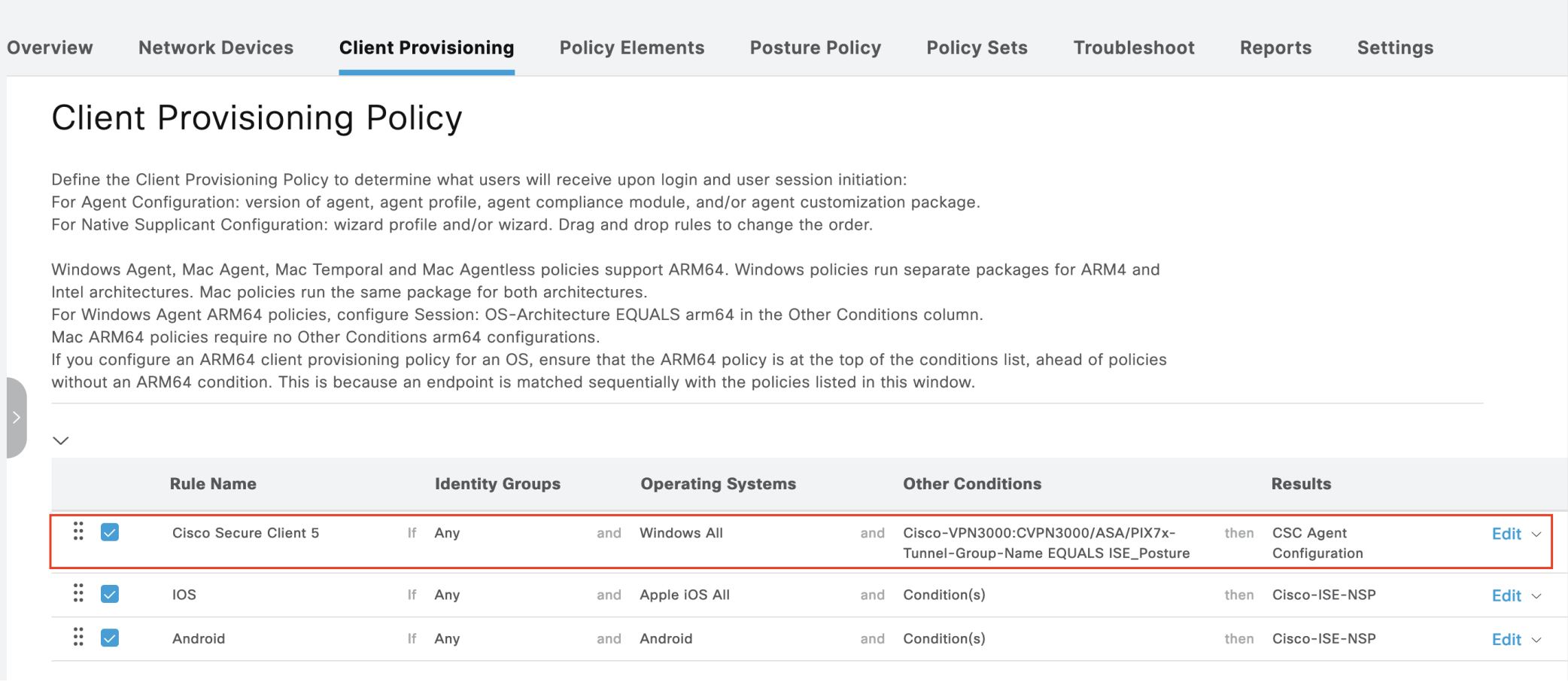
> Agent Configuration > New agent configuration



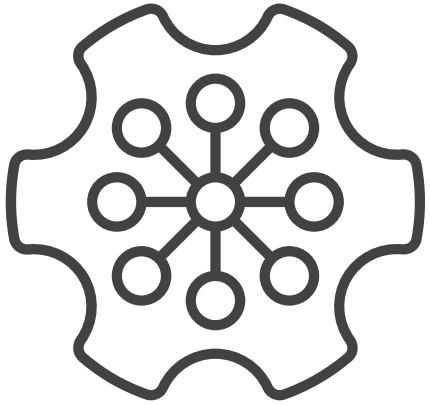
Configuración Básica ISE: Provisionamiento

Paso 5: Configuración de política de provisionamiento de cliente

Policy > Client Provisioning
Edit > Insert Rule Above



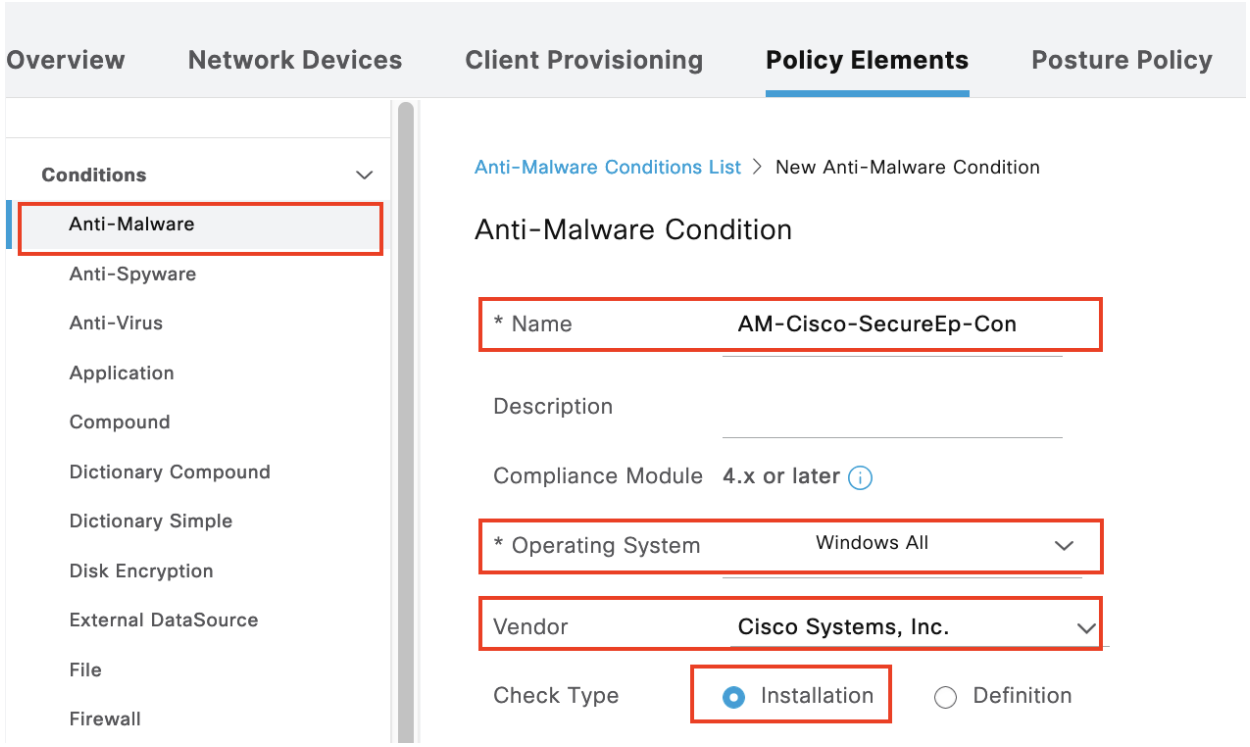
Condiciones, Remediación, Requerimientos y Políticas.



Configuración Básica ISE: Condiciones

Paso 1: Configuración de reglas de Posture para evaluar los clientes, caso de uso, Instalación AM Cisco Secure Endpoint.

Work Centers > Policy Elements > Conditions > Posture > Anti-Malware > Add

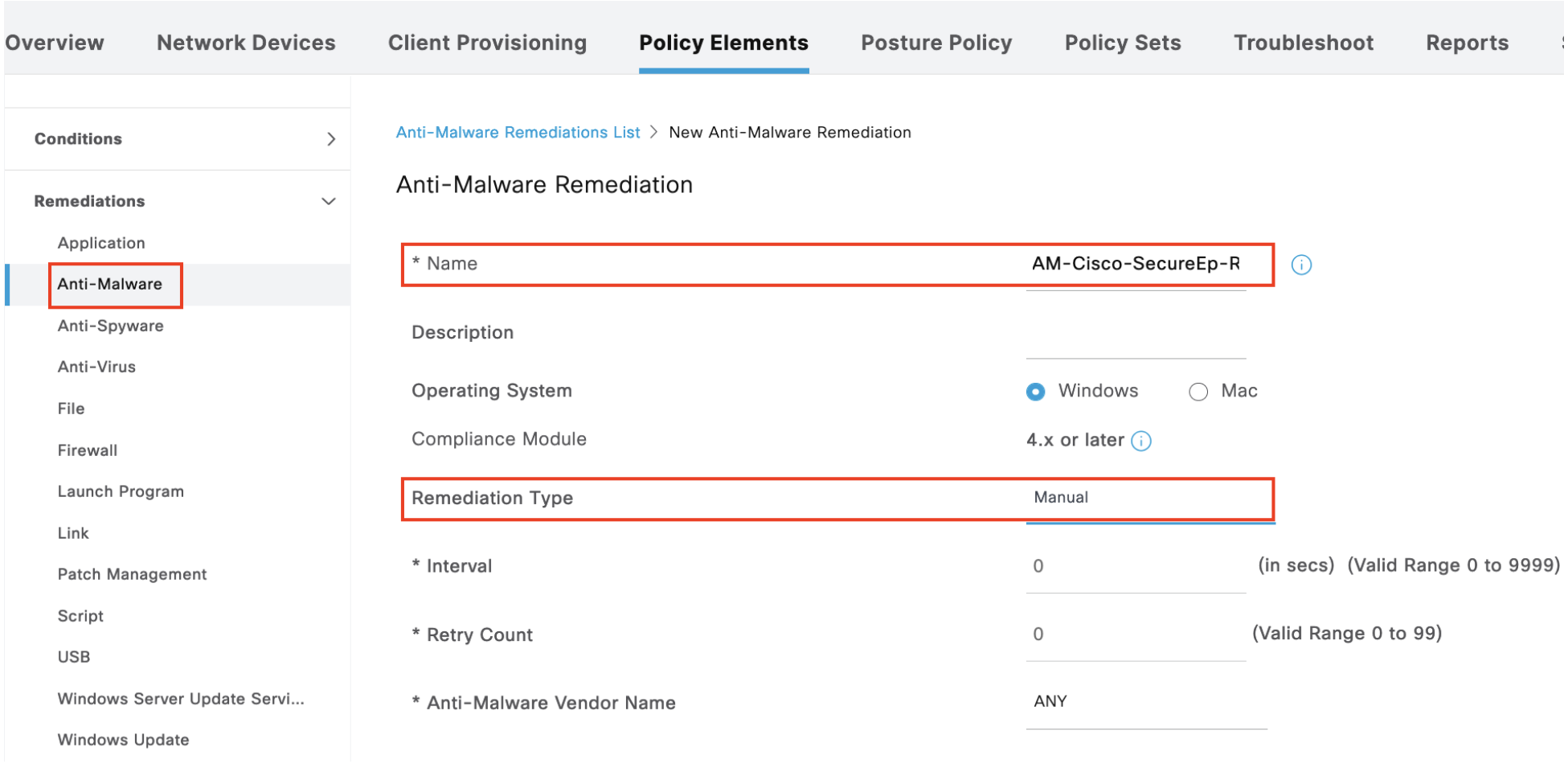


☑	Cisco Secure Endpoint	7.x	8.x	4.3.3726.6145

Configuración Básica ISE: Remediación

Paso 2: Configuración de acciones de remediación.

Work Centers > Policy Elements > Remediations > Posture > Anti-Malware > Add



Configuración Básica ISE: Requerimientos

Paso 3: Configuración de requisitos de Posture para el estado de cumplimiento (Compliant) de usuarios.

Policy > Policy Elements > Results > Posture > Requirements

Requirements

Name		Operating System		Compliance Module		Posture Type		Conditions		Remediations Actions	
_temporal											
Default_AppVis_Requirement_Win_temporal	for	Windows All	using	4.x or later	using	Temporal Agent	met if	Default_AppVis_Condition_Win	then	Select Remediations	Edit
Default_AppVis_Requirement_Mac_temporal	for	Mac OSX	using	4.x or later	using	Temporal Agent	met if	Default_AppVis_Condition_Mac	then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Win_temporal	for	Windows All	using	4.x or later	using	Temporal Agent	met if	Hardware_Attributes_Check	then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Mac_temporal	for	Mac OSX	using	4.x or later	using	Temporal Agent	met if	Hardware_Attributes_Check	then	Select Remediations	Edit
Default_Firewall_Requirement_Win_temporal	for	Windows All	using	4.x or later	using	Temporal Agent	met if	Default_Firewall_Condition_Win	then	Default_Firewall_Remediation_Win	Edit
Default_Firewall_Requirement_Mac_temporal	for	Mac OSX	using	4.x or later	using	Temporal Agent	met if	Default_Firewall_Condition_Mac	then	Default_Firewall_Remediation_Mac	Edit
AM-Cisco-SecureEp-Req	for	Windows All	using	4.x or later	using	Agent	met if	AM-Cisco-SecureEp-Con	then	AM-Cisco-SecureEp-Rem	Edit
AM-Posture-Req	for	Windows All	using	4.x or later	using	Agent	met if	AM-Posture-Win	then	AM-Posture-WinRem	Edit

Los requisitos se evaluarán para todos los usuarios que cumplan con las condiciones configuradas, en caso de no cumplir con los requisitos solicitados se les aplicará la acción de remediación correspondiente.

Configuración Básica ISE: Política de Posture

Paso 4: Configuración y activación de la política de Posture.

Work Centers > Posture > Posture Policy

Overview | Network Devices | Client Provisioning | Policy Elements | **Posture Policy** | Policy Sets | Troubleshoot | Reports | Settings

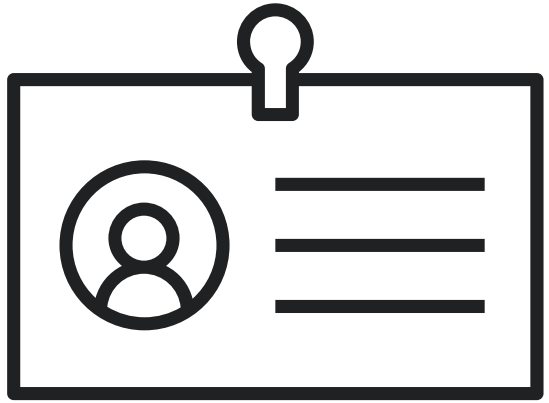
Posture Policy

Guide Me

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements
☑	Policy Options	AM-Cisco-SecureEP-Pol	If	Any	and	Windows All	and	4.x or later	and	Agent	and		then	AM-Cisco-SecureEp-Req
☑	Policy Options	AM-Posture-Policy	If	Any	and	Windows All	and	4.x or later	and	Agent	and		then	AM-Posture-Req
☐	Policy Options	Default_AntiMalware_Policy_Mac	If	Any	and	Mac OSX	and	4.x or later	and	Agent	and		then	Any_AM_Installation_Mac
☐	Policy Options	Default_AntiMalware_Policy_Mac_temporal	If	Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and		then	Any_AM_Installation_Mac_temporal
☐	Policy Options	Default_AntiMalware_Policy_Win	If	Any	and	Windows All	and	4.x or later	and	Agent	and		then	Any_AM_Installation_Win

Políticas de Autenticación y Autorización



Active poll

0

Join at

slido.com

#2535 244

¿Cuál es el propósito principal de las DACL (Listas de Control de Acceso Dinámicas) en la configuración de Cisco ISE para usuarios de VPN de acceso remoto?

a) Restringir el acceso a la red según el estado de cumplimiento de la postura

0%

b) Proporcionar acceso completo a todos los usuarios

0%

c) Asignar direcciones IP estáticas a los usuarios

0%

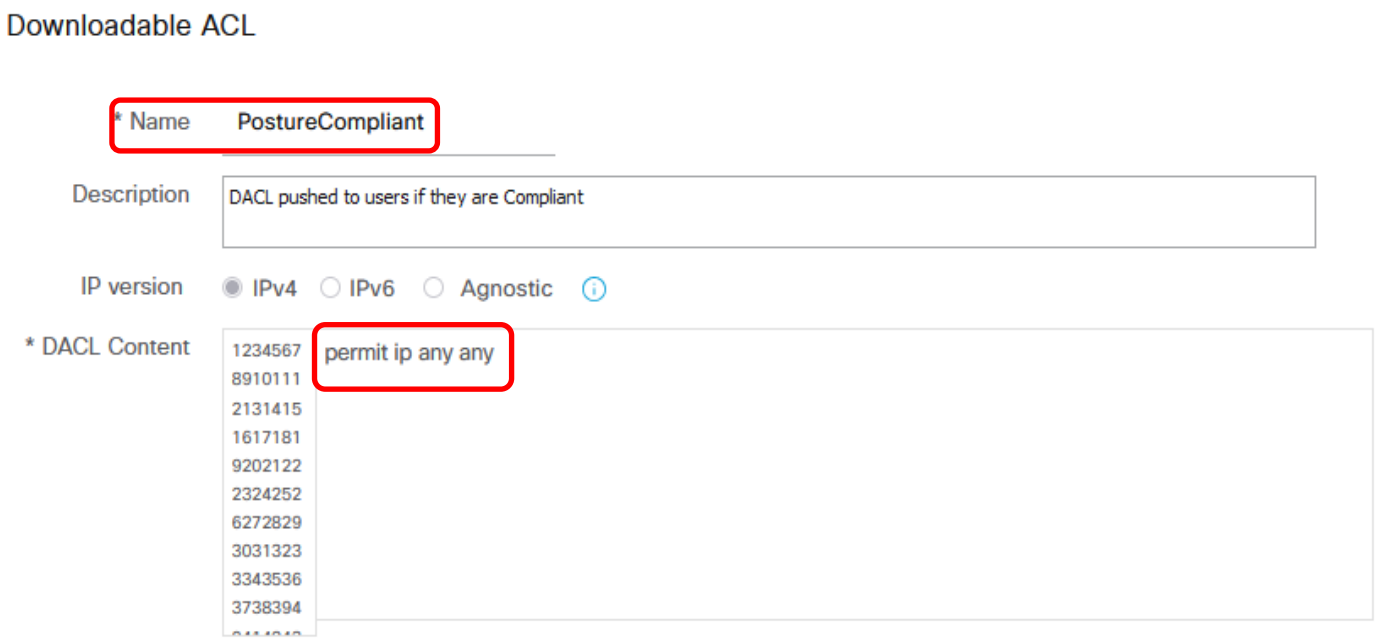
d) Monitorear el tráfico de red en tiempo real

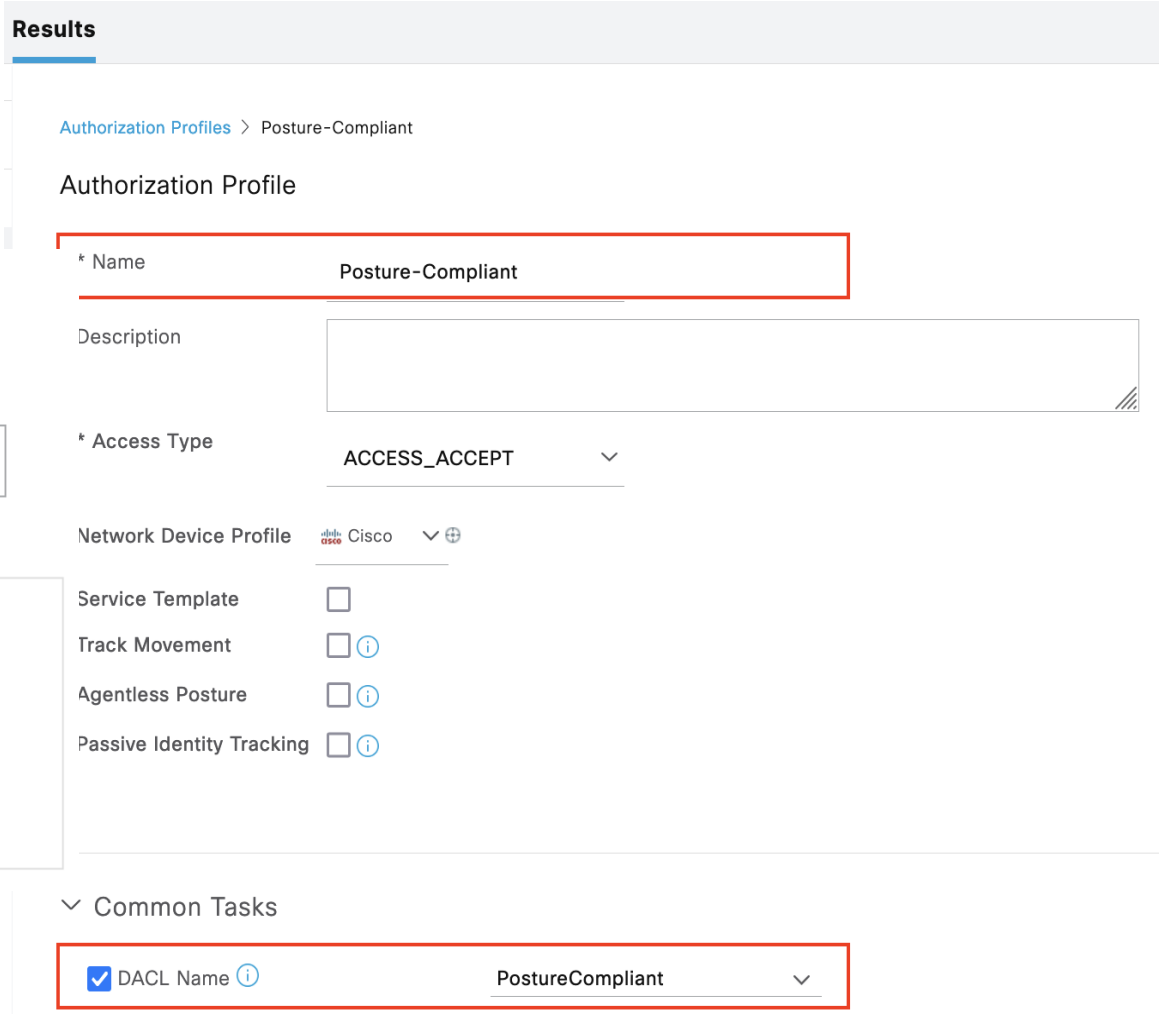
0%

Configuración Básica ISE: Políticas de Autorización

Paso 1: Configuración de políticas de autorización de acuerdo con el estado de Posture: Compliant

Policy > Policy Elements > Results > Authorization > Downloadable ACLS
Policy > Policy Elements > Results > Authorization > Autorization Profiles

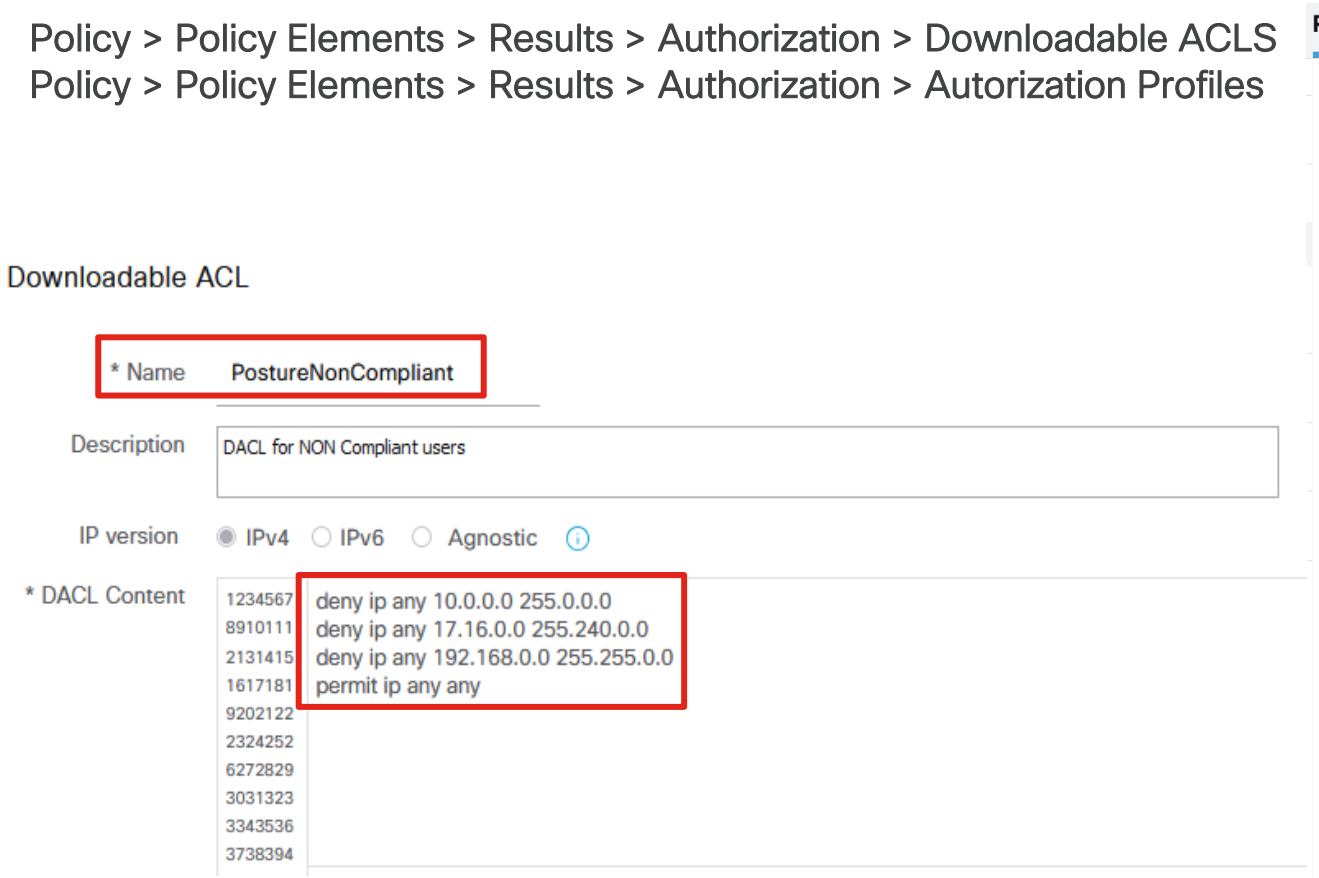


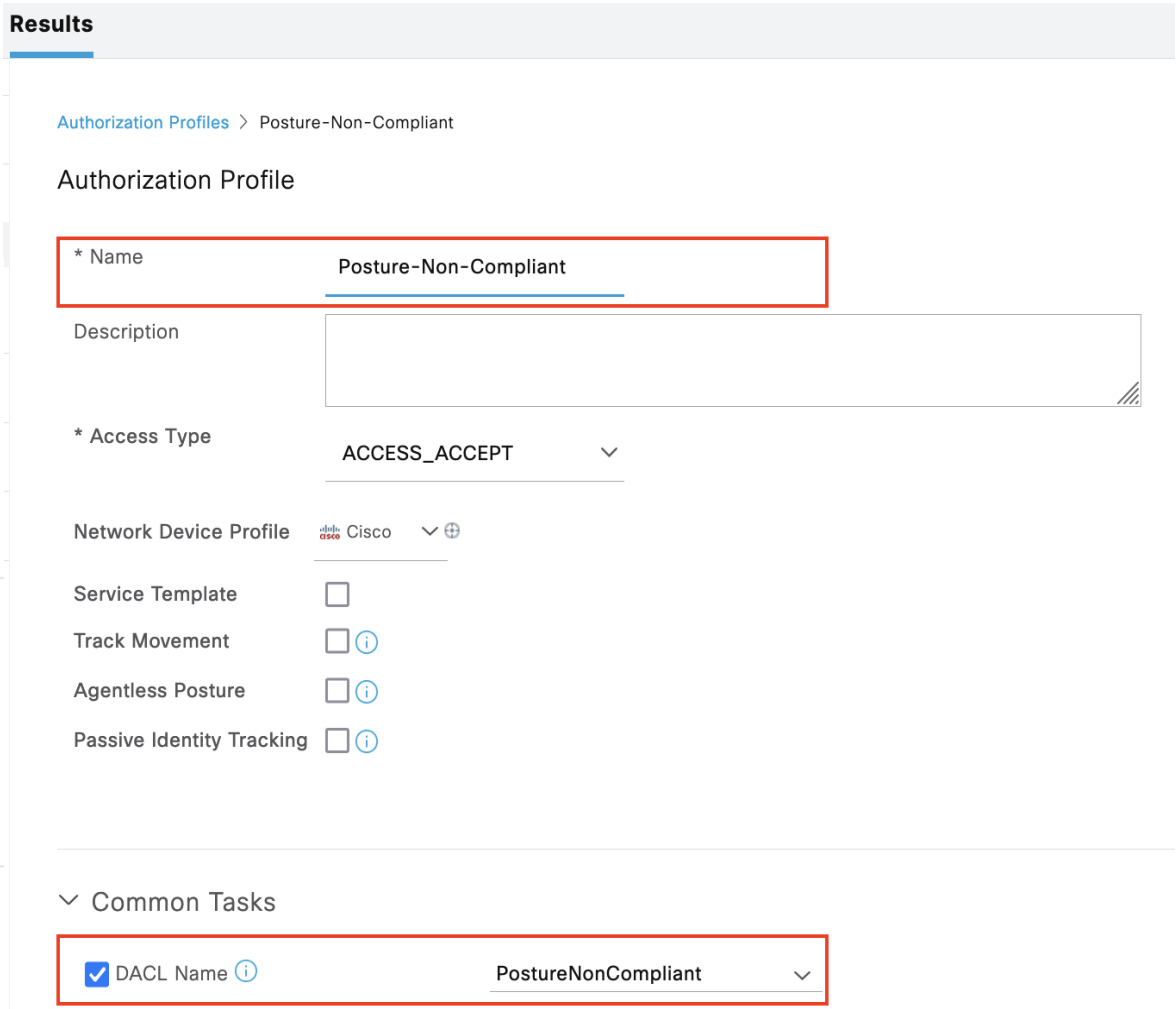


Configuración Básica ISE: Políticas de Autorización

Configuración de políticas de autorización de acuerdo con el estado de Posture: Non-Compliant

Policy > Policy Elements > Results > Authorization > Downloadable ACLS
Policy > Policy Elements > Results > Authorization > Autorization Profiles

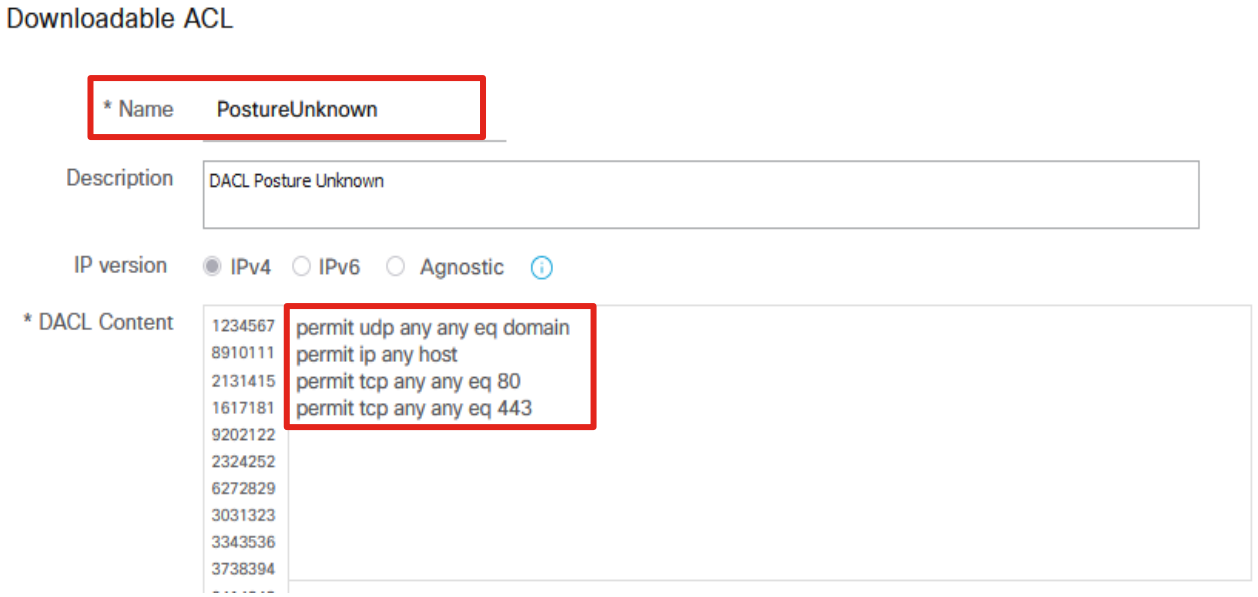


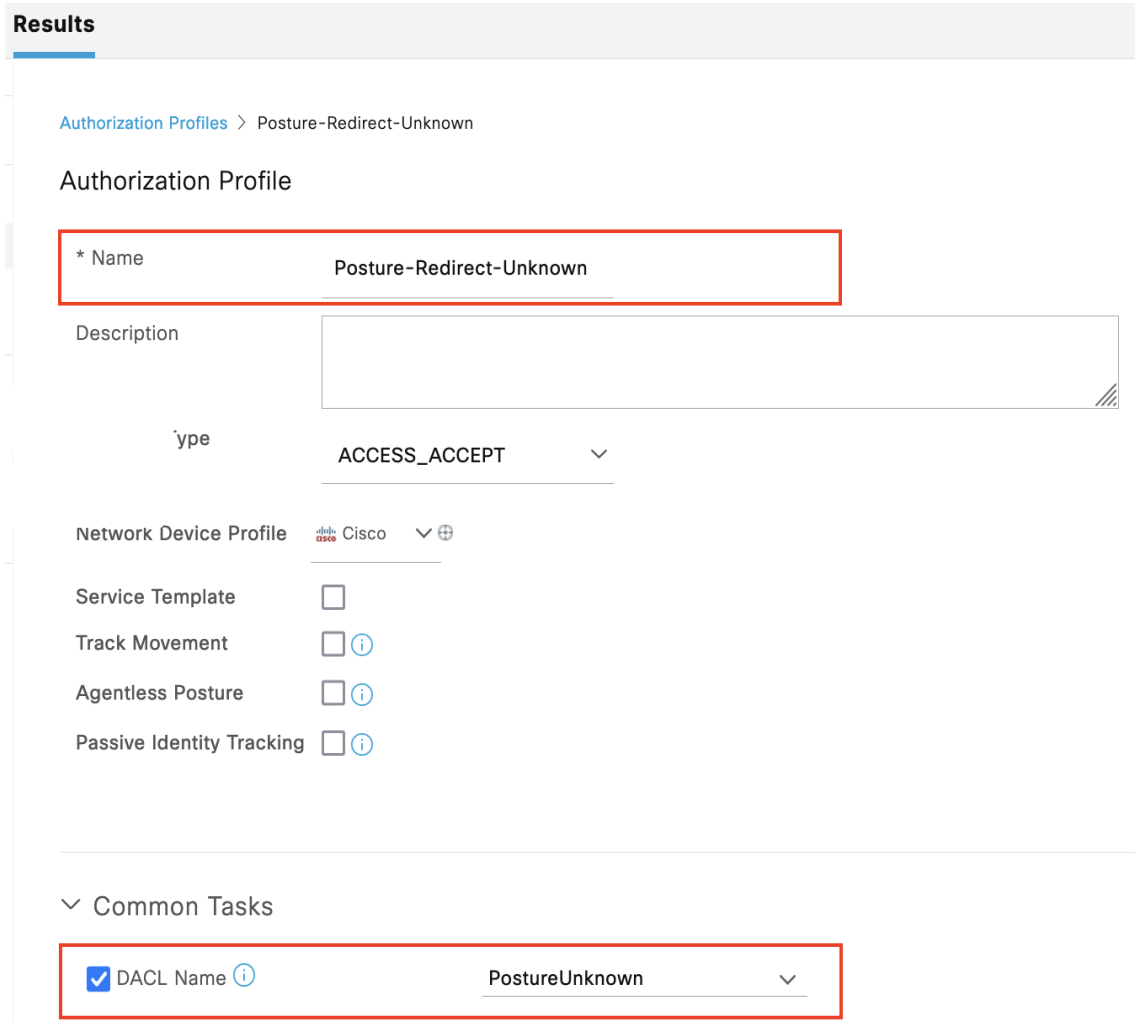


Configuración Básica ISE: Políticas de Autorización

Configuración de políticas de autorización de acuerdo con el estado de Posture: Desconocido / Unknown

Policy > Policy Elements > Results > Authorization > Downloadable ACLS
Policy > Policy Elements > Results > Authorization > Autorization Profiles

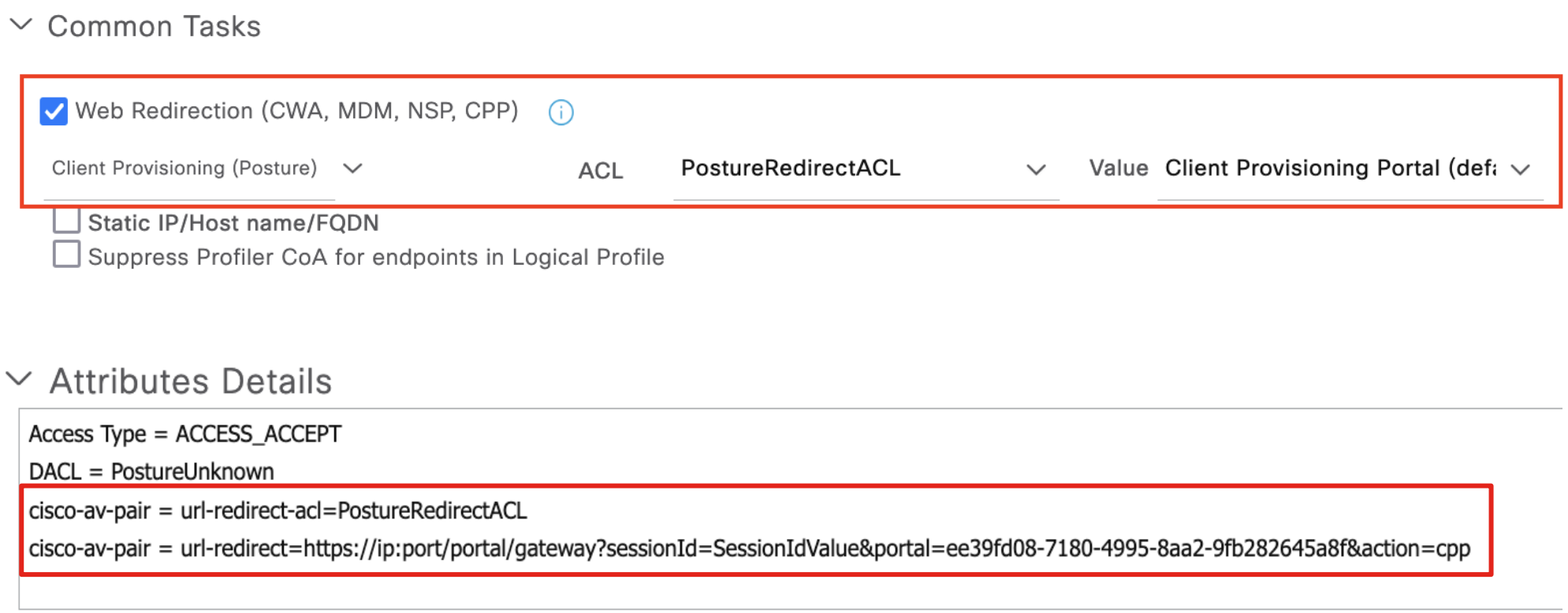




Configuración Básica ISE: Políticas de Autorización

Configuración de políticas de autorización de acuerdo con el estado de Posture: Desconocido / Unknown

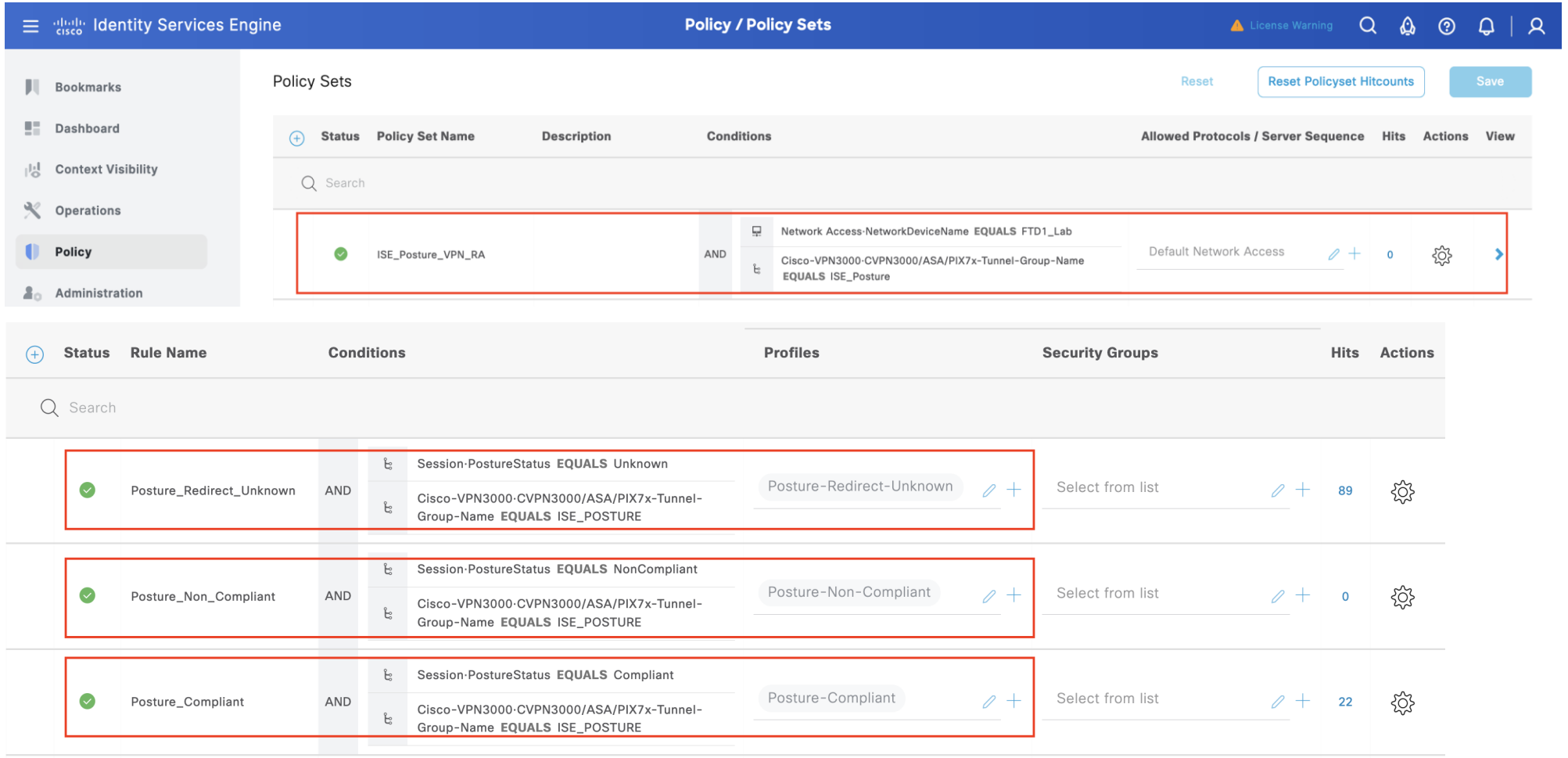
Atributos de redirección



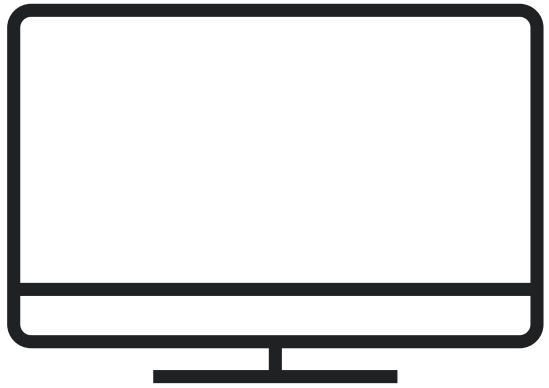
Configuración Básica ISE: Políticas de Autorización

Paso 2: Configuración de un nuevo set de políticas de autenticación y autorización acorde al estado de Posture: Compliant, Non-Compliant, Unknown

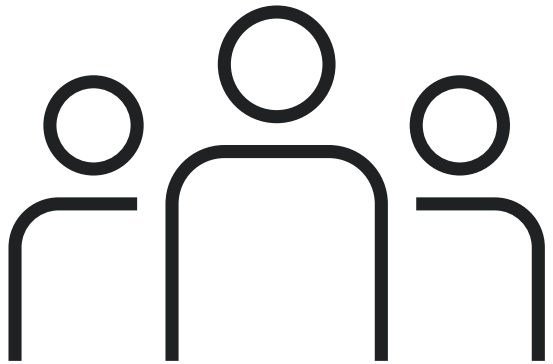
Policy > Policy Sets



Configuración Básica FMC: Túnel, Servidores de ISE, Listas y perfil de acceso



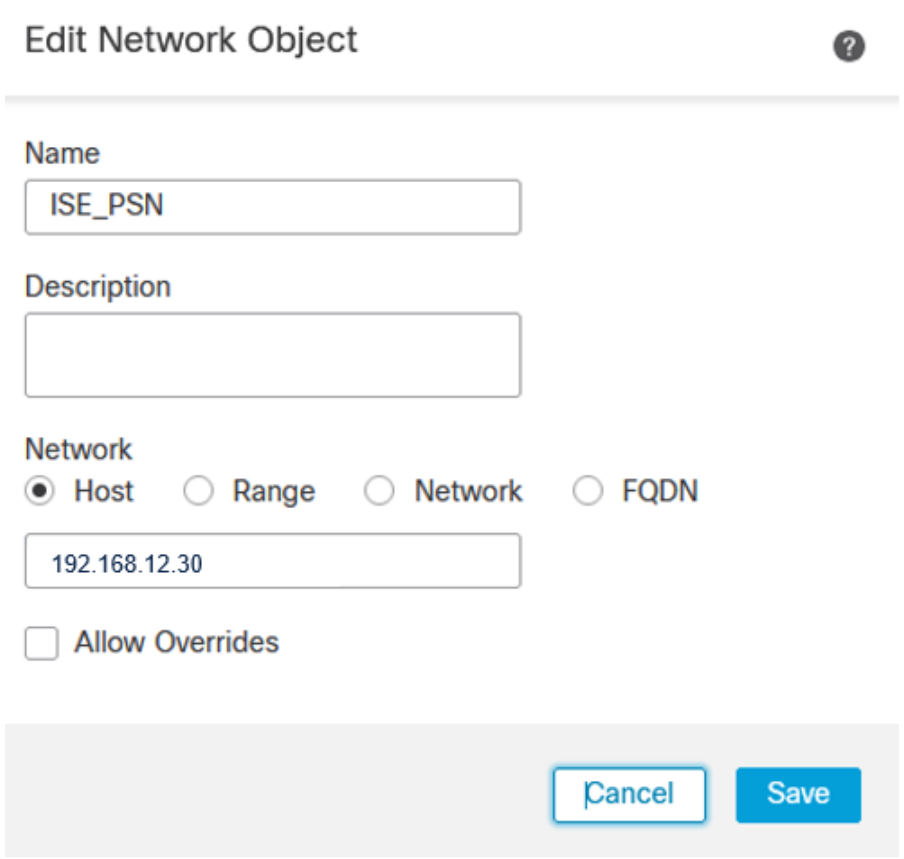
Servidores de ISE y Listas de acceso



Configuración Básica FMC: Servidores de ISE

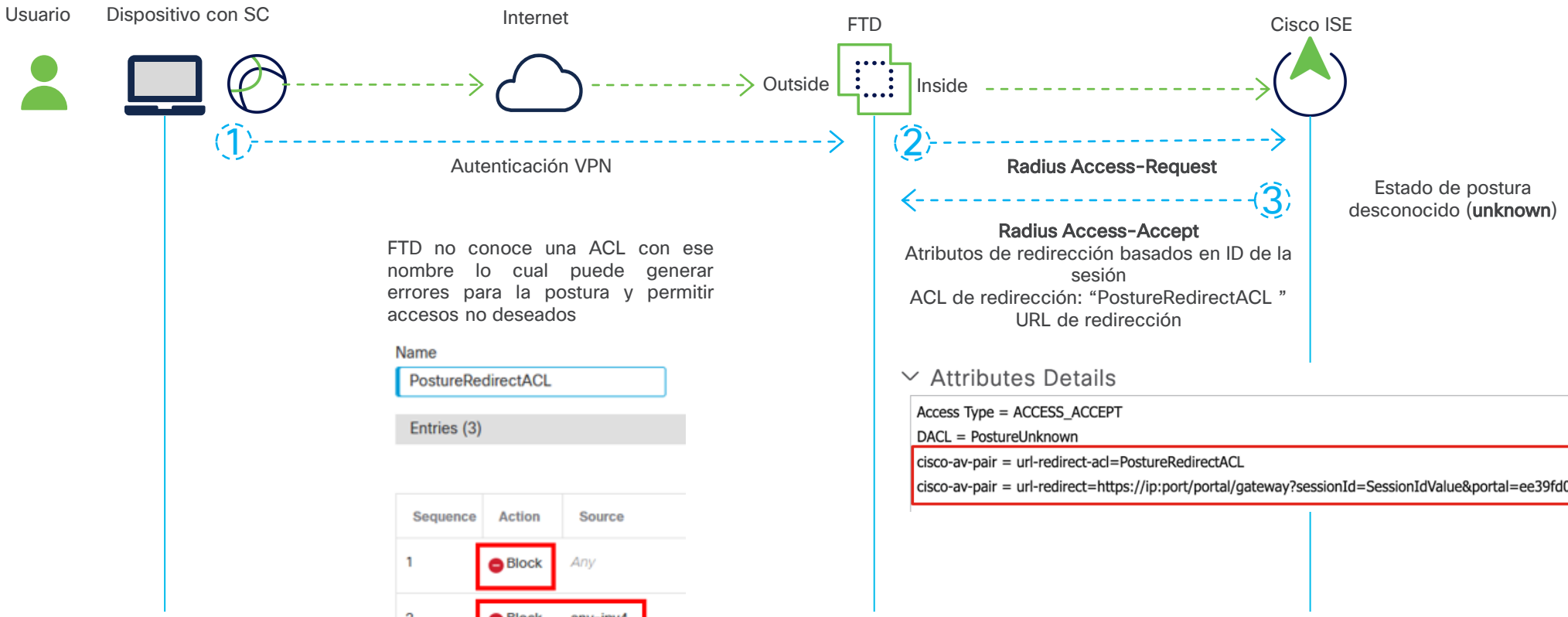
Paso 1: Configuración de objeto de red con la IP del ISE

Objects > Object management > Network > Add object



Atención al nombre de la ACL de redirección

TAC Tip



Configuración Básica FMC: Lista de acceso de redirección

Paso 2: Configurar una ACL de redirección

Allow significará que ese tráfico será redirigido, Deny significará que el tráfico no será redirigido.

Objects > Object management > Access List > Extended > Add Extended Access List

Name

PostureRedirectACL

Entries (3)

Add

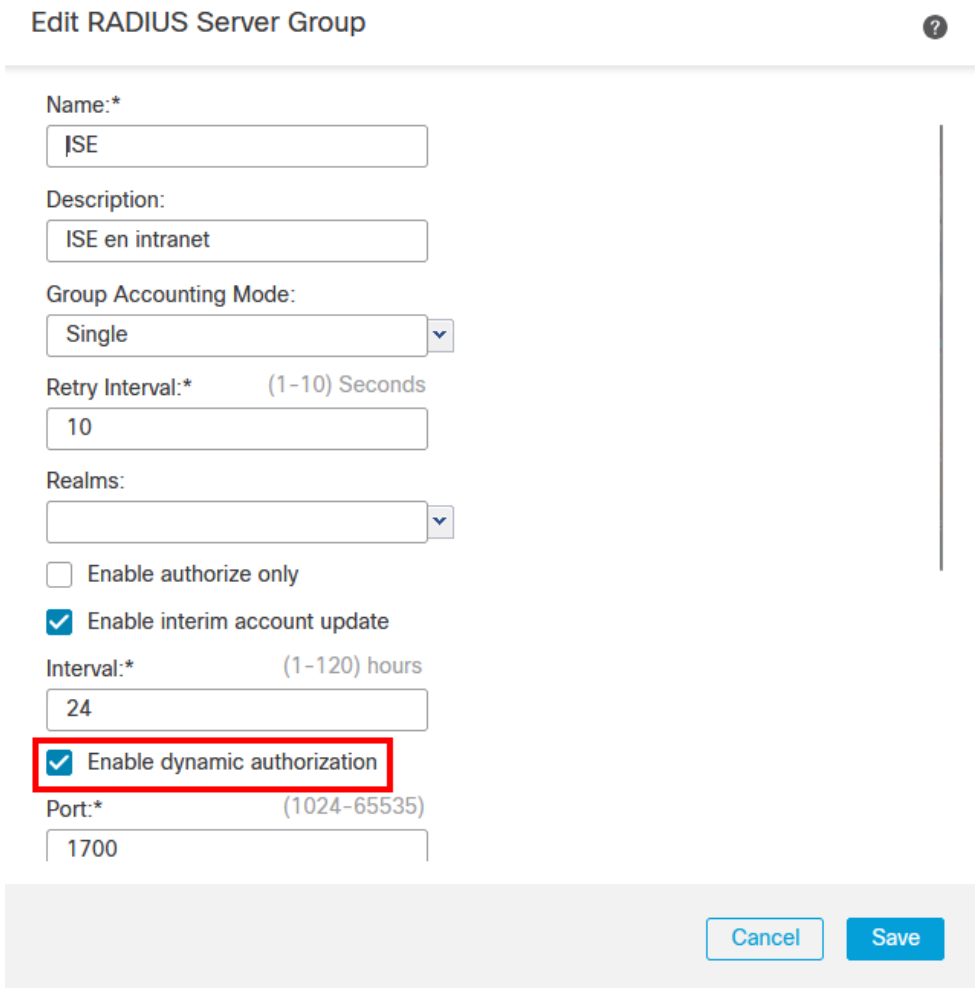
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Block	Any	Any	Any	DNS_over_UDP	Any	Any	Any
2	Block	any-ipv4	Any	ISE_PSN	Any	Any	Any	Any
3	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any

Allow Overrides

Cancel Save

Configuración Básica FMC: Grupo de servidores RADIUS

Paso 3: Configurar un grupo de servidores RADIUS para poder agregar nuestro servidor ISE

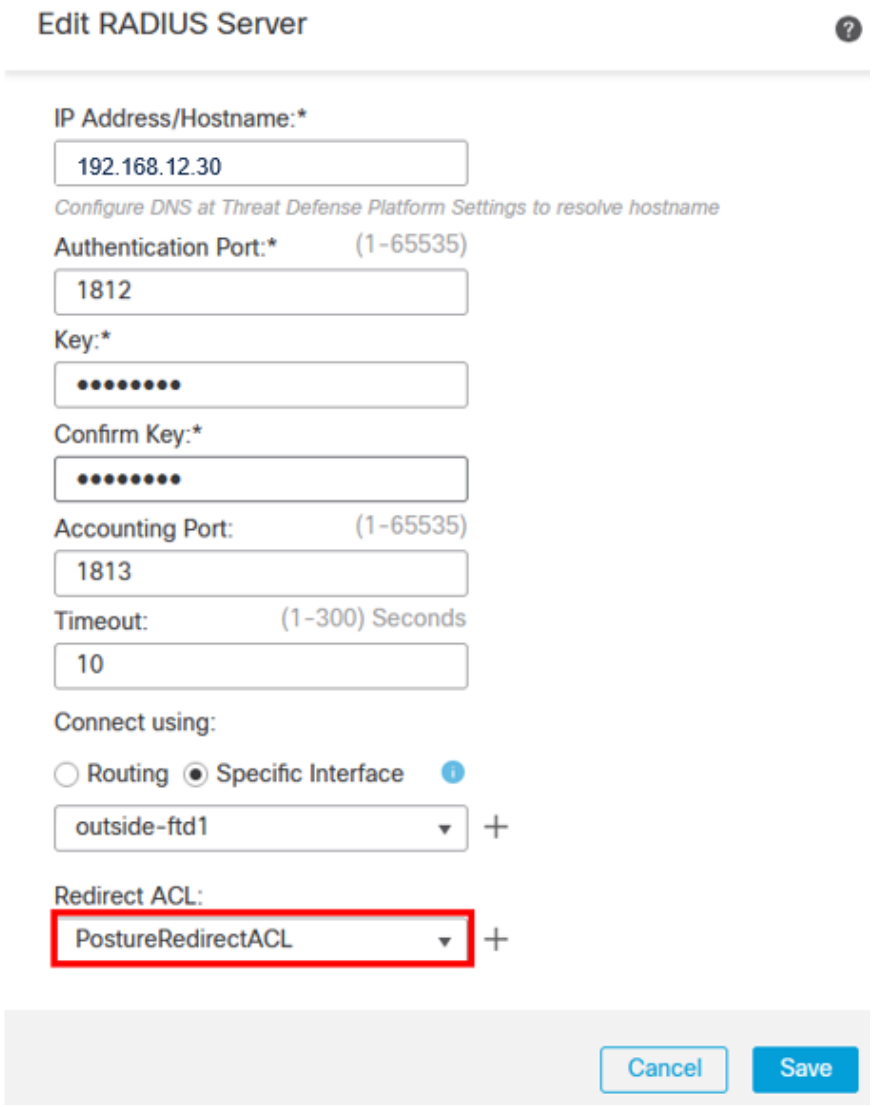


Objects > Object management> AAA Server > RADIUS Server Group > Add RADIUS Server Group

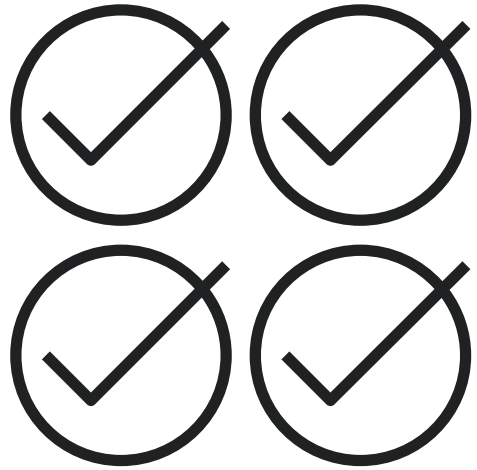
Configuración Básica FMC: Servidores de ISE

Paso 3: Configuración de los servidores individuales de ISE dentro del grupo (autenticación y autorización)

Edit RADIUS Server / Add RADIUS Server



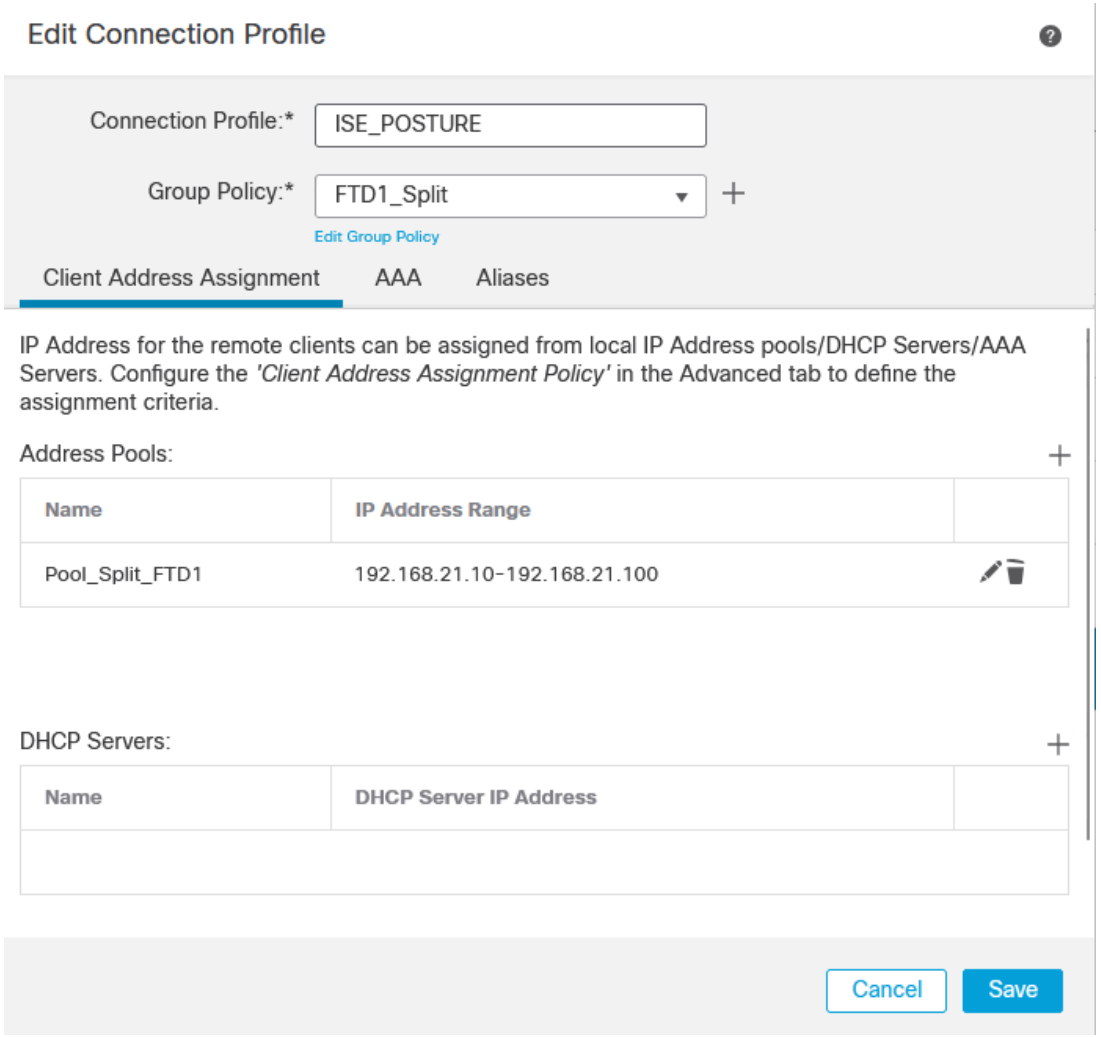
Configuración VPN de acceso remoto (RAVPN)



Configuración Básica FMC: RAVPN

Paso 4: Configuración del Tunnel Group, asegurarnos que el FTD otorgue IPs a los usuarios remotos

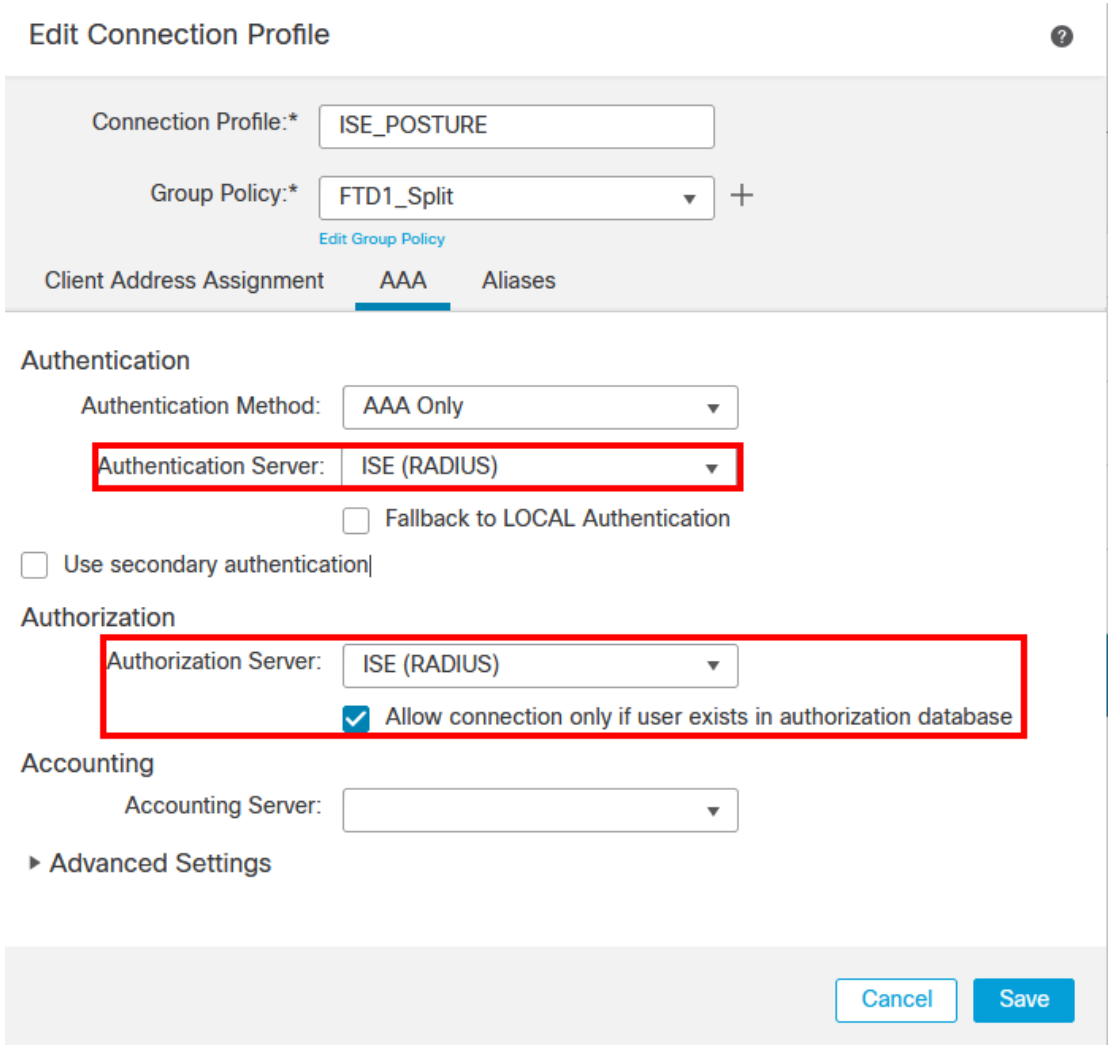
Devices > VPN > Remote Access > Edit Policy > Edit Connection profile



Configuración Básica FMC: RAVPN

Paso 5: Configuración de métodos de autenticación y autorización

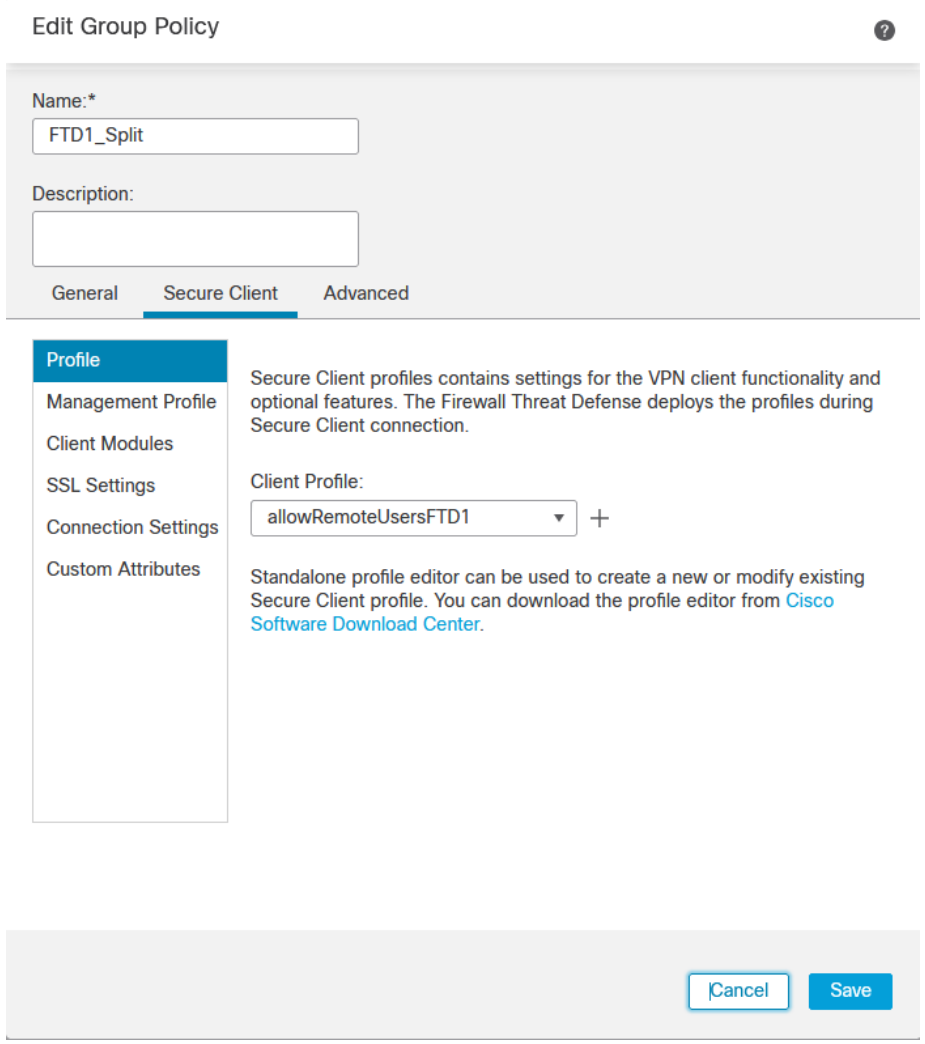
Devices > VPN > Remote Access > Edit Policy > Edit Connection profile > AAA



Configuración Básica FMC: Group policy

Paso 6: Configuración del Group Policy: Perfil

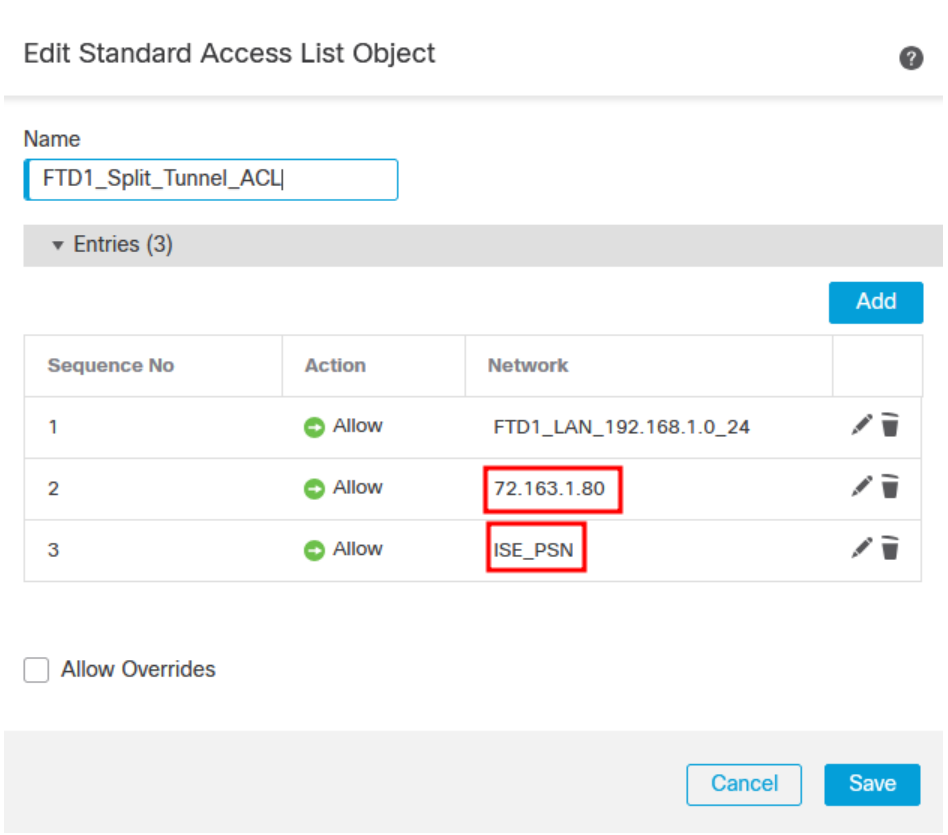
Devices > VPN > Remote Access > Edit Policy > Edit Connection Profile > Edit Group policy > Secure client

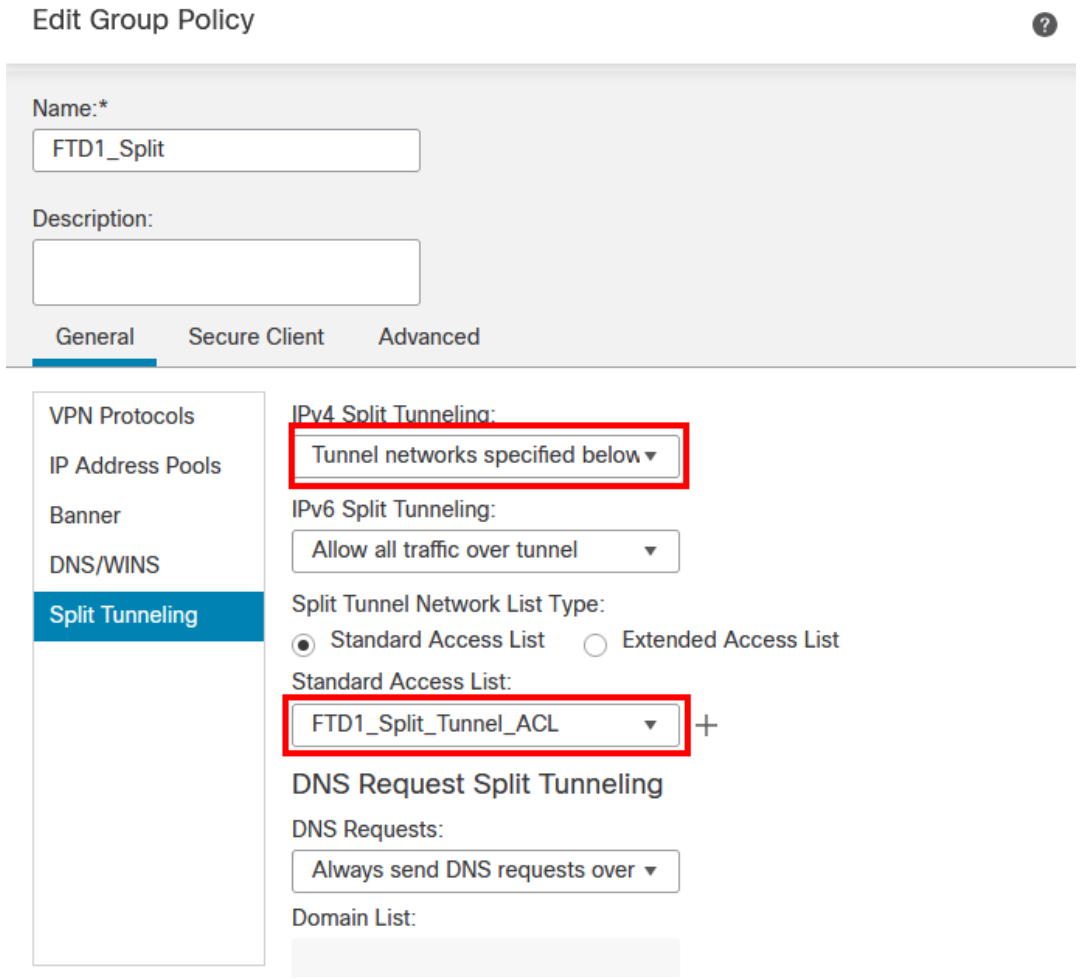


Configuración Básica FMC: Group policy

Paso 7: Configuración del “split tunnel”

Devices > VPN > Remote Access > Edit Policy > Edit Connection profile > Edit Group policy > General > Split Tunneling

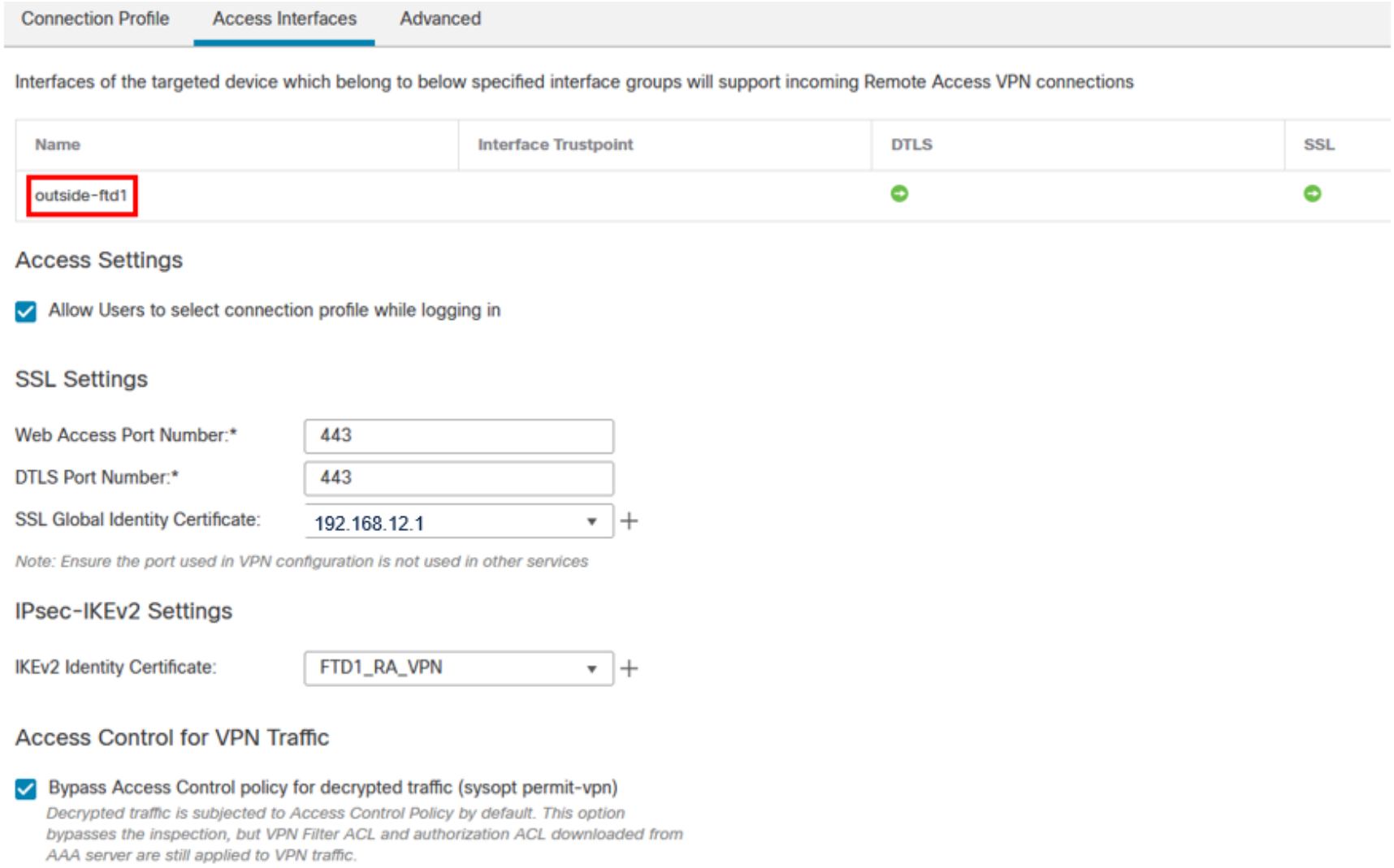




Configuración Básica FMC: Interfaz

Paso 8: Configuración de la interfaz

Devices > VPN > Remote Access > Edit Policy > Access Interfaces



Demo

Comprobación: Monitoreo y Reportes

ISE Live Logs y Reportes de posture

Monitoreo y Reportes: ISE Live Logs

Flujo de posture en caso de uso Cisco Secure Endpoint

Operations > Radius > Live Logs

Reset Repeat Counts | Export To | Filter

Status	Details	Repeat ...		Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
				#ACSACL#-IP-PostureCompliant...					
		0	3	Usuario_Posture	00:50:56:B3:75:CE	Windows10-Workstation	ISE_Posture_VPN_RA >> Default	ISE_Posture_VPN_RA >> Posture_Compliant	Posture-Compliant
			2		00:50:56:B3:75:CE		ISE_Posture_VPN_RA	ISE_Posture_VPN_RA >> Posture_Compliant	Posture-Compliant
				#ACSACL#-IP-PostureUnknown-...					
			1	Usuario_Posture	00:50:56:B3:75:CE		ISE_Posture_VPN_RA >> Default	ISE_Posture_VPN_RA >> Posture_Redirect_Unknown	Posture-Redirect-Unknown

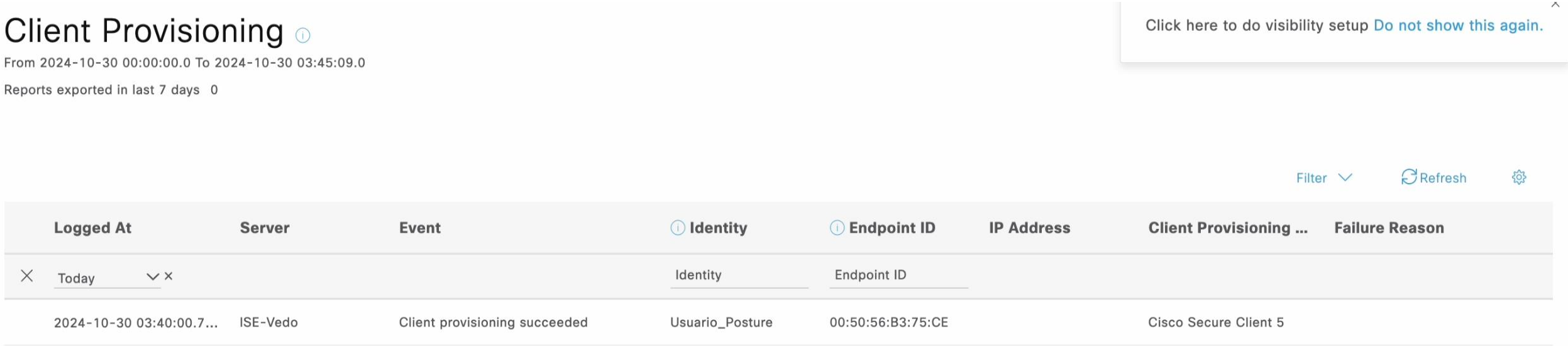
Reset Repeat Counts | Export To

Authorization Profiles	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server	Mdm Ser...	Session ID
		FTD1_Lab				ISE-Vedo		0c046229000d2000672abb12
Posture-Compliant					Compliant	ISE-Vedo		0c046229000d2000672abb12
Posture-Compliant		FTD1_Lab			Compliant	ISE-Vedo		0c046229000d2000672abb12
		FTD1_Lab				ISE-Vedo		0c046229000d2000672abb12
Posture-Redirect-Unknown		FTD1_Lab		User Identity Groups	Pending	ISE-Vedo		0c046229000d2000672abb12

Monitoreo y Reportes: Reportes de Posture

Reportes de provisionamiento: Lista clientes que han descargado SC y perfiles vía portal de provisionamiento

Operations > Reports > Reports > Endpoints and Users > Client Provisioning



Monitoreo y Reportes: Reportes de Posture

Reportes de cumplimiento por dispositivo: Lista y detalles de clientes que han pasado por el proceso de posture, condiciones, requerimientos, programas, etc.

Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint

Posture Assessment by Endpoint

Add to My Reports Export To Schedule

From 2024-11-06 00:00:00.0 To 2024-11-06 00:53:05.0

Reports exported in last 7 days 0

Filter Refresh

Status	Details	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message	PRA Actio
		Identity	Endpoint ID		Endpoint OS			
✗		Usuario_Posture	00:50:56:B3:75:CE		Windows 10 Enterprise 64-bit	Posture Agent for Windows 5.1.6.103	Received a posture report from an endpoint	N/A
		osture	00:50:56:B3:75:CE		Windows 10 Enterprise 64-bit	Posture Agent for Windows 5.1.6.103	Received a posture report from an endpoint	N/A
✓		Usuario_Posture	00:50:56:B3:75:CE		Windows 10 Enterprise 64-bit	Posture Agent for Windows 5.1.6.103	Received a posture report from an endpoint	N/A

Click Here for Detail Report

Posture Report

Posture Status	NonCompliant
Logged At	2024-11-06 00:49:46.352

Monitoreo y Reportes: Reportes de Posture

Detalles del reporte

Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint

AM Installed	Windows Defender;4.18.24090.11;;

Posture Policy Details

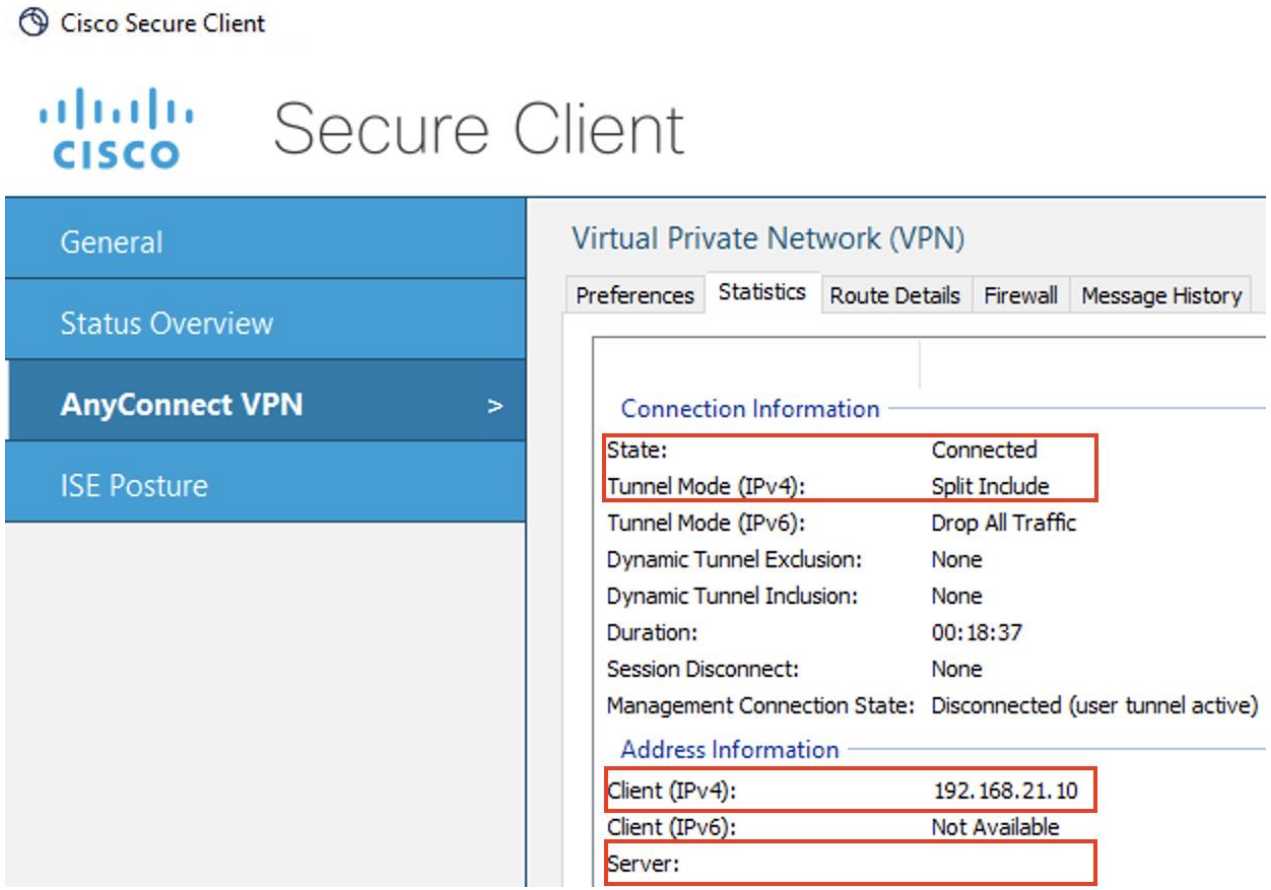
Policy	Name	Enforcement Type	Status	Passed Conditions	Failed Conditions	Skipped Conditions
AM-Cisco-SecureEP-Pol	AM-Cisco-SecureEp-Req	Mandatory	Failed		am_inst_v4_CiscoSecureEndpoint_7_x,am_inst_v4_CiscoSe...	
AM-Posture-Policy	AM-Posture-Req	Mandatory	Passed	am_inst_v4_WindowsDefender_4_x		,am_inst_v4_WindowsDefender_6_x

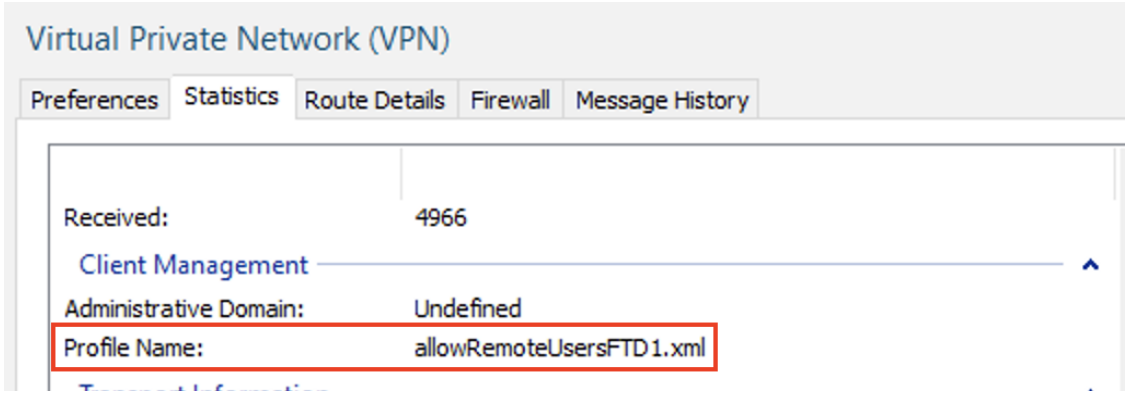
Secure Client: Módulos VPN y ISE Posture

Monitoreo y Reportes: Módulo de VPN

Detalles de la conexión remota de VPN

Secure Client > AnyConnect VPN > Statistics

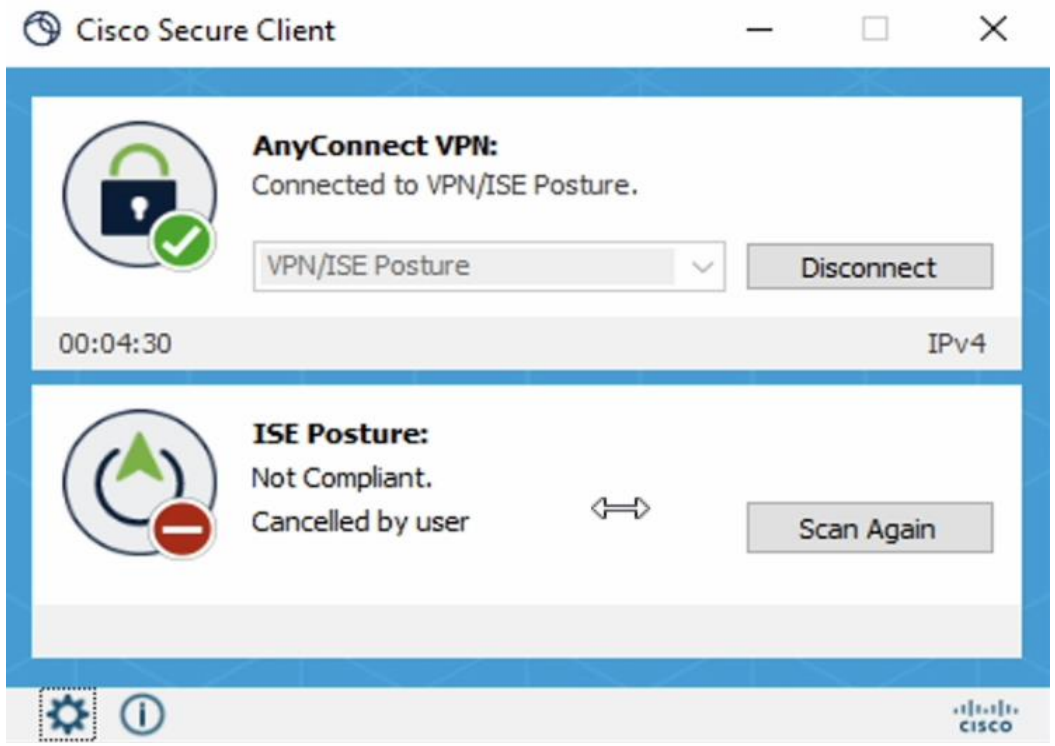




Monitoreo y Reportes: Módulo de ISE Posture

Detalles del estado de posture.

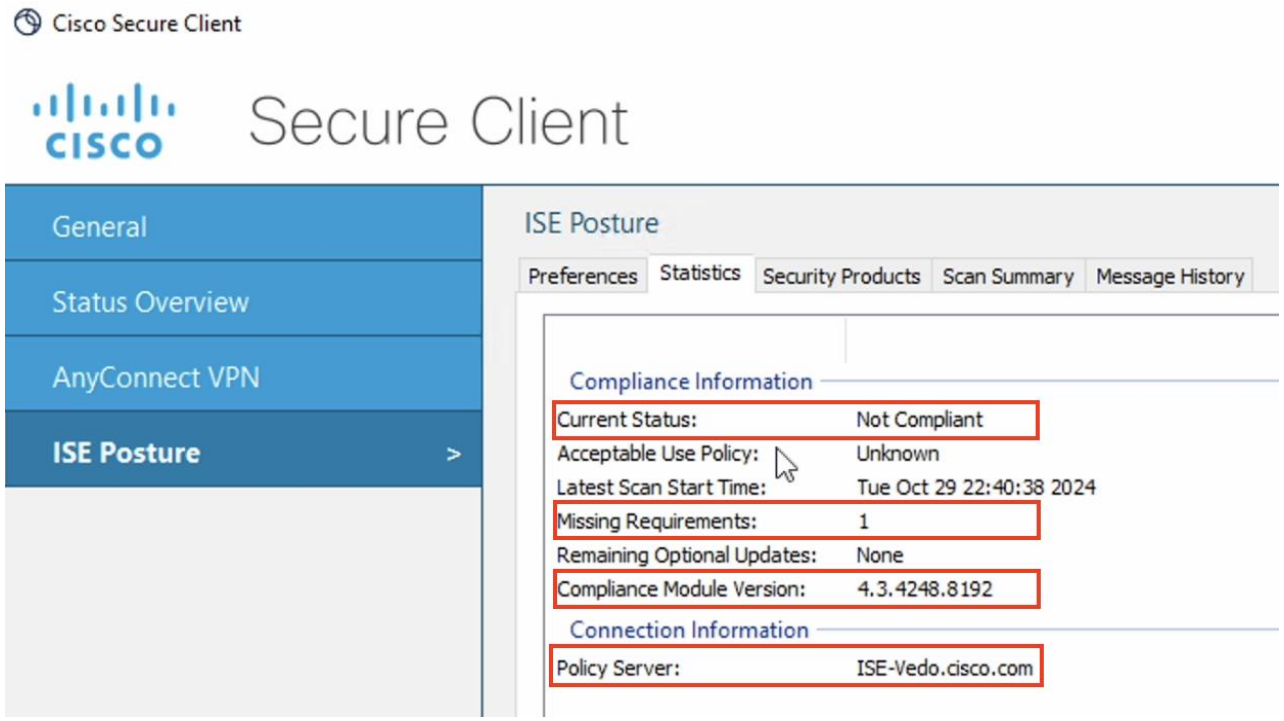
Interfaz de usuario

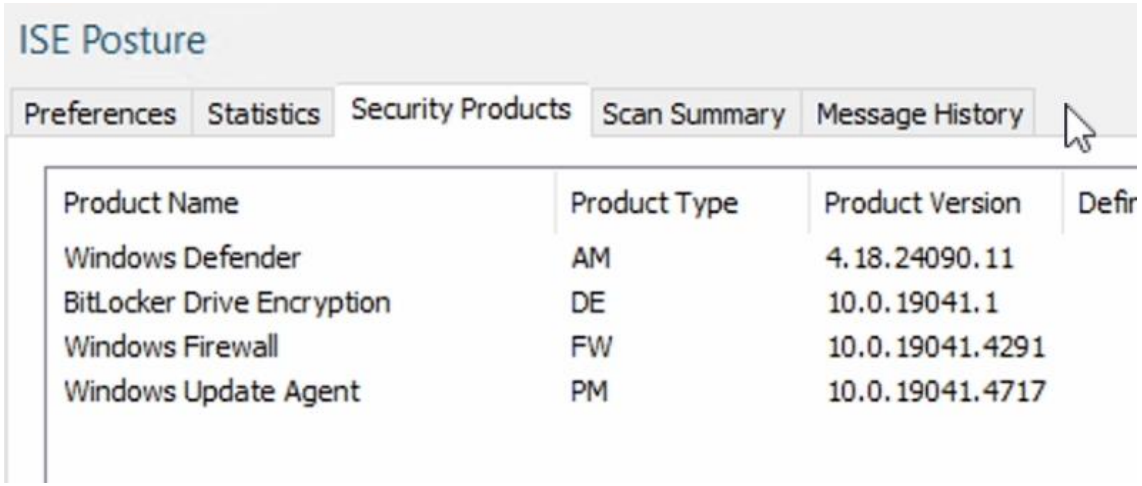


Monitoreo y Reportes: Módulo de ISE Posture

Detalles del estado de posture.

Secure Client > ISE Posture > Statistics / Security Products

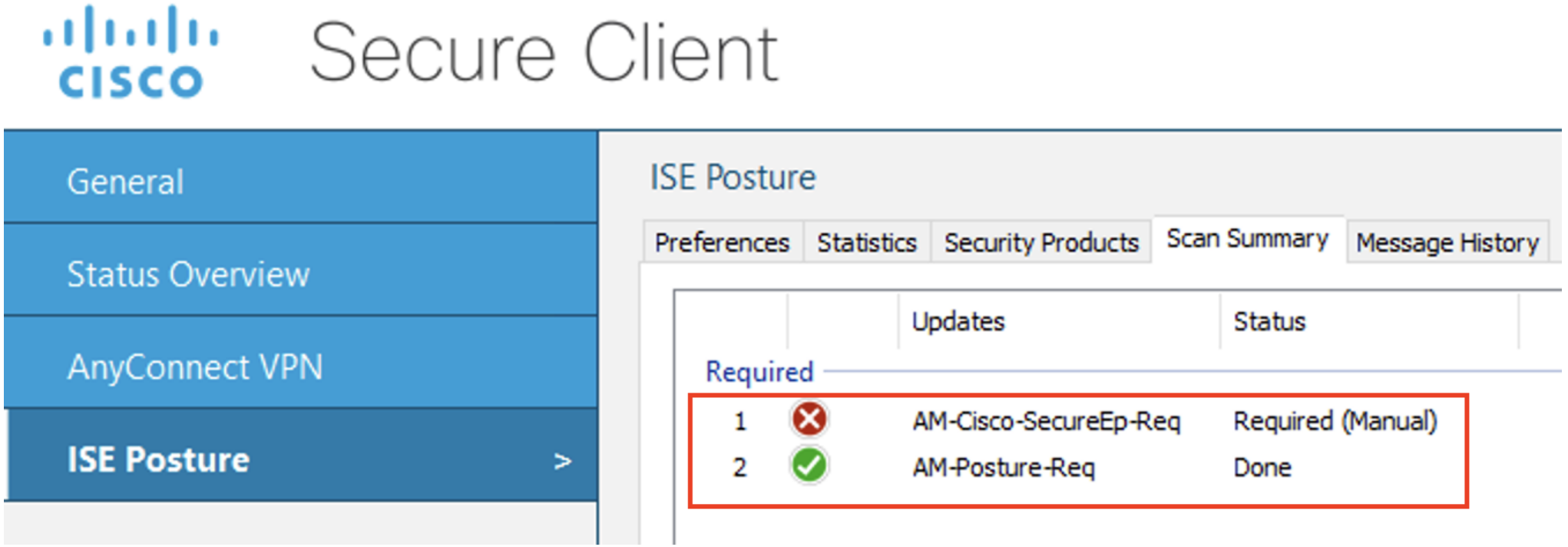




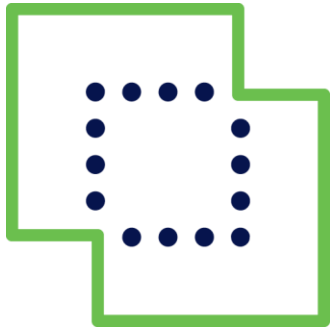
Monitoreo y Reportes: Módulo de ISE Posture

Detalles del estado de posture.

Secure Client > ISE Posture > Scan Summary



FTD: Detalles de la sesión y atributos aplicados



Monitoreo y Reportes: FTD detalles de la sesión

Detalles de la sesión y atributos aplicados

Conexión ssh al FTD > show vpn-sessiondb detail anyconnect (opcional + filter name <nombre del usuario>)

```
> show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : Usuario_Posture        Index        : 182
Assigned IP  : 192.168.21.10          Public IP    : [redacted]
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 15558                  Bytes Rx     : 6093
Pkts Tx      : 2                      Pkts Rx      : 15
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : FTD1 Split             Tunnel Group : ISE POSTURE
Login Time   : 03:37:48 UTC Wed Oct 30 2024
Duration     : 0h:00m:59s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0c046229000b60006721aa0c
Security Grp : none                   Tunnel Zone  : 0
```

Monitoreo y Reportes: FTD detalles de la sesión

Detalles de los atributos de redirección

Conexión ssh al FTD > show vpn-sessiondb detail anyconnect (opcional + filter name <nombre del usuario>)

```
ISE Posture:
  Redirect URL : https://ISE-Vedo.cisco.com:8443/portal/gateway?sessionId=0c046229000b60006721aa0c&portal=ee39fd08-7180...
  Redirect ACL : PostureRedirectACL
```

Monitoreo y Reportes: FTD detalles de la sesión

Detalles de los atributos del estado de postura ejemplo, non-compliant

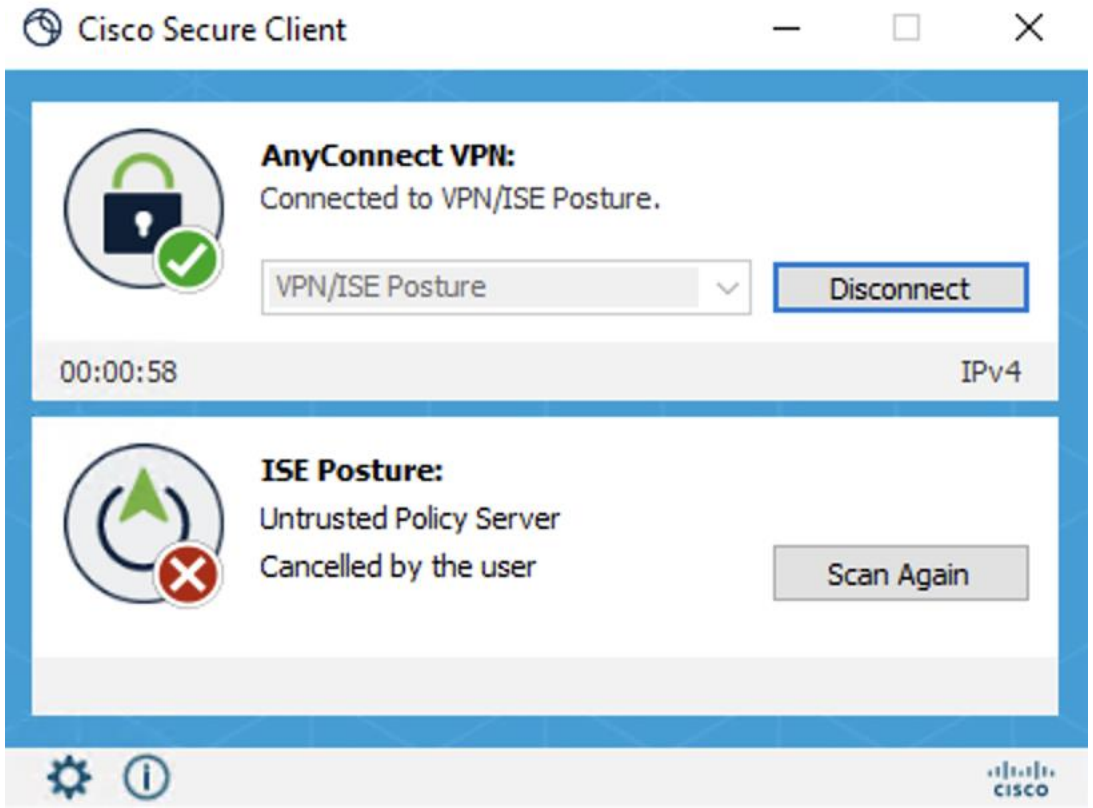
Conexión ssh al FTD > show vpn-sessiondb detail anyconnect (opcional + filter name <nombre del usuario>)

```
SSL-Tunnel:
  Tunnel ID    : 182.2
  Assigned IP  : 192.168.21.10          Public IP    : [redacted]
  Encryption   : AES-GCM-128            Hashing      : SHA256
  Ciphersuite  : TLS_AES_128_GCM_SHA256
  Encapsulation: TLSv1.3                TCP Src Port : 50070
  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 5.1.6.103
  Bytes Tx     : 7779                   Bytes Rx     : 6093
  Pkts Tx      : 1                      Pkts Rx      : 15
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PostureNonCompliant-66f8b3f9

DTLS-Tunnel:
  Tunnel ID    : 182.3
  Assigned IP  : 192.168.21.10          Public IP    : [redacted]
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 58694
  UDP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 25 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
  Bytes Tx     : 455                    Bytes Rx     : 574
  Pkts Tx      : 4                      Pkts Rx      : 6
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PostureNonCompliant-66f8b3f9
```

Mejores Prácticas y Troubleshooting

Secure Client: conexión a un servidor no reconocido

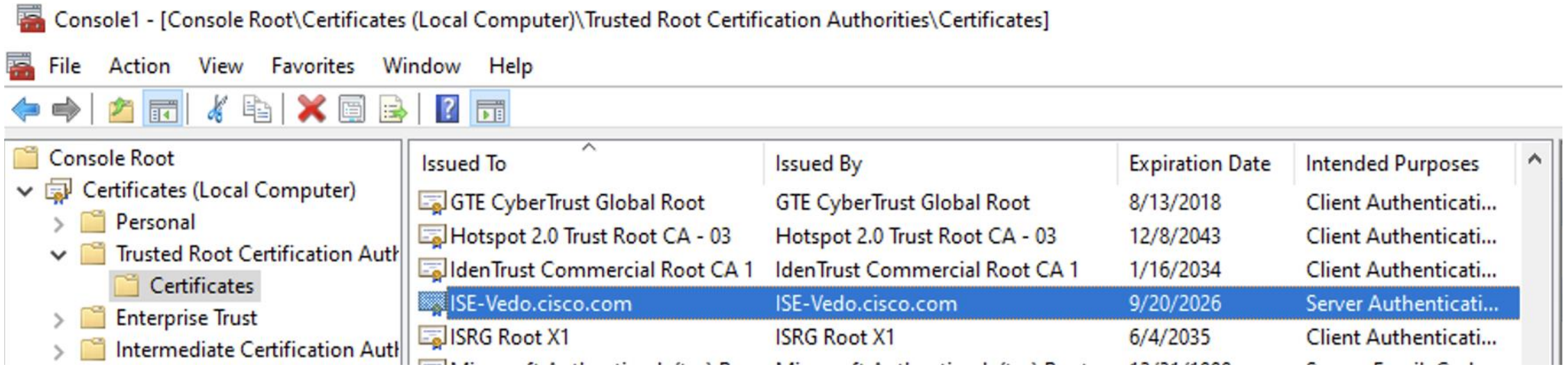


Secure Client: Untrusted Server Connection

Ocurre cuando el equipo no puede verificar el certificado Admin y Portal del servidor en que se está haciendo posture.

¿Qué verificar?

1) Instalación de certificados

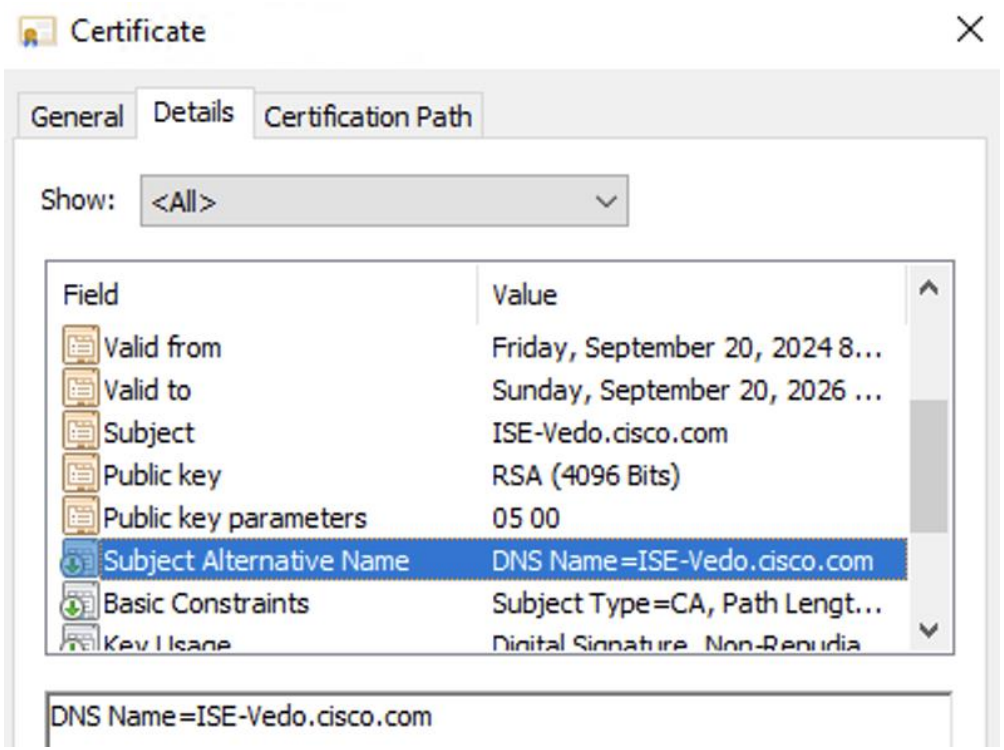


Secure Client: Untrusted Server Connection

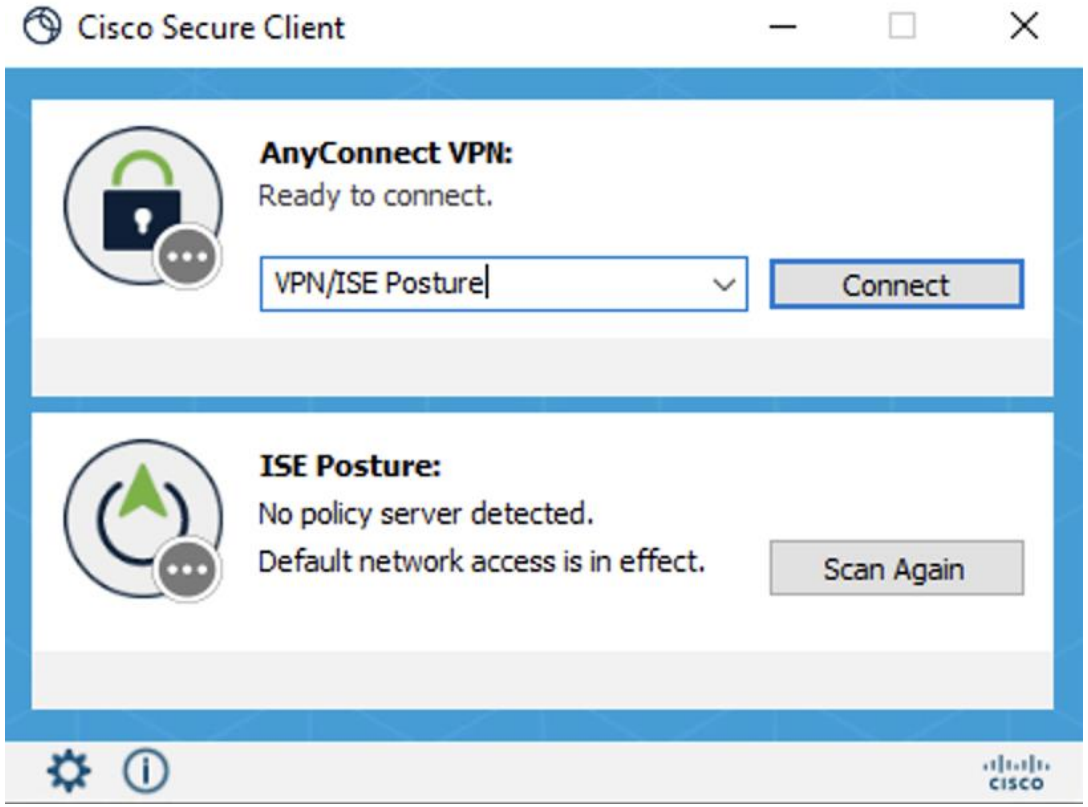
Ocurre cuando el equipo no puede verificar el certificado Admin y Portal del servidor en que se está haciendo posture.

¿Qué verificar?

2) Campos del certificado



Secure Client: Servidor no encontrado



Secure Client: No Policy Server Detected

SC (dispositivo) no puede comunicarse y / o encontrar los servidores ISE, generalmente porque los métodos de descubrimiento fallan.

¿Qué Verificar?

1) Lista de Acceso de Redirección

Name

PostureRedirectACL

Entries (3)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Block	Any	Any	Any	DNS_over_UDP	Any	Any	Any
2	Block	any-ipv4	Any	ISE_PSN	Any	Any	Any	Any
3	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any

Allow Overrides

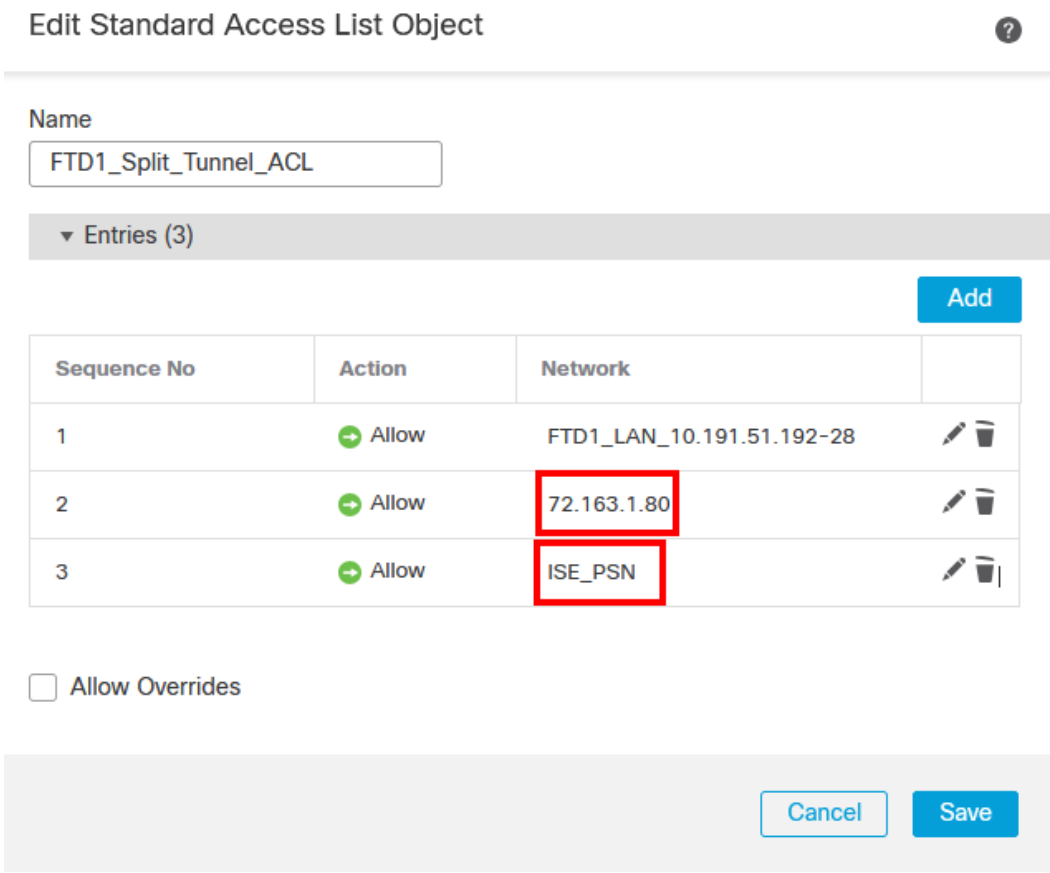
Cancel Save

Secure Client: No Policy Server Detected

SC (dispositivo) no puede comunicarse y / o encontrar los servidores ISE, generalmente porque los métodos de descubrimiento fallan.

¿Qué Verificar?

2) La Lista de Acceso del Túnel



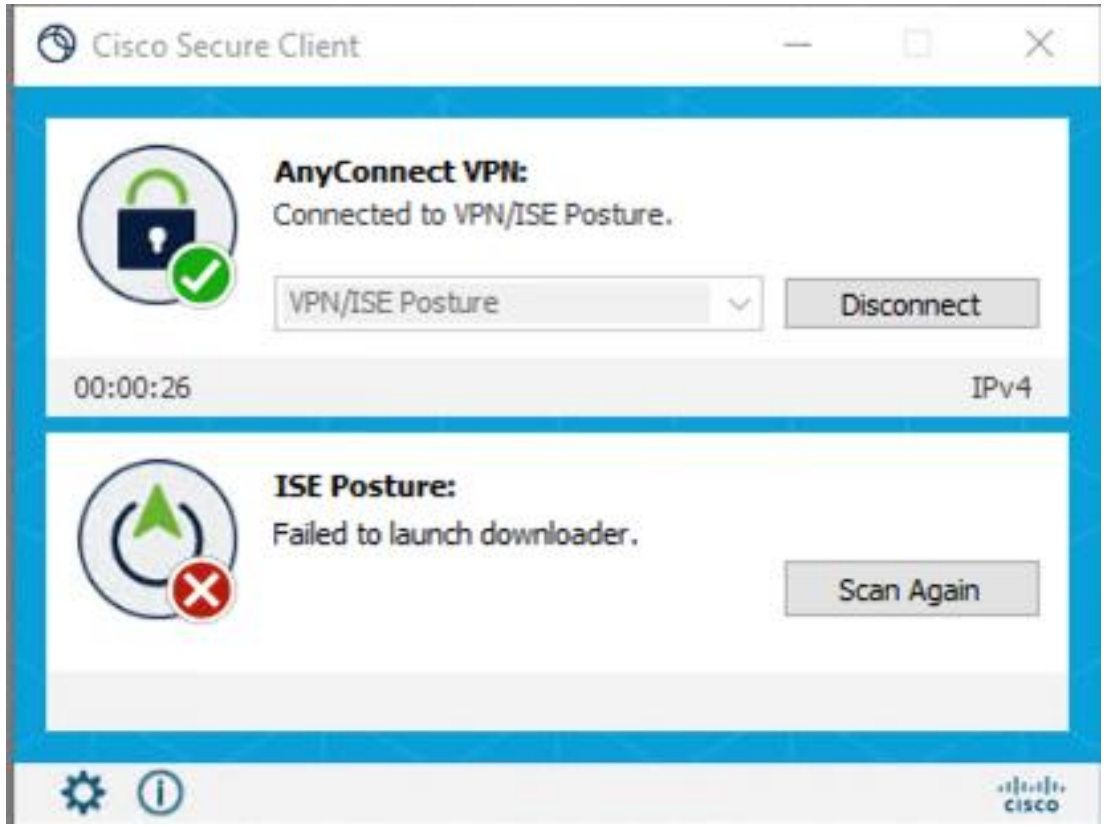
Secure Client: No Policy Server Detected

SC (dispositivo) no puede comunicarse y / o encontrar los servidores ISE, generalmente porque los métodos de descubrimiento fallan.

¿Qué Verificar?

3) En escenarios con FW, que el tráfico http y tcp puerto 8443 está siendo permitido entre el dispositivo y los servidores ISE

Secure Client: Falla al descargar los módulos

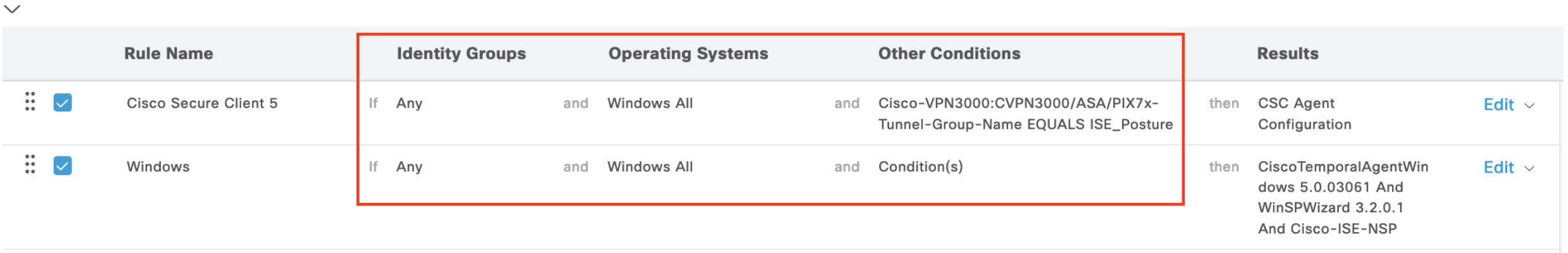


Secure Client: Failed to Launch Downloader

Generalmente ocurre por problemas de provisionamiento, Secure Client o Compliance Module

¿Qué Verificar?

1) Reglas de provisionamiento



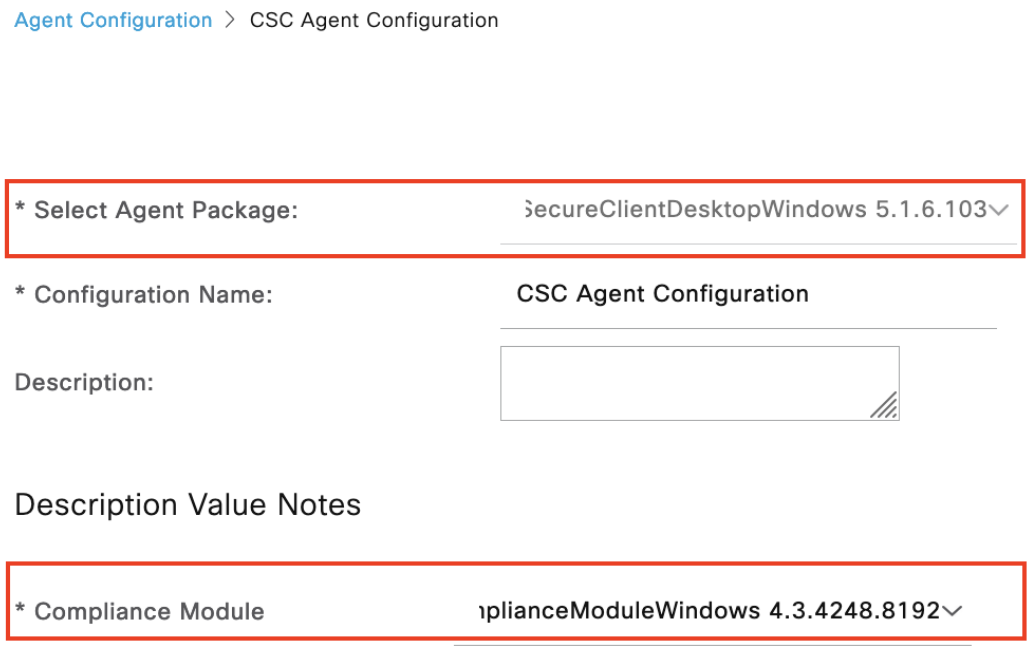
	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
⠿ ☑	Cisco Secure Client 5	If	Any	and	Windows All	and	Cisco-VPN3000:CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS ISE_Posture	then	CSC Agent Configuration	Edit
⠿ ☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	CiscoTemporalAgentWindows 5.0.03061 And WinSPWizard 3.2.0.1 And Cisco-ISE-NSP	Edit

Secure Client: Failed to Launch Downloader

Generalmente ocurre por problemas de provisionamiento, Secure Client o Compliance Module

¿Qué Verificar?

2) Provisionamiento ISE y FTD/FMC.



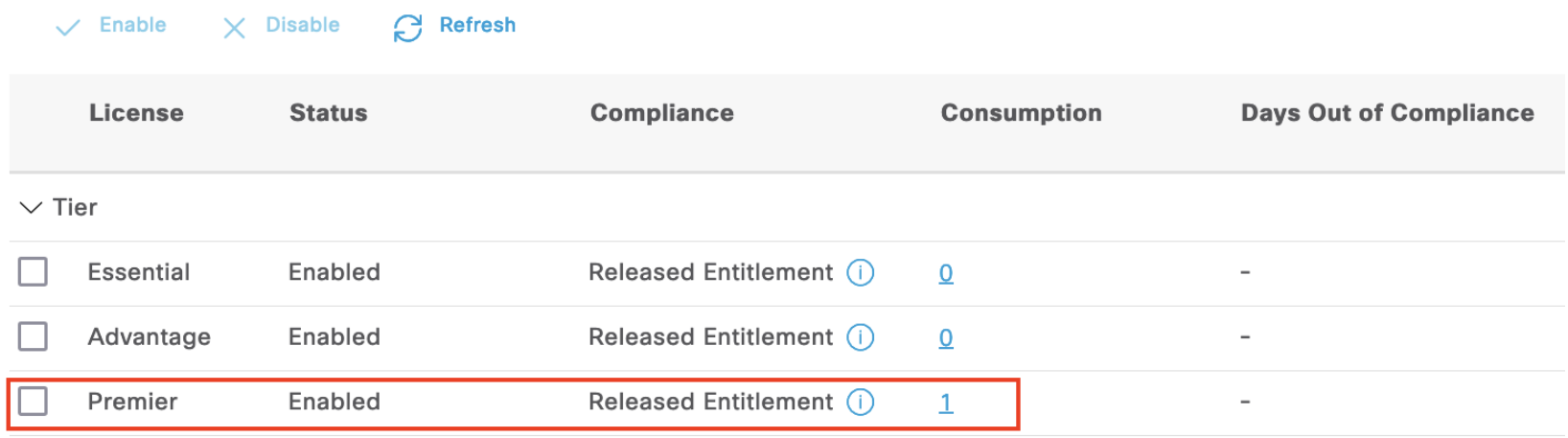
Secure Client: Errores en el servidor ISE

Secure Client: Internal Server Error

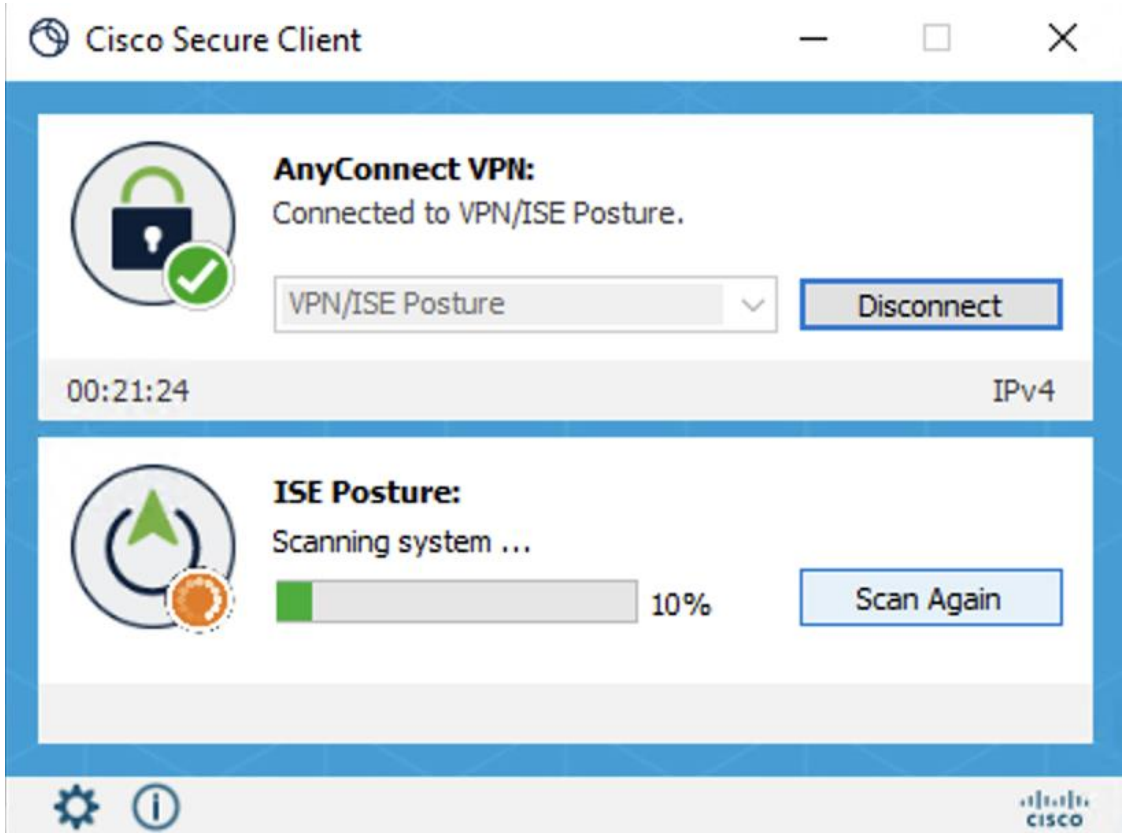
Generalmente ocurre por problemas en el nodo PSN de ISE.

¿Qué Verificar?

1) Licenciamiento en los servidores de ISE para Posture



Secure Client: Scan atascado.

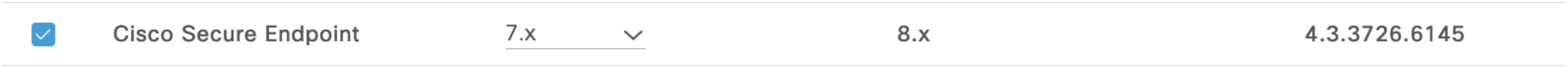


Secure Client: Scan detenido en cierto porcentaje

Generalmente ocurre por problemas en Secure Client o en el dispositivo.

¿Qué Verificar?

1) Módulo de Cumplimiento adecuado

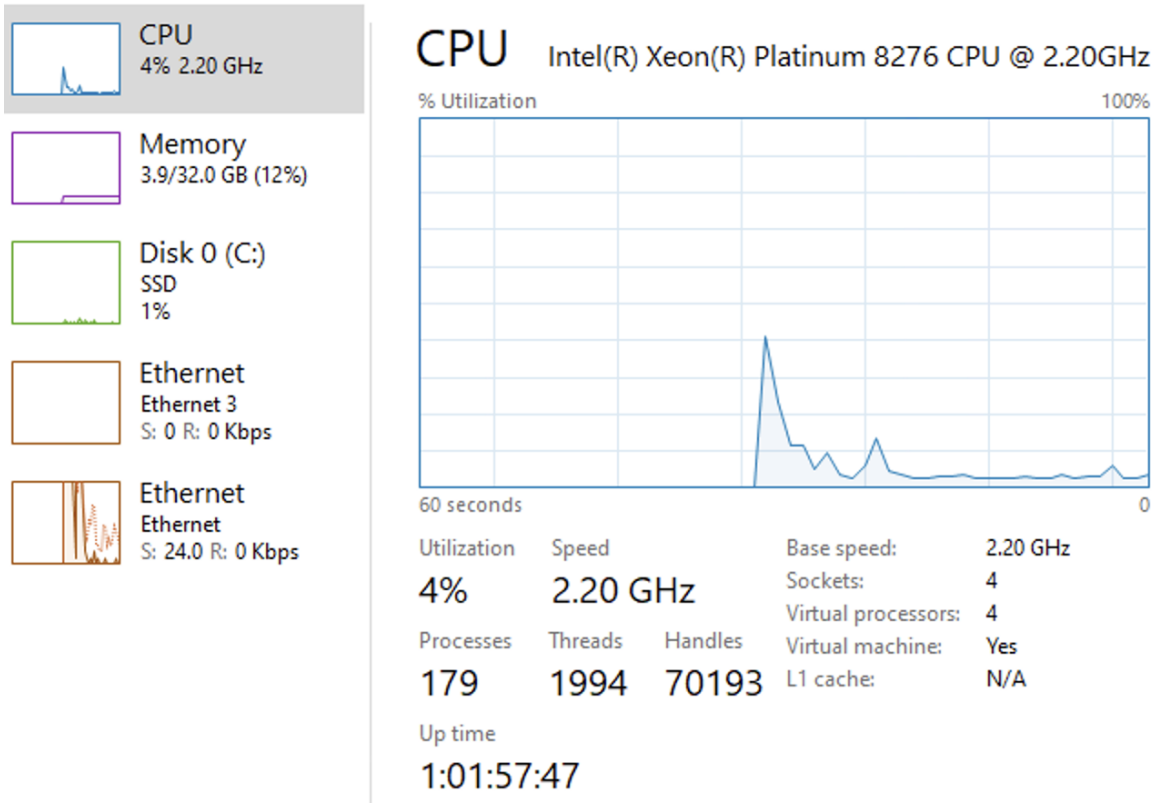


Secure Client: Scan detenido en cierto porcentaje

Generalmente ocurre por problemas en Secure Client o en el dispositivo.

¿Qué Verificar?

2) Rendimiento en el dispositivo



Secure Client: Scan detenido en cierto porcentaje

Generalmente ocurre por problemas en Secure Client o en el dispositivo.

¿Qué Verificar?

3) Secure Client ISE posture este en la lista de programas permitidos por AV/AM

Q&A

¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar

¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) y ¡mande sus dudas antes del viernes de la próxima semana!

Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.

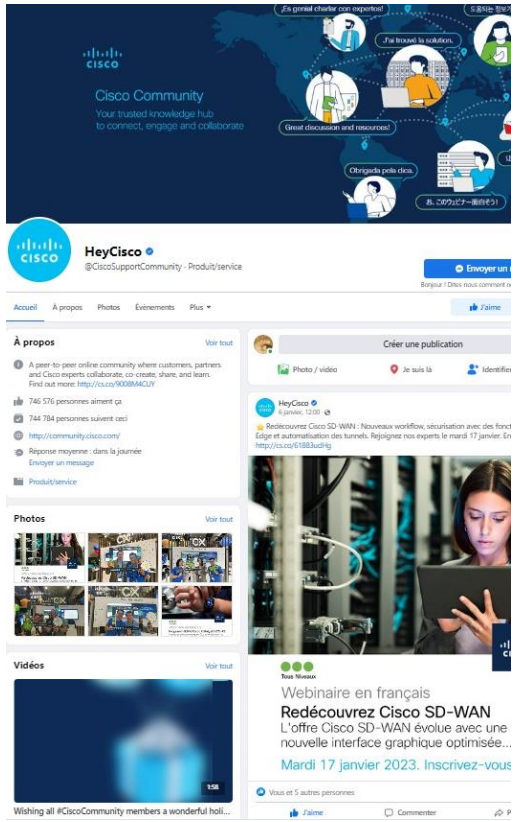
Nuestras Redes Sociales

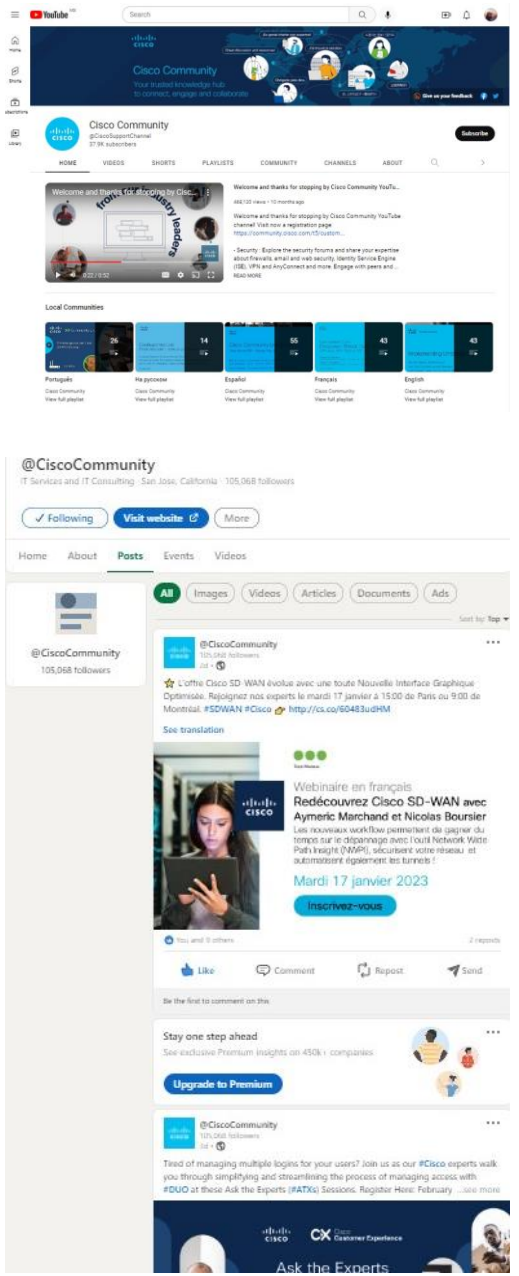
LinkedIn
[Cisco Community]

Twitter
[@CiscoCommunity]

YouTube
[CiscoCommunity]

Facebook
[CiscoCommunity]






CISCO