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

Sommario	
Introduzione	
Prerequisiti	
Requisiti	
Componenti usati	
Configurazione	
Esempio di rete e flusso del traffico	
Configurazioni	
<u>FTD/FMC</u>	
<u>ISE</u>	
Verifica	
Risoluzione dei problemi	

Introduzione

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

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

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

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

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

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

Configurazione

Win10 with FTD ISE AnyConnect Ć Internet VPN Authentication **RADIUS Access-Request** 2 1 3 **RADIUS Access-Accept** Policy Evaluation cisco-av-pair = url-redirect-acl=<Redirect_ALC_Name> Selected policy: cisco-av-pair = url-redirect=<Redirect URL> FTD-VPN-Posture-DACL (optional) Unknown RADIUS Access-Request/Access-Accept for DACL User redirected to ISE 5 Posture/Compliance Module downloaded and installed Posture check triggered and report is sent 6 RADIUS CoA Push with new set of attributes 7 8 Redirect is removed New set of attributes are applied

Esempio di rete e flusso del traffico

- 1. L'utente remoto usa Cisco Anyconnect per l'accesso VPN al FTD.
- 2. L'FTD invia all'ISE una richiesta di accesso RADIUS per tale utente.

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

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

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

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

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

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

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

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

Configurazioni

FTD/FMC

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

Overview Analysis Po	licies	s Devices Objects AM	1P Intelligence					
Object Management	ntrus	sion Rules						
Network A network object represents of	one o	r more IP addresses. Network obj	jects are used in va	rious places, includ	ing access control p	policies, network va	riables, intrusio	n rules, identity rules, ne
Extended		Name					Valu	e
Standard		any-ipv4					0.0.0	0.0/0
Address Pools		any-ipv6					::/0	
IPv6 Pools		enroll.cisco.com					72.1	63.1.80
Application Filters		IPv4-Benchmark-Tests	Edit Network	Object				? ×
Cipher Suite List		IPv4-Link-Local	Name	ISE PSN				
Community List		IPv4-Multicast	Description					
Individual Objects		IPv4-Private-10.0.0.0-8						
Object Groups Object Group		IPv4-Private-172.16.0.0-12	Network	• Host	C Range	C Network	C FQDN	
File List		IPv4-Private-192.168.0.0-16		192.168.15.14				
FlexConfig FlexConfig Object Toxt Object		IPv4-Private-All-RFC1918	Allow Overrides	•	J		Save	Cancel
Geolocation		IPv6-IPv4-Mapped					::!!!!	:0.0.0.0/96
Interface		IPv6-Link-Local					fe80	::/10
Network		IPv6-Private-Unique-Local-Addr	esses				fc00:	::/7
Þ 🖉 PKI		IPv6-to-IPv4-Relay-Anycast					192.	88.99.0/24

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

restituito dal risultato dell'autorizzazione ISE.

Overview Analysis Policies Devices Obj	jects AMP Intelligence				
Object Management Intrusion Rules					
Extended An access list object, also known as an access control Supports IPv4 and IPv6 addresses. You use these obje	list (ACL), selects the traffic to which	h a service will apply. Standard-Ide ures, such as route maps.	ntifies traffic based on destinati	ion address only. Identifies traffic based	Extended Access List
Access List New Extended	d Access List Object				? ×
Extended					
Standard Name	fyusifovredirect				
IPv4 Pools					O Add
Application Filters	Action Source	Source Port	Destination	Destination Port	
Y AS Path		No record	le to dieplay		
💮 Cipher Suite List		NO TECOL	is to display		
and Community List					
Distinguished Name					
Individual Objects					
Object Groups					
Allow Overrides	• 🗖				
C File List				Sauce	Cancel
A Sy HexConfig				Save	Cancer

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

Add Extended Access List Entry					? ×
Action: X Block	¥				
Logging: Default					
Log Level: Informational	Ŧ				
Log Interval: 300	Sec.				
Network Port					
Available Networks 🖒	٢	Source Networks (1)	Des	stination Networks (1)	
Search by name or value		💭 any-ipv4	6	ISE_PSN	
any 🔁	<u> </u>				
any-ipv4					
any-ipv6	Add to Source				
enroll.cisco.com	Add to				
IPv4-Benchmark-Tests	Destination				
IPv4-Link-Local					
IPv4-Multicast					
IPv4-Private-10.0.0.0-8					
IPv4-Private-172.16.0.0-12	•	Enter an IP address	Add Ent	ter an IP address	Add
				Add	Cancel

ime	fyusifovre	direct				
itries (4)						O Ad
Sequence	Action	Source	Source Port	Destination	Destination Port	
1	🗙 Block	🖶 any	Any	Any	DNS_over_UDP	a 🖉
2	🗙 Block	💭 any-ipv4	Any	ISE_PSN	Any	a 6
3	🗙 Block	any-ipv4	Any	RemediationServers	Any	a 🖉
4	🖌 Allow	📰 any-ipv4	Any	any-ipv4	Апу	0

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

E	dit RADIUS Server Group			? X
	Name:*	ISE		
	Description:			
	Group Accounting Mode:	Single	•	
	Retry Interval:*	10	(1-10) Seconds	
	Realms:		 Image: A set of the set of the	
	Enable authorize only			
	Enable interim account update			
	Interval:*	24	(1-120) hours	
	🗹 Enable dynamic authorization			
	Port:*	1700	(1024-65535)	
	RADIUS Servers (Maximum 16 servers)	vers)		
	IP Address/Hostname			
		No records to display		
			Save	Cancel

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

New RADIUS Server			? ×
IP Address/Hostname:*	192.168.15.13 Configure DNC at Three	at Defense Platform Settings	to resolve hostname
Authentication Port:*	1812		(1-65535)
Key:*	•••••		
Confirm Key:*	•••••		
Accounting Port:	1813		(1-65535)
Timeout:	10		(1-300) Seconds
Connect using:	C Routing 💿 Spe	ecific Interface 🕕	
	ZONE-INSIDE		▼ ⊙-
Redirect ACL:	fyusifovredirect		▼ ②
		Save	Cancel

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

Overview Analysis Policies Devices	Dbjects AMP Intelligence			Deploy 🔒 Sy
Object Management Intrusion Rules				
IPv4 Pools IPv4 pool contains list of IPv4 addresses, it is used	for diagnostic interface with clustering, or for VPN remote acc	ess profiles.		Add IPv4 Pools
Standard Name			Value	
Address Pools Edit IPv4 Po	ol	? ×	172.16.1.10-172.16.1.20	
IPv4 Pools Application Filters Y AS Path Cipher Suite List Community List Object Groups Mask Description File List PrexConfig PlexConfig PlexConfig PlexConfig Configure 4 Shared a Override (0)	Range* VPN-172-Pool 172.16.1.10-172.16.1.20 Format: ipaddr-ipaddr e.g., 10 72.1.1-10.72.1.150 255.255.255.0 evice overrides in the address pool object to avoid IP address pross multiple devices	conflicts in case of object		

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

pacchetto, scaricare il pacchetto da <u>Cisco Software Download</u> e selezionare Anyconnect Client Image File Type (Tipo di file immagine client Anyconnect).

Overview Analysis Policie	s Devices Objec	ts AMP Intelligence			Deploy 🌒 Sy
Object Management Intru	sion Rules				
AnyConnect File File objects represent files used in	configurations, typicall	r for remote access VPN policies. They can	contain AnyConnect C	lient Profile and AnyConnect Client Image files.	Add AnyConnect File
Policy List	Name				Value
A Derefix List	Edit AnyConnect	File	? ×		anyconnect-win-4.7.01076-webdepl
 IPv4 Prefix List IPv6 Prefix List RADIUS Server Group Route Map Security Intelligence DNS Lists and Feeds Network Lists and Feeds Sinkhole SIA Monitor Time Range Tunnel Zone URL Variable Set VLAN Tag VPN AnyConnect File R' Certificate Map 	Name:* File Name:* File Type:* Description:	AC47 anyconnect-win-4.7.01076-webdeploy-k AnyConnect Client Image	9. Browse		

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

Overview Analysis P	olicies Devices Objects AMP Intelligence	Deploy 🦺 Sy
Object Management	ntrusion Rules	
Cert Enrollment A certificate enrollment obje	t contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate	Signing Requests (CSRs) and obtaining Identity Certificates fr
Access List	Add Cert Enrollment ? ×	Туре
Address Pools Application Filters	Name* vpn-cert	Self Signed Ce
Y AS Path	Description	
Community List	CA Information Certificate Parameters Key Revocation	
DNS Server Group	Enrollment Type: Self Signed Certificate	
 File List FlexConfig 	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.	
Geolocation		
Key Chain		
PKI Cert Enrollment		
External Cert Group	5	
Thternal CA Groups		
Internal CAs		
Internal Cert Group		
Trusted CA Groups	Allow Overrides	
Trusted CAs		
Policy List		
all Port	Save	Displaying 1 - 1 of 1 rows 🛛 🐇

1	Add Cert Enrollme	nt						? ×
	Name*	vpr	-cert					
	Description							
	CA Information	Certific	ate Parameters	Key	Revocation			
	Include FQDN:		Use Device Hostna	me as f	-QDN		~	
	Include Device's IP	Address:	10.48.26.99					
	Common Name (CN	l):	vpn-cert.example.	com				
	Organization Unit (O)U):						
	Organization (O):		example					
	Locality (L):							
	State (ST):		Krakow					
	Country Code (C):		PL					
	Email (E):							
	Include Device's	Serial Nu	mber					
	Allow Overrides							
						Save		Cancel

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

Overview Analysis	Policies	Devices Objects	AMP	Intelligence		(Deploy	e ,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN ► Remote Access	QoS	Platform Settings	FlexConfig	Certificates					
										0	Add
Name				Status		Last Modified					
	No configuration available Add a new configuration										

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

Remote Access VPN Policy Wizard	
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary	
Targeted Devices and Protocols This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile. Name:* EmployeeVPN Description: VPN Protocols: Y SL VPN Protocols: Y SL I Psec-IKEv2 Targeted Devices: Available Devices Selected Devices YPN Protocols: Y SL I Psec-IKEv2 Targeted Devices: Yearch Yearch Yearch Yearch Yearch Yearch	<section-header><section-header><section-header><text><text><section-header><text><section-header><text></text></section-header></text></section-header></text></text></section-header></section-header></section-header>
	Back Next Cancel

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

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

1) Policy Assignment 2 Connection Profile	3 AnyConnect A A	Access & Certificate S Summary	
	Connection Profile:		
	Connection Profiles specify the itself, how AAA is accomplished group policies.	e tunnel group policies for a VPN connection. These policies pertain to creating the tunnel ad and how addresses are assigned. They also include user attributes, which are defined in	
	Connection Profile Name:*	EmployeeVPN	
		This name is configured as a connection alias, it can be used to connect to the VPN gateway	
	Authentication, Authorization 8	N Accounting (AAA):	
	Specify the method of authentic connections.	ntication (AAA, certificates or both), and the AAA servers that will be used for VPN	
	Authentication Method:	AAA Only	
	Authentication Server:*	* ISE (Realm or RADIUS)	
	Authorization Server:	Use same authentication serve: 🗹 🚱 (RADIUS)	
	Accounting Server:	ISE (RADIUS)	
	Client Address Assignment:		
	Client IP address can be assign selected, IP address assignment	gned from AAA server, DHCP server and IP address pools. When multiple options are rent is tried in the order of AAA server, DHCP server and IP address pool.	
	Use AAA Server (RADII	DIUS only) 0	
	Use DHCP Servers		
	Use IP Address Pools	s	
	IPv4 Address	VPN-172-Pool	
	IPv6 Address		
	Group Policy:		
	A group policy is a collection of established. Select or create a	of user-oriented session attributes which are assigned to client when a VPN connection is a Group Policy object.	
	Group Policy:*	DfttGrpPolicy V Edit Group Policy	

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

Remote Access VPN Policy Wizard		
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary		
Remote User AnyConnect Client Internet Outside VPN Device Inside Corporate Resources		
AnyConnect Client Image The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN 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 huttons		
AnyConnect File Object Name AnyConnect Client Package Name Operating System		
C47 anyconnect-win-4.7.01076-webdeploy-k9 Windows		
	Back	Next

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

Remote Access VPN Policy Wizard			
1 Policy Assignment 2 2 Connection Profile 3 AnyConnect 3 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: Interface Broup/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 VEN gateway Certificate Enrollment:* Vpn-cert Vpn-cert Vm 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. Sypass 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 VVW traffic.			
	Back	Next	Cancel

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

Remote Access VPN Policy Con	Additional Configuration Requirements
Firepower Management Center wi Name: Device Targets: Connection Profile: Connection Alias: AAA: Authentication Method: Authentication Server: Authentication Server: Accounting Server: Accounting Server: Address Assignment: Address Assignment: Address Pools (IPv4): Address Pools (IPv4): Address Pools (IPv6): Group Policy: AnyConnect Images: Interface Objects: Device Certificates:	 After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets. Access Control Policy Update Access Control Policy Update Matter Configuration OPS Configuration To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlaxConfig Policy on the targeted devices. Port Configuration SSL will be enabled on port 443. Please ensure that these ports are not used in MAT Policy or other services before deploying the configuration. Metwork Interface Configuration Make sure to add interface from targeted devices to SecurityZone object "ZONE-OUTSIDE"

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

Overview Analysis Policies Devi	ces Objects AMP Intelligence				Deploy 🔩 System Help 🔻 admin 🔻
Device Management NAT VPN >	Remote Access QoS Platform Settings FlexCo	onfig Certificates			Save Save
Enter Description	Deploy Policies Version:2020-02-02 09:15 PM				? X
	✓ Device	Inspect Interruption	Type Group	Current Version	Policy Assignments (1)
Connection Profile Access Interfac		No	FTD	2020-02-02 09:10 PM	
					0
Name					
DefaultWEBVPNGroup					/ 6
EmployeeVPN					/8
	Coloring devices 1				
	Selected devices: 1			Deploy Cancel	

ISE

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

Posture Updates				
Web Offline				
* Update Feed URL https://www.cisco.com/	web/secure/spa/posture-update.xml Set to Default			
Proxy Address	(i)			
Proxy Port	HH MM SS			
Automatically check for updates starting fro	om initial delay 20 v 49 v 18 v every 2 hours (i)			
Save Update Now Reset				
▼ Update Information				
Last successful update on	2020/02/02 20:44:27(i)			
Last update status since ISE was started	Last update attempt at 2020/02/02 20:44:27 was successful ()			
Cisco conditions version	257951.0.0.0			
Cisco AV/AS support chart version for windows	227.0.0.0			
Cisco AV/AS support chart version for Mac OS)	(148.0.0.0			

Cisco supported OS version 49.0.0.0

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

Download Remote Resources	×
Name 🔺	Description
AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
AnyConnectComplianceModuleOSX 4.3.972.4353	AnyConnect OSX Compliance Module 4.3.972.4353
AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2
AnyConnectComplianceModuleWindows 4.3.1053.6145	AnyConnect Windows Compliance Module 4.3.1053.6145
CiscoTemporalAgentOSX 4.8.03009	Cisco Temporal Agent for OSX With CM: 4.3.972.4353
CiscoTemporalAgentWindows 4.8.03009	Cisco Temporal Agent for Windows With CM: 4.3.1053.6145
ComplianceModule 3.6.11428.2	NACAgent ComplianceModule v3.6.11428.2 for Windows
MACComplianceModule 3.6.11428.2	MACAgent ComplianceModule v3.6.11428.2 for MAC OSX
MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Ab
MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3
MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Rele
MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Pat
For AnyConnect software, please download from http://cisco.com	n/go/anyconnect. Use the "Agent resource from local disk" add
option, to import into ISE	
	Save Cancel

Passaggio 3. Scarica AnyConnect da <u>Cisco Software Download</u>, quindi caricalo in ISE. Passare a Criteri > Elementi criteri > Risultati > Provisioning client > Risorse.

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

Agent Resources From Lo Agent Resources Fro	ocal Disk > Agent Resources From Local Disk om Local Disk				
Cate	Cisco Provided Packages	•			
	Browse anyconnect-win-4.7.01	076-webdeploy-k9.pkg			
	 AnyConnect Uploaded Resource 	25			
	Name	Туре	Version	Description	
	AnyConnectDesktopWindows 4.7.10	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secure Mobility Clie	



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

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

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

ISE Posture	Agent Profile Settings > AC_Posture_Profil	e
* Name: Description	AC Posture Profile	1

Posture Protocol

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

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



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	*	1
Network Visibility	.	1
Umbrella Roaming Security	.	
Customer Feedback	*	1

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

alta cisc	dent	tity Services Engine	Home	Contex	xt Visibility	 Operations 	- Policy		Administration	 Work Centers 			License Warning 🔺	Q	0	•	φ.
Pol	icy Sets	Profiling Posture	Client Provis	ioning	Policy Eleme	ents											
Clier Defin For A For N	nt Provi le the Clie gent Con lative Sup	sioning Policy ent Provisioning Policy to figuration: version of age plicant Configuration: wi	determine wh int, agent profi izard profile an	at users wil le, agent co id/or wizard.	II receive upo mpliance mo Drag and dri	n login and user : dule, and/or ager op rules to chang	session initia nt customizati je the order.	tion: on pac	ckage.								
•		Rule Name		Identity C	Groups	Operating Sy	ystems		Other Condition	ns		Results					
	~	AC_47_Win	If	Any	an	Windows All		and	Condition(s)		then	AC_CF_47				Edit 🕶	
I	~	IOS	lf	Any	an	Apple iOS Al	1	and	Condition(s)		then	Cisco-ISE-NSP				Edit •	
1	~	Android	lf	Any	an	Android		and	Condition(s)		then	Cisco-ISE-NSP				Edit •	
		Windows	If	Any	an	Windows All		and	Condition(s)		then	CiscoTemporalAgentWi ndows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP				Edit 🕶	
		MAC OS	If	Any	an	Mac OSX		and	Condition(s)		then	CiscoTemporalAgentO SX 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE- NSP				Edit 🕶	
1		Chromebook	If	Any	an	Chrome OS	All	and	Condition(s)		then	Cisco-ISE-Chrome- NSP				Edit 🕶	

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

.

cisco identity services Engline H	iome Context Visibility	Operations Policy	Administration	 Work Centers
Policy Sets Profiling Posture Client	t Provisioning			
Dictionaries Conditions Results				
Library Conditions Smart Conditions Time and Date Profiling ✓ Posture Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Disk Encryption Condition File Condition Firewall Condition	Anti-Malware Conditions	Description Any AM installation che Any AM definition che Any AM installation che Any AM definition chec	eck on Wi ck on Wind eck on Mac ck on Mac	

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

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

cisco Identity Services Engine	Home Context Visibility	Operations Policy	Administration Work Centers		License Warning 🔺 🔍	. 🛛 o	•
Policy Sets Profiling Posture Cli	ent Provisioning Policy Element	5					
Dictionaries + Conditions - Result	s						
0							
Authentication					v		P
	Requirements						
 Authorization 	Name	Operating Systems	Compliance Module	Posture			
	Wessage Text Only	Conditions	Remediation Actions			Edit 🔻	-
► Profiling	Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_def	then	
✓ Posture	AnyAVDefRemediationMa c					Edit 🕶	-
- Remediation Actions	Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_inst	then	
- Remediation Actions	Message Text Only					Edit 🔻	()
Requirements	Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_def	then	
Client Provisioning	AnyASDefRemediationMa c					Edit 🕶	1
	Any_AM_Installation_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_inst	then	
	Message Text Only					Edit 🔻	
	Any_AM_Definition_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_def	then	
	AnyAMDefRemediationWi n					Edit 👻	
	Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_inst	then	
	Message Text Only					Edit 🔻	
	Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_def	then	
	AnyAMDefRemediationM					Edit •	-

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

dhahi cisco identit	y Services Engine	Home	ity Operations	▼Policy → Admin	istration + Work Centers					License Warning 🔺	Q, (90	0
Policy Sets	Profiling Postur	e Client Provisioning + Poli	icy Elements										
Posture Poli	CY.												
Define the Pos	ture Policy by config	guring rules based on operating sy	ystem and/or other or	onditions.									م
*													-
Status	Policy Options	Rule Name	Identity Groups	Operating System	ns Compliance Mod	dule Posture Type	Other Conditi	ons	Requirements				-
0	Policy Options	Default_AntiMalware_Policy If _Mac	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then	Any_AM_Installation_ Mac			Edit	•
0	Policy Options	Default_AntiMalware_Policy If _Mac_temporal	Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then	Any_AM_Installation_ Mac_temporal			Edit	•
	Policy Options	Default_AntiMalware_Policy If _Win	Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Any_AM_Installation_ Win			Edit	•
0	Policy Options	Default_AntiMalware_Policy If _Win_temporal	Any	and Windows All	and 4 x or later	and Temporal Agent	and	then	Any_AM_Installation_ Win_temporal			Edit	•
0	Policy Options	Default_AppVis_Policy_Mac If	Any	and Mac OSX	and 4 x or later	and AnyConnect	and	then	Default_AppVis_Requ irement_Mac			Edit	-

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

In questo esempio:

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

Downloadable ACL List > PostureNonCompliant1

Downloadable ACL

* Name	PostureUnknown
Description	
IP version	● IPv4 C IPv6 C Agnostic ①
* DACL Content	1234567 permit udg any any eq domain
	131111 permit (g any host 192, 168, 15, 14
	2 13 14 13 permit kg any any gg 00 1617181 permit kn any any en 443
	9002122
	2324252
	6272829
	3031323
	3343536
	3738394

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name	PostureNonCompliant
Description	
IP version	€ IPv4 C IPv6 C Agnostic (i)
* DACL Content	1234567 deny ig any 10.0.0.0 255.0.0.0
	2131415 denv in any 192 168 0.0 255 255 0.0
	1617/181 permit jo anv anv
	9202122
	2324252
	6272829
	3031323
	3343636
	3738394

- Name	PermitAll
Description	
IP version	⊙ IPv4 C IPv8 C Agnostic (i)
DACL Content	123456 permit jg any any
	121314
	151617
	181920
	242528
	272829
	393/36

Passaggio 12. Creare tre profili di autorizzazione per gli stati di postura non conforme, non

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

Authorization Profiles > New	v Authorization Profile					
Authorization Profile						
* Name	FTD-VPN-Redirect					
Description					11.	
* Access Type	ACCESS_ACCEPT	•				
Network Device Profile	號 Cisco 👻 🕀					
Service Template						
Track Movement	(i)					
Passive Identity Tracking	i					
 Common Tasks 						
DACL Name	Post	ureUnknown	0			
Web Redirection (CWA, N	IDM, NSP, CPP) 🥡					
Client Provisioning (Post	ture) 🔻	ACL fyu	sifovredirect] Valu	e It Provisioning Portal (default) 🔻	
 Attributes Details 						
Access Type = ACCESS_ACCEPT DACL = PostureUnknown cisco-av-pair = url-redirect-acl=fyusifov cisco-av-pair = url-redirect=https://ip:	vredirect port/portal/gateway?sessionId	=SessionIdValue&p	ortal=27b1bc30-2e58-11e9-98	fb-0050568775a	13&action=cpp	1.

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

Authorization Profiles > New Authorization Profile

Authorization Profile	
* Name	FTD-VPN-NonCompliant
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	data Cisco 👻 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
▼ Common Tasks	
DACL Name	PostureNonCompliant 📀

Attributes Details

Access Turne - ACCESS ACCEDT
ACCESS Type = ACCESS_ACCEPT
DACL = PostureNonCompliant

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

Authorization Profiles > New Authorization Profile

Authorization Profile		
* Name	PermitAll	
Description		
* Access Type	ACCESS_ACCEPT	
Network Device Profile	📩 Cisco 👻 🕀	
Service Template		
Track Movement		
Passive Identity Tracking		
 Common Tasks 		
DACL Name	PermitAll 📀	
 Attributes Details 		
Access Type = ACCESS_ACCEPT DACL = PermitAll		11.

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

alada Id	lentity Serv	rices Engine Home 🔸 C	Context Visi	bility	 Operations 		Administration	• Work Ce	nters		License Warning 🔺	۹,	0	•	ø
Policy S	ets Profi	ling Posture Client Provisionin	ig ⊧ Poli	icy Elerr	ients										
	\odot	Default	Default po	licy set							Default Network Access	i.	× * +	•	43
> Autr > Autr > Autr	nentication norization F	Policy (3) Policy - Local Exceptions Policy - Global Exceptions													
► Auth	norization f	Policy (18)													
									Results						
•	Status	Rule Name	Conditio	unditions					Profiles	Security 0	Groups		Hits	Actio	ons
Searc	sh														
				ĥ	Session Posture	Status EQU	ALS Compliant								
	0	FTD-VPN-Posture-Compliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000/ EmployeeVF	ASA/PIX7x-Tunnel-Gro PN	up-	- PermitAII	Select fro	m list 💌	+	4	4	ž
			ĥ	Session Posture	eStatus EQU	ALS NonCompliant									
	Ø	FTD-VPN-Posture-NonCompliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000// EmployeeVF	ASA/PIX7x-Tunnel-Gro PN	up-	×FTD-VPN-NonCompliant	+ Select from list		+	0	\$	¥
				ĥ	Session-Posture	Status EQU	ALS Unknown					_			
	\odot	FTD-VPN-Posture-Unknown	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000/ EmployeeVF	ASA/PIX7x-Tunnel-Gro	up-	× FTD-VPN-Redirect	Select fro	m list 💌	+	9	\$	ł

Verifica

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

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

	Home + Contex	d Visibility	 Operations 	Policy A	dministration Work Cer	nters						License Wa	ming 🔺 🤉	• • •
RADIUS Threat-Centric NAC Li	ve Logs + TACACS	S + Troubl	leshoot + Ad	aptive Network Control	Reports									
ive Logs Live Sessions														
	Misconfigured Supp	licants 0	N	isconfigured Network	Devices 0	RADIUS Dro	ps O	Cli	ent Stopped Res	ponding ()	Repeat	Counter 0		
	0			0		0			0			0		
													_	
									Refr	esh Never	Show Lates	st 20 records	 Within Last 3 	hours
Refresh O Reset Repeat Co	unts 🕹 Export To	•							Refr	esh Never	Show Lates	st 20 records	Within Last 3	Filter • O
C Refresh O Reset Repeat Co Time	unts 🛓 Export To Status	Details	Repeat	identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Refr Authorizati	P Address	Show Lates	at 20 records Device Port	Within Last 3	Filter • O Posture Sta
C Refresh O Reset Repeat Co Time	unts 🛓 Export To Status	Details	Repeat	Identity Identity	Endpoint ID Endpoint ID	Endpoint Pr Endpoint Prc	Authenticat	Authorizati	Authorizati	IP Address	Show Lates	Device Port Device Port	Within Last 3 Identity Group	Filter • O Posture Sta Posture Stat
C Refresh O Reset Repeat Co Time Feb 03, 2020 07:13:31.92	unts Z Export To Status	Details	Repeat	Identity Identity alice@training.e	Endpoint ID Endpoint ID 00:00:29:50:5A:99	Endpoint Pr Endpoint Prc Windows10	Authenticat Authenticatk Default >>	Authorizati Authorization Default >>	Refr Authorizati Authorizatior FTD-VPN-R	IP Address IP Address IP Address 172.16.1.10	Show Lates	Device Port Device Port	Within Last 3 Identity Group	Filter • O Posture Stat. Pending
C Refresh Reset Repeat Co Time Feb 03, 2020 07:13:31.82 Feb 03, 2020 07:13:29.74	unts Z Export To Status	Details	Repeat	Identity Identity alice@training.e #ACSACL#IP-P	Endpoint ID Endpoint ID 00:0C:29:5C:5A:98	Endpoint Pr Endpoint Pr. Windows10	Authenticat Authenticatic Default >>	Authorizati Authorization Default >>	Authorizati Authorization FTD-VPN-R	IP Address IP Address 172.16.1.10	Show Lates	Device Port Device Port	Within Last 3	Filter • • • • • • • • • • • • • • • • • • •

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

Overview

Event	5200 Authentication succeeded	
Username	alice@training.example.com	
Endpoint Id	00:0C:29:5C:5A:96 ⊕	
Endpoint Profile	Windows10-Workstation	
Authentication Policy	Default >> Default	
Authorization Policy	Default >> FTD-VPN-Posture-Unknown	
Authorization Result	FTD-VPN-Redirect	

Authentication Details

Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-28-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

Stato postura in sospeso.

La sezione Risultato mostra quali attributi vengono inviati a FTD.

Result	
Class	CACS:000000000000005e37c81a: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=00000000000000005e37c81a& portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp& token=0d90f1cdf40e83039a7ad6a226603112
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

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

```
<#root>
fyusifov-ftd-64#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username
             : alice@training.example.com
Index
            : 12
Assigned IP : 172.16.1.10
            Public IP
                        : 10.229.16.169
            : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
            : AnyConnect Premium
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Encryption
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
            : 0h:06m:43s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                     VLAN
                                                   : none
Audt Sess ID : 000000000000005e37c81a
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 : win Client OS 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 : userPassword Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes : Windows Client OS 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 : AES256 Encryption Hashing : SHA1 Ciphersuite : DHE-RSA-AES256-SHA UDP Src Port : 59396 Encapsulation: DTLSv1.0 : userPassword UDP Dst Port : 443 Auth Mode 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=00000000000000005e37c83 Redirect ACL : fyusifovredirect È possibile verificare i criteri di provisioning client. Passare a Operazioni > Report > Endpoint e utenti > Provisioning client.

-dealer Identity Services Engine	Home + Context Visibilit	ty Operations Policy	Administration Work Centers			License Wa	ming 🔺 🍳 😑 🧑 Ö
RADIUS Threat-Centric NAC Live	e Logs + TACACS + Tro	subleshoot	ontrol Reports				
Export Summary My Reports	Client Provisioning From 2020-02-03 00:00:00 Reports exported in last 7	0.0 to 2020-02-03 08:14:07.0 days 0				+ My Report	Export To • Schedule
• Reports							Filter - CRefresh Q-
+ Audit	Logged At	Server	Event	Identity	C Endpoint ID	IP Address	Client Provisioning Pol
Device Administration	Today 💌 🗙			Identity	Endpoint ID		
Diagnostics	2020-02-03 08:06:4	fyusifov-26-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	AC_47_Win
Endpoints and Users Authentication Summary Client Provisioning	<u> </u>					Rows/Page 1	1 at 1 Total Rows

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



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

nthelle identity Services Engine	
Posture More Detail Assessment	
From 2020-01-04 00:00:00.0 to 2020-02-03 08:13:36.0 Generated At: 2020-02-03 08:13:37.37	
Client Details	
Username	alice@training.example.com
Mac Address	00:0C:29:5C:5A:96
IP address	172.16.1.10
Location	All Locations
Session ID	00000000000c0005e37c81a
Client Operating System	Windows 10 Professional 64-bit
Client NAC Agent	AnyConnect Posture Agent for Windows 4.7.01076
PRA Enforcement	0
CoA	Received a posture report from an endpoint
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEnabled
System Name	DESKTOP-IE3556M
System Domain	n/a

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

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Authorizati	IP Address		Network Device	Device Port	Identity Group	Posture
	•			Identity	Endpoint ID	Endpoint Prc	Authenticatic	Authorization	Authorization	IP Address	•	Network Device	Device Port	Identity Group	Posture
Feb 03, 2020 08:07:52.05	~	0			10.229.16.169				PermitAccess			FTD			Complia
Feb 03, 2020 08:07:50.03	0	0	0	alice@training.e	00:0C:29:5C:5A:98	Windows10	Default >>	Default >>	FTD-VPN-R	172.16.1.10					Compliar
Feb 03, 2020 07:13:29.74		0		#ACSACL#-IP-P								FTD			
Feb 03, 2020 07:13:29.73		0		alice@training.e	00:0C:29:5C:5A:98	Windows10	Default >>	Default >>	FTD-VPN-R			FTD		Workstation	Pending

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

uthentication Details	
Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fyusifov-28-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	00000000000e0005e385132
Network Device	FTD
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.15.15
Authorization Profile	PermitAll
Posture Status	Compliant
Response Time	2 milliseconds

Other Attributes	
ConfigVersionId	21
Event-Timestamp	1580749119
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	af49ce55-d55c-4778-ad40-b03ea12924d2
CoASourceComponent	Posture
CoAReason	posture status changed
CoAReason CoAType	posture status changed COA-push
CoAReason CoAType Network Device Profile	COA-push Cisco
CoAReason CoAType Network Device Profile Location	posture status changed COA-push Cisco Location#All Locations
CoAReason CoAType Network Device Profile Location Device Type	posture status changed COA-push Cisco Location#All Locations Device Type#All Device Types
CoAReason CoAType Network Device Profile Location Device Type IPSEC	posture status changed COA-push Cisco Location#All Locations Device Type#All Device Types IPSEC#ls IPSEC Device#No
CoAReason CoAType Network Device Profile Location Device Type IPSEC Device IP Address	posture status changed COA-push Cisco Location#All Locations Device Type#All Device Types IPSEC#ls IPSEC Device#No 192.168.15.15

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

<#root>
fyusifov-ftd-64#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username :
alice@training.example.com
Index : 14
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256 Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1 Hashing : 53990 Bytes Tx Bytes Rx : 23808 : 73 Pkts Rx : 120 Pkts Tx Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : EmployeeVPN Login Time : 16:58:26 UTC Mon Feb 3 2020 : 0h:02m:24s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 000000000000005e385132 Security Grp : none Tunnel Zone : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 14.1 Public IP : 10.55.218.19 Encryption : none Hashing : none TCP Src Port : 51965 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : win Client OS Ver: 10.0.18363 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7663 Bytes Rx : 0 Pkts Tx Pkts Rx : 5 : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 14.2 Assigned IP : 172.16.1.10 Public IP : 10.55.218.19 Encryption : AES-GCM-256 : SHA384 Hashing Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 51970 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7715 Bytes Rx : 10157 Pkts Tx : 6 Pkts Rx : 33 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PermitAll-5e384dc0 DTLS-Tunnel: Tunnel ID : 14.3 Assigned IP : 172.16.1.10 Public IP : 10.55.218.19 : SHA1 Encryption : AES256 Hashing Ciphersuite : DHE-RSA-AES256-SHA Encapsulation: DTLSv1.0 UDP Src Port : 51536 UDP Dst Port : 443 Auth Mode : userPassword

```
Idle Time Out:30 MinutesIdle TO Left : 28 MinutesClient OS: WindowsClient Type: DTLS VPN ClientClient Ver: Cisco AnyConnect VPN Agent for Windows 4.7.01076Bytes Tx: 38612Pkts Tx: 62Pkts Tx Drop :0Filter Name:
```

#ACSACL#-IP-PermitAll-5e384dc0

fyusifov-ftd-64#

Risoluzione dei problemi

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

Per un flusso di postura dettagliato e per risolvere i problemi relativi a AnyConnect e ISE, controllare questo collegamento: <u>Confronto tra gli stili di postura ISE per le versioni precedenti e successive alla 2.2.</u>

• Spilt Tunnel

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

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

Overview Analysis Policies Devices Objects AMP Ir	telligence	Deploy 🧕 System Help 🔻 admin 🔻
Device Management NAT VPN > Remote Access QoS	Platform Settings FlexConfig Certificates	
EmployeeVPN Enter Description		Save Save
		Policy Assignments (1)
Connection Profile Access Interfaces Advanced		
		0
Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftkGrpPolicy 🖉 🗑
EmployeeVPN	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: ISE (RADIUS)	DftGrpPolicy

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



• Identity NAT

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

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

Ove	Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🔩 System Help 🔻 ad											∕admin v
Dev	rice Managemer	nt NAT	VPN VQ0	5 Platform Set	tings FlexConfig	Certificates						
FT	D_11		_							🛕 Show Warnings	Save	🔀 Cancel
Ente	r Description											
	Policy Assignments (1)											
Rule	Rules											
台 Filt	er by Device										0	Add Rule
						Original Packet			Translated Packet			
#	Direction	Туре	Source Interface Ob	Destination Interface Ob	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
▼ N/	▼ NAT Rules Before											

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

Add NAT Rule						? ×		
NAT Rule:	Manual NAT Rule	•	Insert:	In Category	VAT Rules Before	•		
Type:	Static	▼ 🔽 Enable	le					
Description:								
Interface Objects	Translation PA	T Pool Advan	ced					
Available Interface C	Objects 🖒		Source Interface Object	ts (1)	Destination Interface O	bjects (1)		
Search by name			ZONE-INSIDE	ũ	ZONE-OUTSIDE	ũ		
ZONE-INSIDE								
ZONE-OUTSIDE		Add to						
		Source						
		Add to Destination						
					0	KCancel		

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

Edit NAT Rule							? ×
NAT Rule:	IAT Rule: Manual NAT Rule				In Category	NAT Rules Before	×
Type:	Static	•	🔽 Enable				
Description:							
Interface Objects	Translation	PAT Pool	Advanced				
Original Packet					Translated Packet		
Original Source:*	any			 O 	Translated Source:	Address	•
Original Destination:	Address		•	•		any	¥ ()
	VPN_Sub	net	•	• •	Translated Destination	VPN_Subnet	v O
Original Source Port:				• 💿	Translated Source Por	t:	v ()
Original Destination P	ort:		•	< 🔾	Translated Destination	Port:	v ()
						ок	Cancel

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

Edit NAT Rule									
NAT Rule:	Manual NAT F	Rule 💌	Insert:	In Category	▼ NAT Rules 8	Before 💙			
Type:	Static	•	Enable						
Description:									
Interface Objects	Translation	PAT Pool	Advanced						
Translate DNS repl	ies that match tl	his rule							
Fallthrough to Inter	face PAT(Destin	ation Interfac	ce)						
IPv6									
Net to Net Mapping									
Do not proxy ARP	on Destination I	nterface	7						
Perform Route Loo	kup for Destinat	ion Interface							
🗖 Unidirectional			- `						
					[OK Cancel			

Informazioni su questa traduzione

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