Risoluzione dei problemi comuni di comunicazione AnyConnect su FTD

Sommario

Introduzione Prerequisiti Requisiti Processo di risoluzione dei problemi consigliato I client AnyConnect non possono accedere alle risorse interne I client AnyConnect non dispongono di accesso a Internet I client AnyConnect non possono comunicare tra loro I client AnyConnect non possono stabilire chiamate telefoniche I client AnyConnect possono stabilire chiamate telefoniche, ma le chiamate non contengono audio Informazioni correlate

Introduzione

In questo documento viene descritto come risolvere alcuni dei problemi di comunicazione più comuni di Cisco AnyConnect Secure Mobility Client su Firepower Threat Defense (FTD) quando si usa Secure Socket Layer (SSL) o Internet Key Exchange versione 2 (IKEv2).

Contributo di Angel Ortiz e Fernando Jimenez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AnyConnect Secure Mobility Client.
- FTD Cisco.
- Cisco Firepower Management Center (FMC).

Componenti usati

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

- FTD gestito da FMC 6.4.0.
- AnyConnect 4.8.1

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.

Processo di risoluzione dei problemi consigliato

Questa guida spiega come risolvere alcuni problemi di comunicazione comuni dei client AnyConnect quando l'FTD viene usato come gateway VPN (Virtual Private Network) di accesso remoto. Le sezioni seguenti affrontano e forniscono soluzioni ai problemi riportati di seguito:

- I client AnyConnect non possono accedere alle risorse interne.
- I client AnyConnect non dispongono di accesso a Internet.
- I client AnyConnect non possono comunicare tra loro.
- I client AnyConnect non possono stabilire chiamate telefoniche.
- I client AnyConnect possono stabilire delle chiamate telefoniche. Nelle chiamate, tuttavia, non è presente alcun audio.

I client AnyConnect non possono accedere alle risorse interne

Attenersi alla seguente procedura:

Passaggio 1. Verificare la configurazione del tunnel suddiviso.

- Passare al profilo di connessione a cui sono connessi i client AnyConnect: Dispositivi > VPN > Accesso remoto > Profilo di connessione > Seleziona profilo.
- Passare al criterio di gruppo assegnato a tale Profile: Edit Criteri di gruppo > Generale.
- Controllare la configurazione del tunneling diviso, come mostrato nell'immagine.

Edit Group Policy

Name:*	Anyconn	ect_GroupPolicy			
Description:					
General	AnyConnec	t Advanced			
VPN Protocols IP Address Poo Banner	bls	IPv4 Split Tunneling: IPv6 Split Tunneling:	Tunnel networks specified below Tunnel networks specified below	~]
DNS/WINS		Split Tunnel Network List Type:	• Standard Access List C Extended Acce	ess List	
Split Tunneling	1	Standard Access List:	Split-tunnel-ACL	~	0
		DNS Request Split Tunneling DNS Requests: Domain List:	Send DNS requests as per split tunnel poli	icy 💙	
			Save	Ca	ncel

• Se è configurato come **rete tunnel specificata di** seguito, verificare la configurazione dell'elenco di controllo di accesso (ACL):

Selezionare Oggetti > Gestione oggetti > Elenco accessi > Modifica elenco accessi per tunneling diviso.

• Verificare che le reti che si tenta di raggiungere dal client VPN AnyConnect siano elencate nell'elenco degli accessi, come mostrato nell'immagine.

Edit Standard Access List Object

Nar	me Entries (1)	Split-tunnel-	ACL			
l,	Sequence No		Action	Network		Add
	1		Allow	InternalNetwork1 InternalNetwork2		<i>(</i>
Allo	ow Overrides					
					Save	Cancel

Passaggio 2. Verificare la configurazione dell'esenzione NAT (Network Address Translation).

Tenere presente che è necessario configurare una regola di esenzione NAT per evitare che il traffico venga convertito nell'indirizzo IP dell'interfaccia, in genere configurato per l'accesso a Internet (con Port Address Translation (PAT)).

- Passare alla configurazione NAT: Dispositivi > NAT.
- Verificare che la regola di esenzione NAT sia configurata per le reti corrette di origine (interne) e di destinazione (pool VPN di AnyConnect). Verificare inoltre che siano state selezionate le interfacce di origine e di destinazione corrette, come mostrato nell'immagine.

R	tules											
68	Filter by	Device									0	Add Rule
					Original P	acket		Translated	Packet	h		
*	Dire	ту	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	0 S	Translated Sources	Translated Destinations	т s	Options	
•	NAT Ru	es Before	1									
1	*	Sta	Linside_interface	🐥 outside_interface	InternalNetworksGroup	🛖 Anyconnect_Pool		InternalNetworksGroup	Anyconnect_Pool		🥞 Dns:false 🤹 route-lookup 🥞 no-proxy-ar	<i>i</i> 1

Nota: Quando sono configurate le regole di esenzione NAT, controllare l'opzione **no-proxyarp** ed eseguire le opzioni di **ricerca route** come procedura consigliata.

Passaggio 3. Verificare i criteri di controllo di accesso.

In base alla configurazione dei criteri di controllo dell'accesso, verificare che il traffico proveniente dai client AnyConnect possa raggiungere le reti interne selezionate, come mostrato nell'immagine.

Ru	ules Security Intelligence HTTP Response			Logging	Advanced													
商	Filter by Device					_ s	how Rule	Conflicts	0 0	Add Cat	egory	😳 Add	Rule S	Search Rul	les			×
	Name Source Dest		Dest	Source Netwo	orks De	st Networks	VL	Users	Ар	Sou	Des	URLs	ISE	Ac	v 🗅 🔉	ta 🔳 🖛	٢	
-	Mandatory - Policy1 (1-3)																	
•	External (1-2)												ø	8				
•	AnyconnectPolicy (3-3)														ø	5		
3	Anyconnect-to-internal	🚓 Outside	🚓 Inside	anyconne	ct_Pool	InternalNetworksGroup	Any	Any	Any	Any	Any	Any	Any	🖌 🗸	0 0 2	會日0	0	6

I client AnyConnect non dispongono di accesso a Internet

Esistono due possibili scenari per questo problema.

1. Il traffico destinato a Internet non deve passare attraverso il tunnel VPN.

Verificare che Criteri di gruppo sia configurato per il tunneling suddiviso come **reti tunnel specificate di seguito** e NON come **Consenti tutto il traffico sul tunnel**, come mostrato nell'immagine.

Edit Group Policy	у					?	×
Name:* A Description:	Anyconnec	ct_GroupPolicy					
General AnyC	Connect	Advanced					
VPN Protocols		IPv4 Split Tunneling:	Tunnel networks specifie	ed below	*]	
IP Address Pools Banner		IPv6 Split Tunneling:	Tunnel networks specifie	ed below	~		
DNS/WINS		Split Tunnel Network List Type:	 Standard Access List 	O Extended Acce	ess List		
Split Tunneling		Standard Access List:	Split-tunnel-ACL		~	\bigcirc	
		DNS Request Split Tunneling					
		DNS Requests:	Send DNS requests as p	er split tunnel poli	icy 💙		
		Domain List:					
				Save	Ca	ncel	

2. Il traffico destinato a Internet deve passare attraverso il tunnel VPN.

In questo caso, la configurazione di Criteri di gruppo più comune per il tunneling ripartito consiste nel selezionare **Consenti tutto il traffico sul tunnel**, come mostrato nell'immagine.

Edit Group Policy

Name:*	Anyconn	ect_GroupPolicy_TunnelAll		
Description:				
General	AnyConnec	t Advanced		
VPN Protocols		IPv4 Split Tunneling:	Allow all traffic over tunnel	~
IP Address Poo Banner	ols	IPv6 Split Tunneling:	Allow all traffic over tunnel	~
DNS/WINS		Split Tunnel Network List Type:	Standard Access List Extended Access	List
Split Tunneling)	Standard Access List:	Split-tunnel-ACL	¥ 🔘
		DNS Request Split Tunneling		
		DNS Requests:	Send DNS requests as per split tunnel policy	~
		Domain List:		
			Save	Cancel

Passaggio 1. Verificare la configurazione di esenzione NAT per la raggiungibilità della rete interna.

Ricorda che dobbiamo ancora configurare una regola di esenzione NAT per avere accesso alla rete interna. Esaminare il **Passaggio 2** della **I client AnyConnect non possono accedere alle risorse interne** sezione.

Passaggio 2. Verificare la configurazione dell'hairpinning per le traduzioni dinamiche.

Affinché i client AnyConnect possano accedere a Internet tramite il tunnel VPN, dobbiamo verificare che la configurazione NAT del hairpinning sia corretta per il traffico da convertire nell'indirizzo IP dell'interfaccia.

- Passare alla configurazione NAT: Dispositivi > NAT.
- Verificare che la regola NAT dinamico sia configurata per l'interfaccia corretta (collegamento ISP (Internet Service Provider)) come origine e destinazione (hairpinning). Verificare inoltre che la rete utilizzata per il pool di indirizzi VPN AnyConnect sia selezionata in Originale e nell'IP dell'interfaccia di destinazione è selezionata per Origine tradotta, come mostrato nell'immagine.

Rules													
đð	Filter by Dev	vice									0	Add Rule	
						Original Packet			ranslated Packet				
#	Dire	Туре	Source Interface	Destination Interface	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options		
۲	NAT Rules	Before											
۳	Auto NAT	Rules											
#	Dynamic 4 outside_int 4 outside_in				: 🚔 Anyconnect_Pool			🍓 Interface			🍓 Dns:fai	/0	

Passaggio 3. Verificare i criteri di controllo di accesso.

In base alla configurazione dei criteri di controllo dell'accesso, verificare che il traffico proveniente dai client AnyConnect possa raggiungere le risorse esterne, come mostrato nell'immagine.

Ru	les Security Intellige	nce HTTP	Responses	Logging	Advanced													
68	Filter by Device						Show Rule	Conflicts	0 0	Add Cat	egory	🔾 Add	Rule S	Search Rule	is			×
	Name	Source	Dest	Source Netv	works De	est Networks	VL	Users	Ар	Sou	Des	URLs	ISE	Ac	, .	A 🕁 🔳 =	٥	
-	Mandatory - Policy1 (1-	5)																
•	External (1-2)																0	8
•	AnyconnectPolicy (3-5)												0	Ð				
3	Anyconnect-to-internet	🚓 Outside	🚓 Outside	e 📻 Anyconn	ect_Pool	4.ny	Any	Any	Any	Any	Any	Any	Any	🛹 Allo	00	·2 🖄 🗌 o	ø	6
4	Internet-to-Anyconnect	🚠 Outside	🚠 Outside	e Any	6	Anyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	🖌 Allo	00	2000	0	

I client AnyConnect non possono comunicare tra loro

Esistono due possibili scenari per questo problema:

- 1. Client AnyConnect con Consenti tutto il traffico sul tunnel configurazione sul posto.
- 2. Client AnyConnect con Reti tunnel specificate di seguito configurazione sul posto.

1. Client AnyConnect con **Consenti tutto il traffico sul tunnel** configurazione sul posto. Quando **Consenti tutto il traffico sul tunnel** è configurato per AnyConnect significa che tutto il traffico, interno ed esterno, deve essere inoltrato all'headend AnyConnect. Questa situazione si verifica quando si dispone di NAT per l'accesso a Internet pubblico, in quanto il traffico proveniente da un client AnyConnect destinato a un altro client AnyConnect viene convertito

Passaggio 1. Verificare la configurazione di esenzione NAT.

all'indirizzo IP dell'interfaccia e pertanto la comunicazione non riesce.

Per risolvere questo problema, è necessario configurare una regola di esenzione NAT manuale per consentire la comunicazione bidirezionale all'interno dei client AnyConnect.

- Passare alla configurazione NAT: **Dispositivi > NAT**.
- Verificare che la regola di esenzione NAT sia configurata per l'origine (pool VPN AnyConnect) e la destinazione corretti. (AnyConnect VPN Pool). Verificare inoltre che sia presente la configurazione corretta del hairpin, come mostrato nell'immagine.

- N	lics											
齝	Filter by Dev	rice									0	Add Rule
						Original Packet			ranslated Packet			
#	Dire	Туре	Source Interface	Destination Interface	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
•	NAT Rules	Before										
1	\$	Static	🚆 outside_int	autside_int	Rnyconnect_Pool	🚔 Anyconnect_Pool		🚔 Anyconnect_Pool	🚍 Anyconnect_Pool		Ons:fal: Conte-la Con	<i>P</i> 1

Passaggio 2. Verificare i criteri di controllo di accesso.

In base alla configurazione dei criteri di controllo dell'accesso, verificare che il traffico proveniente dai client AnyConnect sia consentito, come mostrato nell'immagine.

Ru	es Security In	ntelligence	HTTP F	Responses	Logging	Advand	ed											
68	Filter by Device							Show Rule	Conflicts	0	Add Cat	egory	🔾 Add	Rule	Search Ru	ules		Х
	Name Source Dest		Dest	Source Netv	vorks	Dest Networks	VL	Users	Ар	Sou	Des	URLs	ISE	Ac	U 🗞 🕫 🔳 🤉		9	
-	Mandatory - Policy1 (1-6)																	
•	ixternal (1-2)																0	8
•	AnyconnectPolicy	(3-6)															0	8
3	Anyconnect-intra	4	Outside	👍 Outside	R Anyconn	ect_Pool	Anyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	1	NOT D. 2 to I	6	0

2. I client Anyconnect con Reti tunnel specificate di seguito configurazione sul posto.

Con **Reti tunnel specificate di seguito** configurati per i client AnyConnect, solo il traffico specifico viene inoltrato a tramite il tunnel VPN. Tuttavia, dobbiamo verificare che l'headend abbia la configurazione corretta per consentire la comunicazione tra i client AnyConnect.

Passaggio 1. Verificare la configurazione di esenzione NAT.

Controllare il Passaggio 1, nella sezione Consenti tutto il traffico sul tunnel.

Passaggio 2. Verificare la configurazione del tunneling ripartito.

Per consentire ai client AnyConnect di comunicare tra loro, è necessario aggiungere gli indirizzi del pool VPN nell'ACL dello split-tunnel.

- Seguire il **punto 1** della **I client AnyConnect non possono accedere alle risorse interne** sezione.
- Verificare che la rete del pool VPN AnyConnect sia elencata nell'elenco degli accessi al tunneling suddiviso, come mostrato nell'immagine.

Edit Stan	dard Acces			? ×	
Name	Split-t	unnel-ACL			Add
Sequen	nce No	Action	Network		
1		🖋 Allow	InternalNetwork3		J 🗍
2		🖌 Allow	Anyconnect_Pool	←	6
Allow Over	rides 🗌				
				Save	Cancel

Nota: Se sono presenti più pool IP per i client AnyConnect e la comunicazione tra i diversi pool è necessaria, aggiungere tutti i pool nell'ACL di tunneling suddiviso, quindi aggiungere anche una regola di esenzione NAT per i pool IP necessari.

Passaggio 3. Verificare i criteri di controllo di accesso.

Verificare che il traffico proveniente dai client AnyConnect sia consentito, come mostrato nell'immagine.

Ru	les Secu	ity Intelligen	ules Security Intelligence HTTP Response		Logging	Advance	d													
â	Filter by Dev	ce					C	Show Rule	Conflicts	0	🕽 Add Ca	tegory	🔾 Add	I Rule	Search Ru	ules				×
	Name	lame Source Dest		Dest	Source Netv	vorks E	Dest Networks	VL	Users	Ар	Sou	Des	URLs	ISE	Ac	•	<u>,</u> a 🗞 🛛		٢	
-	Mandatory ·	Policy1 (1-6)																	
•	External (1	2)																	Ø	3
 AnyconnectPolicy (3-6) 																			Ø	a
3	Anyconnect	intra	🚓 Outside	🔒 Outsid	e 🚍 Anyconn	ect_Pool	Rhyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	1	Allo 🗍 🗓	2 m [0	ø	6

I client AnyConnect non possono stabilire chiamate telefoniche

In alcuni scenari, i client AnyConnect devono stabilire chiamate telefoniche e videoconferenze tramite VPN.

I client AnyConnect possono connettersi all'headend AnyConnect senza alcun problema. Possono raggiungere risorse interne ed esterne, ma non è possibile effettuare chiamate telefoniche.

In questi casi dobbiamo considerare i seguenti punti:

- Topologia di rete per la voce.
- Protocolli interessati. ad esempio il Session Initiation Protocol (SIP), il Rapid Spanning Tree Protocol (RSTP), ecc.
- Modalità di connessione dei telefoni VPN a Cisco Unified Communications Manager (CUCM).

Per impostazione predefinita, l'ispezione delle applicazioni viene abilitata per impostazione predefinita nell'FTD e nell'ASA nella mappa dei criteri globale.

Nella maggior parte dei casi, i telefoni VPN non sono in grado di stabilire una comunicazione affidabile con CUCM perché l'headend AnyConnect ha un'ispezione dell'applicazione abilitata che modifica il segnale e il traffico vocale.

Per ulteriori informazioni sull'applicazione voce e video in cui è possibile eseguire il controllo delle applicazioni, vedere il documento seguente:

Capitolo: Ispezione per protocolli voce e video

Per verificare se il traffico di un'applicazione viene interrotto o modificato dalla mappa dei criteri globale, è possibile utilizzare il comando **show service-policy**, come mostrato di seguito.

firepower#show service-policy

Global policy: Service-policy: global_policy Class-map: inspection_default Inspect: sip , packet 792114, lock fail 0, drop 10670, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0

In questo caso possiamo vedere come l'ispezione SIP scarta il traffico.

Inoltre, l'ispezione SIP può anche tradurre gli indirizzi IP all'interno del payload, non nell'intestazione IP, e causare diversi problemi, quindi si consiglia di disabilitarla quando si desidera utilizzare i servizi voce su AnyConnect VPN.

Per disabilitarlo, è necessario completare la procedura seguente:

Passaggio 1. Accedere alla modalità di esecuzione privilegiata.

Per ulteriori informazioni su come accedere a questa modalità, consultare il documento successivo:

Capitolo: Uso dell'interfaccia della riga di comando (CLI)

Passaggio 2. Verificare la mappa dei criteri globale.

Eseguire il comando successivo e verificare se l'ispezione SIP è abilitata.

firepower#show running-config policy-map

policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp

inspect sip

inspect netbios inspect tftp inspect ip-options inspect icmp inspect icmp error inspect esmtp

Passaggio 3. Disabilitare l'ispezione SIP.

Se l'ispezione SIP è abilitata, disattivarla eseguendo il comando seguente dal prompt dei comandi:

> configure inspection sip disablePassaggio 4. Verificare nuovamente la mappa dei criteri globali.

Verificare che l'ispezione SIP sia disabilitata dalla mappa dei criteri globale:

firepower#show running-config policy-map

.

.

policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp

inspect netbios

inspect tftp

inspect ip-options

inspect icmp

inspect icmp error

inspect esmtp

I client AnyConnect possono stabilire chiamate telefoniche, ma le chiamate non contengono audio

Come accennato nella sezione precedente, una necessità molto comune per i client AnyConnect è stabilire le chiamate telefoniche quando sono connessi alla VPN. In alcuni casi è possibile stabilire la chiamata, ma i client potrebbero non avere audio. Ciò si applica agli scenari successivi:

• Nessun segnale audio nella chiamata tra un client AnyConnect e un numero esterno.

• Nessun segnale audio nella chiamata tra un client AnyConnect e un altro client AnyConnect. Per risolvere questo problema, è possibile eseguire la procedura seguente:

Passaggio 1. Verificare la configurazione del tunneling ripartito.

- Passare al profilo di connessione utilizzato per la connessione a: Dispositivi > VPN > Accesso remoto > Profilo di connessione > Seleziona profilo.
- Passare al criterio di gruppo assegnato a tale Profile: Edit Criteri di gruppo > Generale.
- Controllare la configurazione del tunneling diviso, come mostrato nell'immagine.

Edit Group Policy

Name:*	Anyconn	ect_GroupPolicy				
Description:						
General	AnyConnec	t Advanced				
VPN Protocols IP Address Poo	ls	IPv4 Split Tunneling:	Tunnel networks specifie	d below	*	
Banner DNS/WINS		Split Tunnel Network List Type:	Standard Access List		ess List	
Split Tunneling		Standard Access List:	Split-tunnel-ACL		~	0
		DNS Request Split Tunneling				
		DNS Requests:	Send DNS requests as pe	r split tunnel polic	cy 💙	
		Domain List:				
			(Save	Car	ncel

- Se configurato come Reti tunnel specificate di seguitoverificare la configurazione dell'elenco degli accessi: Oggetti > Gestione oggetti > Elenco accessi > Modifica elenco accessi per tunneling diviso.
- Verificare che i server voce e le reti del pool IP AnyConnect siano elencati nell'elenco degli accessi al tunneling suddiviso, come mostrato nell'immagine.

me Sp	olit-tunnel-ACL		
Entries (2)			Add
Sequence No	Action	Network	
1	🛹 Allow	InternalNetwork3	J 🗇
2	🛹 Allow	Anyconnect_Pool	Ø 🛙
ow Overrides			
		Sav	e Cance

Edit Standard Access List Object

Passaggio 2. Verificare la configurazione di esenzione NAT.

Le regole di esenzione NAT devono essere configurate per esentare il traffico dalla rete VPN di AnyConnect alla rete dei server voce e anche per consentire la comunicazione bidirezionale all'interno dei client AnyConnect.

- Passare alla configurazione NAT: Dispositivi > NAT.
- verificare che la regola di esenzione NAT sia configurata per le reti di origine (server voce) e di destinazione (pool VPN AnyConnect) corrette e che la regola NAT hairpin per consentire la comunicazione tra il client AnyConnect e il client AnyConnect sia configurata. Verificare inoltre che per ogni regola sia disponibile la configurazione corretta delle interfacce in entrata e in uscita, in base alla progettazione di rete, come mostrato nell'immagine.

商 Filter by Device														
					Origina	al Packet	Translate							
#	Dir	т	Source Interface Ob	Destination Interface Obje	Original Sources	Original Destinations	0 s	Translated Sources	Translated Destinations	т s	Options			
▼ NAT Rules Before														
1	4	S	🐣 Inside_interfac	e outside_interface	a InternalNetworksGroup	Anyconnect_Pool		a InternalNetworksGroup	Anyconnect_Pool		Ons:false or route-loo or no-proxy	6		
2	4	S	🐥 Inside_interfac	autside_interface	VoiceServers	Rhyconnect_Pool		VoiceServers	Anyconnect_Pool		🝓 Dns:false 🍓 route-loo 🍓 no-proxy-	6		
3	4	S	🝰 outside_interfa	🚑 outside_interface	Anyconnect_Pool	Anyconnect_Pool		Anyconnect_Pool	Anyconnect_Pool		Ons:false oute-loo oproxy.	J		

Passaggio 3. Verificare che l'ispezione SIP sia disabilitata.

Bulas

Rivedere la sezione precedente I client AnyConnect non possono stabilire chiamate telefoniche per sapere come disabilitare l'ispezione SIP.

Passaggio 4. Verificare i criteri di controllo di accesso.

In base alla configurazione dei criteri di controllo dell'accesso, verificare che il traffico proveniente dai client AnyConnect possa raggiungere i server voce e le reti coinvolte, come mostrato nell'immagine.

Ru	les Security Intelliger	nce HTTP	Responses	Logging	Advanced													
68	Filter by Device						Show Rule	Conflicts	9 6	Add Cat	egory	😳 Add	Rule	Search Rules	1			×
	Name	Source	Dest	Source Netv	works De	st Networks	VL	Users	Ар	Sou	Des	URLS	ISE	Ac	/ 🗅 🔏 😓		۵	
-	▼ Mandatory - Policy1 (1-7)																	
•	• External (1-2)									0	6							
•	AnyconnectPolicy (3-7)																ø	8
3	Anyconnect-intra	🚠 Outside	🚠 Outside	Anyconn	ect_Pool	Anyconnect_Pool	Any	Any	Any	Any	Any	Any	Any	🖋 Allo	0.81	0 🗍	ø	8
4	Anyconnect-to-voice-serv	a 🚠 Outside	🔥 Inside	Anyconn	ect Pool	VoiceServers	Any	Any	Any	Any	Any	Any	Any	🖌 Allo	OD.A.	D D	0	8

Informazioni correlate

- In questo video viene illustrato l'esempio di configurazione per i diversi problemi discussi in questo documento.
- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido: <u>Contatti del supporto Cisco internazionali.</u>
- Puoi anche visitare la Cisco VPN Community qui.