Implementazione delle misure di protezione avanzata per la VPN AnyConnect Secure Client

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Principi base
Procedure di protezione avanzata dei client su Cisco Secure Firewall:
Identificazione degli attacchi tramite ID di log e syslog
Verifica degli attacchi
Esempi di configurazione di FMC
<u>Disabilitare l'autenticazione AAA nei profili di connessione DefaultWEBVPNGroup e</u> <u>DefaultRAGroup</u>
<u>Disabilitare Hostscan / Secure Firewall Posture su DefaultWEBVPNGroup e DefaultRAGroup</u> (facoltativo)
<u>Disabilitare gli alias di gruppo e abilitare gli URL di gruppo</u>
Mapping certificati
IPsec-IKEv2
Esempi di configurazione di ASA
<u>Disabilitare l'autenticazione AAA nei profili di connessione DefaultWEBVPNGroup e</u> <u>DefaultRAGroup</u>
<u>Disabilitare Hostscan / Secure Firewall Posture su DefaultWEBVPNGroup e DefaultRAGroup</u> (facoltativo)
<u>Disabilitare gli alias di gruppo e abilitare gli URL di gruppo</u>
Mapping certificati
IPsec-IKEv2
Conclusioni
Informazioni correlate

Introduzione

Questo documento descrive come migliorare la sicurezza dell'implementazione della VPN ad accesso remoto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Client AnyConnect VPN.
- Configurazione dell'accesso remoto ASA/FTD.

Componenti usati

La guida alle best practice si basa sulle seguenti versioni hardware e software:

- Cisco ASA 9.x
- Firepower Threat Defense 7.x / FMC 7.x

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.



Attenzione: questo documento non contiene i passaggi per Firepower Device Manager (FDM). FDM supporta solo la modifica del metodo di autenticazione in DefaultWEBVPNGroup. Utilizzare gli ACL del control plane o una porta personalizzata

nella sezione 'Impostazioni globali' della VPN di accesso remoto all'interno dell'interfaccia utente di FDM. Contattare il Cisco Technical Assistance Center (TAC) per ulteriore assistenza, se necessario.

Premesse

Lo scopo di questo documento è garantire che la configurazione VPN AnyConnect di Cisco Secure Client sia conforme alle best practice per la sicurezza in un mondo moderno in cui gli attacchi informatici sono comuni.

Gli attacchi di forza bruta solitamente implicano ripetuti tentativi di accedere a una risorsa utilizzando combinazioni di nome utente e password. Gli aggressori tentano di utilizzare il browser Internet, l'interfaccia utente Secure Client o altri strumenti per immettere più nomi utente e password sperando di trovare una combinazione corretta in un database AAA. Quando si utilizza il server AAA per l'autenticazione, ci si aspetta che l'utente finale immetta il proprio nome utente e la propria password, in quanto ciò è necessario per stabilire la connessione. Allo stesso tempo, la verifica dell'identità dell'utente viene eseguita solo dopo l'immissione delle credenziali. Per natura, questo permette agli aggressori di trarre vantaggio da questi scenari:

- 1. Nomi di dominio completi esposti per Cisco Secure Firewall (in particolare quando si utilizzano alias di gruppo nel profilo di connessione):
 - Se l'utente malintenzionato rileva il nome di dominio completo (FQDN) del firewall VPN, può scegliere di selezionare il gruppo di tunnel utilizzando l'alias di gruppo in cui desidera avviare l'attacco di forza bruta.
- 2. Profilo di connessione predefinito configurato con AAA o database locale:
 - Se l'autore dell'attacco trova il nome di dominio completo (FQDN) del firewall VPN, può tentare di forzare l'attacco al server AAA o al database locale. Questo si verifica perché la connessione all'FQDN viene stabilita nel profilo di connessione predefinito, anche se non sono specificati alias di gruppo.
- 3. Esaurimento risorse sul firewall o sui server AAA:
 - Gli aggressori possono sovraccaricare i server AAA o le risorse del firewall inviando grandi quantità di richieste di autenticazione e creando una condizione DoS (Denial of Service).

Principi base

Alias di gruppo:

 Nome alternativo con cui il firewall può fare riferimento a un profilo di connessione. Dopo l'avvio di una connessione al firewall, questi nomi vengono visualizzati in un menu a discesa nell'interfaccia utente di Secure Client da selezionare. La rimozione degli alias di gruppo rimuove la funzionalità dell'elenco a discesa nell'interfaccia utente di Secure Client. URL del gruppo:

 URL che può essere associato a un profilo di connessione in modo che le connessioni in ingresso vengano mappate direttamente a un profilo di connessione desiderato. Non è disponibile alcuna funzionalità di elenco a discesa, in quanto gli utenti possono immettere l'URL completo nell'interfaccia utente di Secure Client, oppure l'URL può essere integrato con un 'Nome visualizzato' nel profilo XML per nascondere l'URL all'utente.

In questo caso, la differenza consiste nel fatto che quando vengono implementati gli alias di gruppo, un utente avvia una connessione to vpn_gateway.example.com e viene presentato con gli alias per selezionare l'unità che li indirizza a un profilo di connessione. Con gli URL di gruppo, un utente avvia una connessione a vpn_gateway.example.com/example_group e li indirizza direttamente al profilo di connessione senza la necessità o l'opzione di un menu a discesa.

Procedure di protezione avanzata dei client su Cisco Secure Firewall:

Questi metodi si basano sul mapping di utenti legittimi a gruppi di tunnel/profili di connessione appropriati, mentre utenti potenzialmente dannosi vengono inviati a un gruppo di tunnel trap configurato per non consentire combinazioni di nome utente e password. Sebbene non tutte le combinazioni debbano essere implementate, per il corretto funzionamento dei suggerimenti è necessario disattivare gli alias di gruppo e modificare il metodo di autenticazione di DefaultWEBVPNGroup e DefaultRAGroup.

- Disabilitare gli alias dei gruppi e utilizzare solo l'URL del gruppo nella configurazione del profilo di connessione. In questo modo è possibile disporre di un FQDN specifico che non sarà facile da individuare e selezionare da parte di un utente non autorizzato, in quanto solo i client con il FQDN appropriato possono avviare la connessione. Ad esempio, per un utente non autorizzato è più difficile individuare vpn_gateway.example.com/example_group che vpn_gateway.example.com.
- Disabilitare l'autenticazione AAA in DefaultWEBVPNGroup e DefaultRAGroup e configurare l'autenticazione dei certificati, in modo da evitare una possibile forzatura brute sul database locale o sul server AAA. L'autore dell'attacco in questo scenario riceverebbe errori immediati durante il tentativo di connessione. Non è presente alcun campo relativo al nome utente o alla password poiché l'autenticazione è basata sui certificati, impedendo così i tentativi di forzatura bruta. In alternativa è possibile creare un server AAA senza configurazione di supporto per creare un sinkhole per le richieste dannose.
- Utilizzare il mapping dei certificati per il profilo di connessione. In questo modo è possibile mappare le connessioni in ingresso a profili di connessione specifici in base agli attributi ricevuti dai certificati nel dispositivo client. Gli utenti che dispongono dei certificati appropriati vengono mappati correttamente, mentre gli autori di attacchi che non soddisfano i criteri di mappatura vengono inviati a DefaultWEBVPNGroup.

 L'utilizzo di IKEv2-IPSec anziché di SSL fa in modo che i gruppi di tunnel si basino su un mapping utente-gruppo specifico nel profilo XML. Senza questo codice XML sul computer dell'utente finale, gli utenti vengono automaticamente inviati al gruppo di tunnel predefinito.



Nota: per ulteriori informazioni sulla funzionalità group-alias, vedere <u>ASA VPN</u> <u>Configuration Guide</u> e osservare la tabella 1. Attributi del profilo di connessione per SSL VPN'.

Identificazione degli attacchi tramite ID di log e syslog

Gli attacchi di tipo "brute-force" rappresentano il metodo predominante per compromettere le VPN ad accesso remoto, sfruttando password deboli per ottenere l'accesso non autorizzato. È fondamentale sapere come riconoscere i segni di un attacco sfruttando l'uso di log e di valutazione dei syslog. Di seguito sono riportati gli ID di syslog comuni che possono indicare un attacco in caso di rilevamento di un volume anomalo:

%ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

%ASA-6-113005

<#root>

%ASA-6-113005

```
: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =
```

%ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.> Authentication: rejected, Session Type: WebVPN

Il nome utente è sempre nascosto finché il comando no logging hide username non viene configurato sull'appliance ASA.



Nota: questo fornisce informazioni dettagliate se gli utenti validi sono generati o conosciuti da IP offensivi. Tuttavia, prestare attenzione in quanto i nomi utente sono visibili nei log.

Registrazione Cisco ASA:

Guida per l'utente per proteggere il firewall ASA

Capitolo Logging della guida alla configurazione della CLI per le operazioni generali di Cisco Secure Firewall serie ASA

Registrazione FTD Cisco:

Configurazione dei log sull'FTD tramite FMC

Sezione <u>Configure Syslog</u> nel capitolo Platform Settings della Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center <u>Configurazione e verifica di Syslog in Gestione periferiche di Firepower</u> Sezione <u>Configurazione delle impostazioni di registrazione del sistema</u> nel capitolo System Settings della Guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager

Verifica degli attacchi

Per verificare, accedere all'interfaccia della riga di comando (CLI) ASA o FTD, eseguire il comando show aaa-server e verificare la presenza di un numero insolito di richieste di autenticazione tentate e rifiutate su uno dei server AAA configurati:

<#root>

ciscoasa#

show aaa-server

Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time Oms
Number of authentication requests 8473575 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - >>>> Unusual increments

<#root>

ciscoasa#

show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server Server Protocol: ldap Server Hostname: ldap-server.example.com Server Address: 10.10.10.10 Server port: 636 Server status: ACTIVE, Last transaction at unknown Number of pending requests 0 Average round trip time Oms Number of authentication requests 2228536 - - - - - >>> Unusual increments Number of authorization requests 0 Number of accounting requests 0 Number of retransmissions 0 Number of accepts 1312 Number of rejects 2225363 - - - - - >>>> Unusual increments Number of challenges 0 Number of malformed responses 0

Esempi di configurazione di FMC

Disabilitare l'autenticazione AAA nei profili di connessione DefaultWEBVPNGroup e DefaultRAGroup

Selezionare Dispositivi > Accesso remoto.

	Firewa Overview	II Manage / Dashboards	ement Center	Overview	Analysis	Policies	Devices	Objects	Integration	
Sum Provides a Netwo	IMARY a summary c rork	Dashboa of activity on the a Threats	ard (<u>switch dashboard)</u> appliance Intrusion Events	Status	Geolocation	QoS	Device I NAT QoS Platform FlexCon Certifica	Management Settings fig tes	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture
► Top	p Zero Tru	ist Application	ns			- ×				Upgrade Threat Defense Upgrade Chassis Upgrade

Visualizza l'esplorazione dell'interfaccia utente di FMC per accedere alla configurazione dei criteri VPN di Accesso remoto.

Modificare il criterio VPN di Accesso remoto esistente e creare un profilo di connessione denominato 'DefaultRAGroup'

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	0 ¢ (admin ~	teneo SECURE
											Add
Name				Status			Last Modified				
RAVPN				Targeting 1 C	devices on all targeted		2024-03-07 10:58:20 Modified by "admin"			9 / i	

Visualizza come modificare i criteri VPN di Accesso remoto nell'interfaccia utente di FMC.

Modificare i profili di connessione denominati DefaultWEBVPNGroup e DefaultRAGroup



Visualizza come modificare DefaultWEBVPNGroup nell'interfaccia utente di FMC.

Passare alla scheda AAA e selezionare l'elenco a discesa Authentication Method (Metodo di autenticazione). Selezionare "Solo certificato client" e selezionare Salva.

Edit Connection Profile		
Connection Profile:*	DefaultWEBVPNGroup	
Group Policy:*	DfltGrpPolicy +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method:	Client Certificate Only -	
•	Enable multiple certificate authentication	
Map username from clier	nt certificate	
Authorization		
Authorization Server:	▼	
	Allow connection only if user exists in authorization database	
Accounting		
Accounting Server:		
	Cancel	е

Modifica del metodo di autenticazione in certificato client solo per DefaultWEBVPNGroup nell'interfaccia utente di FMC.

Modificare il gruppo DefaultRAGroup, selezionare la scheda AAA e selezionare l'elenco a discesa Authentication Method (Metodo di autenticazione). Selezionare 'Solo certificato client' e selezionare Salva.

Edit Connection Profile		
Connection Profile:*	DefaultRAGroup	
Group Policy:*	DfltGrpPolicy - +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method:	Client Certificate Only	
'	Enable multiple certificate authentication	
► Map username from clie	nt certificate	
Authorization		
Authorization Server:	▼	
	Allow connection only if user exists in authorization database	
Accounting		
Accounting Server:	▼	
	Cancel	ave

Modifica del metodo di autenticazione in certificato client solo per DefaultRAGroup nell'interfaccia utente di FMC.



Nota: il metodo di autenticazione può essere anche un server AAA sinkhole. Se si utilizza questo metodo, la configurazione del server AAA è falsa e non elabora effettivamente alcuna richiesta. Per salvare le modifiche, è inoltre necessario definire un pool VPN nella scheda 'Assegnazione indirizzo client'.

Disabilitare Hostscan / Secure Firewall Posture su DefaultWEBVPNGroup e DefaultRAGroup (facoltativo)

Questa operazione è necessaria solo se si dispone di Hostscan/Secure Firewall Posture nell'ambiente. Questo passaggio impedisce agli autori di attacchi di aumentare l'utilizzo delle risorse nel firewall causato dal processo di scansione dell'endpoint. Nel FMC, questo si ottiene creando un oggetto FlexConfig con il comando without-csd per disabilitare la funzionalità di scansione dell'endpoint.

Selezionare Oggetti > Gestione oggetti > Oggetto FlexConfig > Aggiungi oggetto FlexConfig.

Firewall Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 🕢 admin 🗸	cisco SECURE
> AAA Server > Access List > Address Pools Application Filters	FlexConfig Object FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.	Add FlexConfig Object Q, Filter	
AS Path	Name	Description	
BFD Template Cinher Suite List	Anyconnect_route_thering		6/7 [*]
> Community List	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNS	¶a Q ≣
DHCP IPv6 Pool	Default_Inspection_Protocol_Disable	Disable Default Inspection.	¶a Q ⊕
Distinguished Name DNS Server Group	Default_Inspection_Protocol_Enable	Enable Default Inspection.	Faq =
> External Attributes	DHCPv6_Prefx_Delegation_Configure	Configure one outside (PD client) and one inside interface (recip	¶aq ≣
File List	DHCPv6_Prefx_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside i	¶aq. ⊒
FlexConfig FlexConfig Object	DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and	¶a ⊜
Text Object	DNS_UnConfigure	Remove the DNS configurations.	¶aq ⊒
Geolocation	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-su	¶a q ≣
Key Chain	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authent	¶a q ⊒
Network	Eigrp_UnContgure	Clears eigrp configuration for an AS	Eg Q ≣

Spostamento nell'interfaccia utente di FMC per creare un oggetto FlexConfig.

Assegnare un nome all'oggetto FlexConfig, impostare la distribuzione su Everytime con il tipo Append. Immettere quindi la sintassi esattamente come indicato e salvare l'oggetto.

Edit FlexConfig Object							9
Name: Wtihout-CSD Description: Copy-pasting any rich text might in	troduce line breaks	s while generating C	LI Please	ع verify the	CLI before deploy	ment	
Insert - B Deployment	Everytime	gg _	•	Туре:	Append	•)
tunnel-group DefaultWEBVPNGroup w without-csd	ebvpn-attribute	3					
tunnel-group DefaultRAGroup webvr	on-attributes						
▼ Variables							
Name	Dimension	Default Value	Prop (Typ	erty e:Name)	Override	Description	
		No records to	display				
						Cancel	Save

Creazione di un oggetto FlexConfig con 'without-csd'

Passare a Dispositivi > FlexConfig e fare clic sulla matita per modificare il criterio FlexConfig.

Deploy Q 💕 🎝 🕢 admin 🗸 🔩 Secure		Objects Integration	Devices	Policies	Analysis	Overview	Firewall Management Center Devices / FlexConfig	Ð
New Policy								
	Last Modified	Status					FlexConfig Policy	F
21:54:19 domin"	2024-04-10 21:54:19 Modified by "admin"	Targeting 1 devices Out-of-date on 1 targeted device					Flex-Test	
15419 dmm"	2024-04-10 21 54 19 Modified by "admin"	Targeting 1 devices Cut-of-cute on 1 targeted devic					Flox-Tost	

Modifica del criterio FlexConfig in FMC.

Individuare l'oggetto creato dalla sezione Definito dall'utente. Quindi, selezionare la freccia per aggiungerla al componente FlexConfigs di aggiunta selezionato. Infine, selezionare Salva per salvare il criterio FlexConfig.

Firewall Management Center Devices / Flexconfig Policy Editor	Overvie	w Analysis	Policies	Devices	Objects	Integration	Depkoy Q 🥐 🏠 🛛 admin 🗸 👘 SECURE
FlexConfig Enter Description							You have unaswed changes It tyrate Control Preview Control Swe Cancel
citer oracipion							Policy Assignments (1)
	"i Sel	ected Prepend F	lexConfigs				
Available FlexConfig C FlexConfig Object		Name			Description		
V User Defined	- I						
"] Anyconnect_route_filtering							
1 No_Keepout 11 Without-CSD							
V System Defined							
"? Default_DNS_Configure							
Default_Inspection_Protocol_Disable							
Default_Inspection_Protocol_Enable	.) Se	ected Append F	lexConfigs				
"2 DHCPv6_Prefix_Delegation_Configure		Name			Description		
DHCPV6_Prenx_Delegation_UnConfigure DNS_Configure	1	Wtihout-CSD					<i>م</i>
DNS_UnConfigure							
"B Eigrp_Configure							
"2 Eigrp_Interface_Configure							

Collegare l'oggetto FlexConfig ai criteri FlexConfig.

Selezionare Assegnazioni criteri e scegliere l'FTD a cui si desidera applicare il criterio FlexConfig, quindi selezionare OK. Selezionare nuovamente Save se si tratta di una nuova assegnazione FlexConfig e distribuire le modifiche. Dopo la distribuzione, verificare

Firewall Management Center Devices / Flexcorify Policy Editor	Overview Anal	ysis Policies	Devices 0	Objects Inte	egration			Deploy Q 🧬 🛱 😡	admin ~ duto SECURE
FlexConfig Enter Description									Cencel
Available FlexConfig C FlexConfig Object	Selected Prep	end FlexConfigs	Desc	cription					Policy Assignments (1)
✓ User Defined 2 ¹ Anyconnect_route_filtering ² Keepout ² Without-CBD ✓ System Defined ² Default_DNS_Configure .1 Default_Inspection_Protocol_Disable		Targeted Devices Targeted Devices Select devices to t Available Devices Q. Search by nam FTD1	swhich you want to	o apply this policy	y. Selected Devices FTD1	Ŧ			
Default_Inspection_Protocol_Enable DHCPv6_Probs_Delegation_Configure DHCPv6_Probs_Delegation_UncConfigure DNS_Configure DNS_Configure DNS_Configure Egyp_Configure Egyp_Linterface_Configure Egyp_Linterface_Configure	Selected App Name						Cancel		Q. 🗑

Assegnare il criterio FlexConfig a un dispositivo FirePOWER.

Immettere la CLI FTD e usare il comando show run tunnel-group per DefaultWEBVPNGroup e DefaultRAGroup. Verificare che without-csd sia presente nella configurazione.

<#root>

FTD72#

show run tunnel-group DefaultRAGroup

tunnel-group DefaultRAGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultRAGroup webvpn-attributes
authentication certificate

without-csd

FTD72#

show run tunnel-group DefaultWEBVPNGroup

tunnel-group DefaultWEBVPNGroup general-attributes address-pool TEST-POOL tunnel-group DefaultWEBVPNGroup webvpn-attributes authentication certificate

without-csd

Disabilitare gli alias di gruppo e abilitare gli URL di gruppo

Passare a un profilo di connessione e selezionare la scheda 'Alias'. Disabilitare o eliminare l'alias

del gruppo e fare clic sull'icona più per aggiungere un alias URL.

Edit Connection Profile		
Connection Profile:* LDAP-TG		
Group Policy:* DfltGrpPolicy	• +	
Client Address Assignment AAA Aliases		
Alias Names:		
Incoming users can choose an alias name upon first login. Alias on this device can be turned on or off for display.	ses from all connections	configured +
Name	Status	
LDAP	Disabled	1
URL Alias:		
Configure the list of URL alias which your endpoints can select following URLs, system will automatically log them in via this co	on web access. If users onnection profile.	choose the
URL	Status	

Disattivazione dell'opzione group-alias per un gruppo di tunnel all'interno dell'interfaccia utente di FMC.

Configurare un nome oggetto per l'alias URL e compilare il nome di dominio completo (FQDN) e/o l'indirizzo IP del firewall per l'URL, seguito dal nome a cui si desidera associare il profilo di connessione. In questo esempio, abbiamo scelto 'aaldap'. Più è oscuro, più è sicuro, perché è meno probabile che gli aggressori indovinino l'URL completo anche se hanno ottenuto il tuo FQDN. Al termine, selezionare Salva.

Edit URL Objects		8
Name LDAP-ALIAS		
Description		
URL https://ftd1	.com/aaaldaj	
Allow Overrides		
	Cancel	Save

Creazione di un oggetto URL-Alias nell'interfaccia utente di FMC.

Selezionare l'alias dell'URL dall'elenco a discesa, selezionare la casella Abilitato e selezionare OK.



Verificare che l'URL-Alias sia abilitato nell'interfaccia utente di FMC.

Verificare che l'alias del gruppo sia stato eliminato o disabilitato e che l'alias dell'URL sia abilitato, quindi selezionare Salva.

Edit Connection Profile		0	
Connection Profile:* LDAP-TG			
Group Policy:* DfltGrpPolicy Edit Group Policy	• +		
Client Address Assignment AAA Aliases			
Incoming users can choose an alias name upon first login. Alia on this device can be turned on or off for display.	ases from all connections config	gured 1	
Name	Status		
LDAP	Disabled 💉	Ì	
URL Alias: Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile. +			
URL	Status		
LDAP-ALIAS (https://ftd1 com/aaaldap)	Enabled 💉	ī	
	Cancel	Save	

Attivazione dell'opzione URL-Alias per un gruppo di tunnel all'interno dell'interfaccia utente di FMC.

Se lo si desidera, è inoltre possibile eseguire il push degli alias URL come parte del file XML. A tale scopo, è possibile modificare il codice XML utilizzando l'Editor di profili VPN o l'Editor di profili ASA. A tale scopo, passare alla scheda Elenco server e verificare che il campo Gruppo utenti corrisponda all'alias URL del profilo di connessione quando si utilizza SSL. Per IKEv2, verificare che il campo Gruppo utenti corrisponda esattamente al nome del profilo di connessione.

Server List Entry X
Primary Server Display Name (required) FTD1-5SL Primary Protocol SSL PQDN or IP A Ider Group finds Group URL finds Bachup Servers Bachup Servers
Host Address Add Move Up Move D Delete
OK Cancel

Modifica del profilo XML in modo che abbia un URL-Alias per le connessioni SSL.

Mapping certificati

Passare alla scheda Avanzate nei criteri VPN di Accesso remoto. Scegliere un'opzione di impostazione generale in base alle preferenze. Una volta selezionato, selezionare Aggiungi mapping.

RAVPN			You have unsaved changes Save Cancel
Enter Description			
			Policy Assignments.(1)
Overseller Derfle Assessleted	and the second	Local Realm:	None Dynamic Access Policy: None
Connection Profile Access Intern	aces Advanced		
Secure Client Images	General Settings for Connection Profile Mapping The device processes the policies in the order listed below until it finds a match		
GUI Text and Messages	Use group URL if group URL and Certificate Map match different Connection Profiles		
Icons and Images	Use the configured rules to match a certificate to a Connection Profile		
Scripts	Certificate to Connection Profile Mapping		
Binaries	Client request is checked against each Centricate Map, associated Connection Prome will be used when rules are may Please provide at least one Certificate Mapping.	neo. Il none ol trie Ceruncate Map is matcheo, delaut connection prolite Will de chosen.	
Custom Installer Transforms			Add Mapping
Localized Installer Transforms	Certificate Map	Connection Profile	
Address Assignment Policy		No Records Found	
Certificate Maps			
Group Policies			
LDAP Attribute Mapping			
Load Balancing			
✓ IPsec			
Crypto Maps			
IKE Policy	Defecti Generative Beekin		
IPsec/IKEv2 Parameters	This Connection Profile will be applied when none of the Cartificate Map's rule is matched.		•

Passare alla scheda Avanzate nell'interfaccia utente di FMC per creare un oggetto mappa certificati nell'interfaccia utente di FMC.

Assegnare un nome all'oggetto mappa certificati e selezionare Aggiungi regola. In questa regola, definire le proprietà del certificato che si desidera identificare per mappare l'utente a un determinato profilo di connessione. Al termine, selezionare OK, quindi Salva.

Add Certificate N	Мар			0
Map Name*: Certificate-Map-C Mapping Rule Configure the certifi	CN icate matching rule		(Add Rule
# Field	Component	Operator	Value	
1 Subject	CN (Common Name	Equals 🔻	customvalu	e
OK Canc	el			
			Cance	Save

Creare una mappa certificati e aggiungere i criteri per la mappa all'interno dell'interfaccia utente di FMC.

Dall'elenco a discesa selezionare l'oggetto mappa certificati e il profilo di connessione a cui si desidera associare la mappa certificati. Quindi selezionare OK.

Add Connection Profile to Cer	rtificate Map 🛛 🔞
Choose a Certificate Map and associat selected Certficate Map.	te Connection Profiles to
Certificate Map Name*:	
Certificate-Map-CN -) +
Connection Profile*:	
LDAP-TG 👻]
	Cancel

Collegare l'oggetto mappa certificato al gruppo di tunnel desiderato all'interno dell'interfaccia utente di FMC.

Assicurarsi che il profilo di connessione predefinito sia configurato come DefaultWEBVPNGroup in modo che se un utente non riesce a eseguire il mapping, venga inviato a DefaultWEBVPNGroup. Al termine, selezionare Salva e distribuire le modifiche.

RAVPN			You have unasved changes Save Cancel
Enter Description			Policy Assignments (1)
			Local Realm: None Dynamic Access Policy: None
Connection Profile Access Inter	faces Advanced		
Secure Client Images Secure Client Customization GUI Text and Messages Icons and Images	General Settings for Connection Profile Mapping The divice processes the policies in the order tailed below until it india a match Use group URI, if group URI, and Certificate Map match different Connection Profiles group URI is the configured rules to match a certificate to a Connection Profile Certificate to Connection Profile		
Scripts	Client request is checked against each Certificate Map, associated Connection Profile will be used when rul	es are matched. If none of the Certificate Map is matched, default connect	tion profile will be chosen.
Binaries			Add Mapping
Localized Installer Transforms	Pertificate Man	Connection Profile	
Address Assignment Policy	Certificate Map	Connection Prome	
Certificate Maps	Certificate-Map-CN	LDAP-TG	
Group Policies			
LDAP Attribute Mapping			
Load Balancing			
V IPsec			
Crypto Maps			
IKE Policy IPsec/IKEv2 Parameters	Default Connection Profile: This Connection Profile will be applied when more of the Contribute May's note is matched.		DefaultWEBVPNGroup *

Modificare il profilo di connessione predefinito per il mapping dei certificati in DefaultWEBVPNGroup all'interno dell'interfaccia utente di FMC.

IPsec-IKEv2

Selezionare il profilo di connessione IPsec-IKEv2 desiderato e passare a Modifica Criteri di

gruppo.

Edit Connection Profil	e	
Connection Profile:*	IKEV2	
Group Policy:*	IKEV2-IPSEC +	
Client Address Assignmen	t AAA Aliases	

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools:

Name	IP Address Range	
AnyConnect_Pool	10.50.50.1-10.50.50.6	/1
DHCP Servers:		+
Name	DHCP Server IP Address	
	Can	cel Save

Modificare un criterio di gruppo nell'interfaccia utente di FMC.

Nella scheda General (Generale), individuare la sezione VPN Protocols (Protocolli VPN) e verificare che la casella IPsec-IKEv2 sia selezionata.

Edit Group Policy	
Name:* IKEV2-IPSEC Description:	
General Secure	Client Advanced
VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling	VPN Tunnel Protocol: Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel. ☐ SSL ✔ IPsec-IKEv2

Abilitare IPsec-IKEv2 in un criterio di gruppo nell'interfaccia utente di FMC.

Nell'Editor di profili VPN o nell'Editor di profili ASA, passare alla scheda Elenco server. Il nome del gruppo di utenti DEVE corrispondere esattamente al nome del profilo di connessione sul firewall. Nell'esempio, IKEV2 era il profilo di connessione/nome del gruppo di utenti. Il protocollo primario è configurato come IPsec. Il nome visualizzato in viene visualizzato nell'interfaccia utente del client protetto quando si stabilisce una connessione a questo profilo di connessione.

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certifica	ate Pinning
Primary Server Display Name (required) FTD1-IPSEC FQDN or IP A User Group ftd1 com / IKEV2 Group URL	Connection Information Primary Protocol IPsec ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect KE Identity (IOS gateway only)
Backup Servers Host Address	Add Move Up Move D Delete
OK	Cancel

Modificare il profilo XML in modo che il protocollo primario sia IPsec e che il gruppo di utenti corrisponda al nome del profilo di connessione.



Attenzione: è necessaria una connessione SSL per eseguire il push dei profili XML dal firewall al client. Quando si utilizza solo IKEV2-IPsec, è necessario eseguire il push dei profili XML ai client tramite un metodo fuori banda.

Una volta eseguito il push del profilo XML al client, Secure Client utilizza il gruppo di utenti del profilo XML per connettersi al profilo di connessione IKEV2-IPsec.

🕲 Cisco Secure	e Client	_		×
	AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC	~	Connect	
Cisco Sec	cure Client FTD1-IPSEC		×	altalta cisco
Use Pas	ername: nroche sword:			
		1		

Visualizzazione interfaccia utente client sicura del tentativo di connessione RAVPN IPsec-IKEv2.

Esempi di configurazione di ASA

Disabilitare l'autenticazione AAA nei profili di connessione DefaultWEBVPNGroup e DefaultRAGroup

Immettere la sezione webvpn-attributes per il gruppo di tunnel DefaultWEBVPNGroup e specificare l'autenticazione come basata sul certificato. Ripetere questa procedura per DefaultRAGroup. Gli utenti che accedono a questi profili di connessione predefiniti sono costretti a presentare un certificato per l'autenticazione e non hanno la possibilità di immettere credenziali di nome utente e password.

Disabilitare Hostscan / Secure Firewall Posture su DefaultWEBVPNGroup e DefaultRAGroup (facoltativo)

Questa operazione è necessaria solo se si dispone di Hostscan/Secure Firewall Posture nell'ambiente. Questo passaggio impedisce agli autori di attacchi di aumentare l'utilizzo delle risorse nel firewall causato dal processo di scansione dell'endpoint. Immettere la sezione webvpn-attributes per i profili DefaultWEBVPNGroup e DefaultRAGroup e connessione e implementare without-csd per disabilitare la funzionalità di scansione dell'endpoint.

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

ASA# configure terminal ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

Disabilitare gli alias di gruppo e abilitare gli URL di gruppo

Immettere i gruppi di tunnel a cui gli utenti si stanno connettendo. Se è presente un alias di gruppo esistente, disabilitarlo o rimuoverlo. In questo esempio è disattivato. Al termine, creare un URL del gruppo utilizzando l'FQDN o l'indirizzo IP dell'interfaccia di terminazione RAVPN. Il nome alla fine dell'URL del gruppo deve essere oscuro. Evitare valori comuni come VPN, AAA, RADIUS, LDAP in quanto questi rendono più facile agli aggressori indovinare l'URL completo se ottengono l'FQDN. Usare al suo interno nomi significativi che consentano di identificare il gruppo di tunnel.

ASA# configure terminal ASA(config)# tunnel-group NAME webvpn-attributes ASA(config-tunnel-webvpn)# group-alias NAME disable ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable

Mapping certificati

In modalità di configurazione globale, creare una mappa dei certificati e assegnarle un nome e un numero di sequenza. Definire quindi una regola a cui gli utenti devono corrispondere per utilizzare il mapping. In questo esempio, gli utenti devono soddisfare i criteri di un valore di nome comune uguale a "customvalue". Quindi, immettere la configurazione webvpn e applicare la mappa dei certificati al gruppo di tunnel desiderato. Al termine, immettere DefaultWEBVPNGroup e impostare questo gruppo di tunnel come predefinito per gli utenti che non eseguono correttamente il mapping dei certificati. Se il mapping ha esito negativo, gli utenti vengono indirizzati al DefaultWEBVPNGroup. Mentre DefaultWEBVPNGroup è configurato con l'autenticazione del certificato, gli utenti non hanno l'opzione di passare le credenziali di nome utente o password.

ASA(config)# crypto ca certificate map NAME 1 ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

ASA(config)# webvpn ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME

ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# tunnel-group-map default-group

IPsec-IKEv2

In modalità di configurazione globale è possibile modificare un criterio di gruppo esistente o crearne uno nuovo e immettere gli attributi per tale criterio. Nella sezione degli attributi, abilitare IKEv2 come unico protocollo del tunnel vpn. Verificare che questo criterio di gruppo sia associato a un gruppo di tunnel che verrà utilizzato per le connessioni VPN ad accesso remoto IPsec-IKEV2. Analogamente alla procedura FMC, è necessario modificare il profilo XML con l'Editor di profili VPN o l'Editor di profili ASA e modificare il campo User Group in modo che corrisponda al nome del gruppo di tunnel sull'appliance ASA, quindi modificare il protocollo in IPsec.

ASA# configure terminal ASA(config)# group-policy GP-NAME internal ASA(config)# group-policy GP-NAME attributes ASA(config-group-policy)# vpn-tunnel-protocol ikev2

ASA(config)# tunnel-group TG-NAME general-attributes ASA(config-tunnel-general)# default-group-policy GP-NAME

Nell'Editor di profili VPN o nell'Editor di profili ASA, passare alla scheda Elenco server. Il nome del gruppo di utenti DEVE corrispondere esattamente al nome del profilo di connessione sul firewall. Il protocollo primario è configurato come IPsec. Il nome visualizzato viene visualizzato nell'interfaccia utente del client protetto quando si stabilisce una connessione a questo profilo di connessione.

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certific	cate Pinning
Primary Server Display Name (required) ASA-IPsec FQDN or IP A FQDN FQDN FQDN FQDN FQDN FQDN/TG-NAME FQDN/TG-NAME	Connection Information Primary Protocol IPsec ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only)
Backup Servers	Add Move Up Move D Delete
ОК	Cancel

Modificare il profilo XML in modo che il nome del protocollo primario sia IPsec e il nome del gruppo di utenti corrisponda al nome del gruppo di tunnel dell'ASA per le connessioni VPN IPsec-IKEv2.



Attenzione: è necessaria una connessione SSL per eseguire il push dei profili XML dal firewall al client. Quando si utilizza solo IKEV2-IPsec, è necessario eseguire il push dei profili XML ai client tramite un metodo fuori banda.

Conclusioni

In sintesi, lo scopo delle procedure di protezione avanzata descritte in questo documento è mappare gli utenti legittimi a profili di connessione personalizzati, mentre gli utenti non autorizzati sono obbligati a utilizzare DefaultWEBVPNGroup e DefaultRAGroup. In una configurazione ottimizzata, i due profili di connessione predefiniti non dispongono di alcuna configurazione legittima del server AAA personalizzato. Inoltre, la rimozione degli alias di gruppo impedisce agli aggressori di identificare facilmente i profili di connessione personalizzati rimuovendo la visibilità a discesa durante lo spostamento sull'FQDN o sull'indirizzo IP pubblico del firewall.

Informazioni correlate

- Supporto tecnico Cisco e download
- Attacchi con spray di password
- Vulnerabilità degli accessi non autorizzati, settembre 2023
- Guide alla configurazione dell'ASA
- Guide alla configurazione di FMC / FDM

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).