Implementierung von Härtungsmaßnahmen für Secure Client AnyConnect VPN

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konzepte Sichere Client-Härtung bei Cisco Secure Firewall: Identifizierung von Angriffen mithilfe von Protokollierung und Syslog-IDs Überprüfung des Angriffs Beispiele für FMC-Konfiguration Deaktivieren Sie die AAA-Authentifizierung in den Verbindungsprofilen DefaultWEBVPNGroup und DefaultRAGroup. Deaktivieren Sie Hostscan/Secure Firewall Posture auf der DefaultWEBVPNGroup und DefaultRAGroup (optional). Gruppenaliase deaktivieren und Gruppen-URLs aktivieren **Zertifikatszuordnung** IPsec-IKEv2 ASA-Konfigurationsbeispiele Deaktivieren Sie die AAA-Authentifizierung in den Verbindungsprofilen DefaultWEBVPNGroup und DefaultRAGroup. Deaktivieren Sie Hostscan/Secure Firewall Posture auf der DefaultWEBVPNGroup und DefaultRAGroup (optional). Gruppenaliase deaktivieren und Gruppen-URLs aktivieren Zertifikatszuordnung IPsec-IKEv2 **Schlussfolgerung** Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Sicherheit Ihrer Remote Access VPN-Implementierung verbessern können.

Voraussetzungen

Anforderungen

Cisco empfiehlt Ihnen, sich mit folgenden Themen vertraut zu machen:

- Cisco Secure Client AnyConnect-VPN
- Konfiguration von ASA/FTD für Remote-Zugriff.

Verwendete Komponenten

Der Leitfaden mit Best Practices basiert auf den folgenden Hardware- und Softwareversionen:

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

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



Achtung: Dieses Dokument enthält keine Schritte für den FirePOWER Geräte-Manager (FDM). Der FDM unterstützt nur das Ändern der Authentifizierungsmethode in der DefaultWEBVPNGroup-Gruppe. Verwenden Sie Kontrollebenen-ACLs oder einen

benutzerdefinierten Port im Abschnitt "Globale Einstellungen" des Remote Access-VPN in der FDM-Benutzeroberfläche. Wenden Sie sich bei Bedarf an das Cisco Technical Assistance Center (TAC).

Hintergrundinformationen

Mit diesem Dokument soll sichergestellt werden, dass die Cisco Secure Client AnyConnect VPN-Konfiguration den Best Practices für die Sicherheit in einer modernen Welt entspricht, in der Cyberangriffe weit verbreitet sind.

Brute-Force-Angriffe beinhalten in der Regel wiederholte Versuche, über eine Kombination aus Benutzername und Passwort Zugriff auf eine Ressource zu erhalten. Angreifer versuchen, ihren Internet-Browser, die Secure Client-Benutzeroberfläche oder andere Tools zu verwenden, um mehrere Benutzernamen und Kennwörter einzugeben, in der Hoffnung, dass sie mit einer legitimen Kombination in einer AAA-Datenbank übereinstimmen. Bei Verwendung von AAA für die Authentifizierung erwarten wir, dass der Endbenutzer seinen Benutzernamen und sein Kennwort eingibt, da dies für die Herstellung der Verbindung erforderlich ist. Gleichzeitig überprüfen wir erst, wer der Benutzer ist, wenn er seine Anmeldeinformationen eingegeben hat. Dadurch können Angreifer die folgenden Szenarien ausnutzen:

- 1. Verfügbare vollqualifizierte Domänennamen für die Cisco Secure Firewall (insbesondere bei Verwendung von Gruppen-Aliasnamen im Verbindungsprofil):
 - Wenn der Angreifer den FQDN Ihrer VPN-Firewall erkennt, hat er die Möglichkeit, die Tunnel-Gruppe unter Verwendung des Gruppenalias auszuwählen, unter dem er den Brute-Force-Angriff starten möchte.
- 2. Mit AAA oder lokaler Datenbank konfiguriertes Standard-Verbindungsprofil:
 - Wenn der Angreifer den FQDN der VPN-Firewall findet, kann er versuchen, einen Brute-Force-Angriff auf den AAA-Server oder die lokale Datenbank durchzuführen. Dies liegt daran, dass die Verbindung zum FQDN im Standardverbindungsprofil landet, selbst wenn keine Gruppenaliase angegeben ist.
- 3. Auslastung der Ressourcen auf der Firewall oder auf AAA-Servern:
 - Angreifer können AAA-Server oder Firewall-Ressourcen überlasten, indem sie große Mengen an Authentifizierungsanforderungen senden und eine Denial of Service (DoS)-Bedingung auslösen.

Konzepte

Gruppenaliase:

• Ein alternativer Name, über den die Firewall auf ein Verbindungsprofil verweisen kann. Nach dem Herstellen einer Verbindung zur Firewall werden diese Namen in einem Dropdown-

Menü in der Secure Client UI angezeigt, das von Benutzern ausgewählt werden kann. Beim Entfernen von Gruppenaliasen wird die Dropdown-Funktion in der Secure Client-Benutzeroberfläche entfernt.

Gruppen-URLs:

 Eine URL, die mit einem Verbindungsprofil verknüpft werden kann, sodass eingehende Verbindungen direkt einem gewünschten Verbindungsprofil zugeordnet werden. Es gibt keine Dropdown-Funktion, da Benutzer die vollständige URL in der Secure Client-Benutzeroberfläche eingeben können, oder die URL kann mit einem Anzeigenamen im XML-Profil integriert werden, um die URL vor dem Benutzer auszublenden.

Der Unterschied besteht darin, dass bei der Implementierung von Gruppenaliasen ein Benutzer eine Verbindung to vpn_gateway.example.com herstellt und Aliase erhält, die ihn zu einem Verbindungsprofil führen. Mit Gruppen-URLs stellt ein Benutzer eine Verbindung zu vpn_gateway.example.com/example_group her und leitet diese direkt zum Verbindungsprofil weiter, ohne dass ein Dropdown-Menü erforderlich oder verfügbar wäre.

Sichere Client-Härtung bei Cisco Secure Firewall:

Diese Methoden basieren auf der Zuordnung legitimer Benutzer zu entsprechenden Tunnelgruppen/Verbindungsprofilen, während potenziell böswillige Benutzer an eine Trap-Tunnelgruppe gesendet werden, die wir so konfigurieren, dass sie keine Kombinationen von Benutzernamen und Kennwort zulassen. Obwohl nicht alle Kombinationen implementiert werden müssen, müssen Gruppenaliase deaktiviert und die Authentifizierungsmethode von DefaultWEBVPNGroup und DefaultRAGroup geändert werden, damit die Empfehlungen wirksam funktionieren.

- Deaktivieren Sie Gruppen-Aliase, und verwenden Sie nur group-url in der Konfiguration des Verbindungsprofils. Dies ermöglicht Ihnen, einen bestimmten FQDN zu haben, der für einen Angreifer nicht einfach zu erkennen und auszuwählen ist, da nur die Clients mit dem richtigen FQDN die Verbindung initiieren können. Beispielsweise ist vpn_gateway.example.com/example_group für einen Angreifer schwieriger zu erkennen als vpn_gateway.example.com.
- Deaktivieren Sie die AAA-Authentifizierung in DefaultWEBVPNGroup und DefaultRAGroup, und konfigurieren Sie die Zertifikatsauthentifizierung. Dadurch wird Brute-Force-Angriffe auf die lokale Datenbank oder den AAA-Server vermieden. In diesem Szenario würde der Angreifer sofort Fehler erhalten, wenn er versucht, eine Verbindung herzustellen. Es gibt kein Feld für den Benutzernamen oder das Kennwort, da die Authentifizierung auf Zertifikaten basiert und somit Brute-Force-Versuche gestoppt werden. Eine weitere Option besteht darin, einen AAA-Server ohne unterstützende Konfiguration zu erstellen, um eine Sicherheitslücke für böswillige Anfragen zu schaffen.
- Verwenden Sie die Zertifikatszuordnung für das Verbindungsprofil. Auf diese Weise können eingehende Verbindungen bestimmten Verbindungsprofilen zugeordnet werden, basierend

auf Attributen, die von Zertifikaten auf dem Clientgerät empfangen wurden. Benutzer, die über die richtigen Zertifikate verfügen, werden korrekt zugeordnet, während Angreifer, die die Zuordnungskriterien nicht erfüllen, an die DefaultWEBVPNGroup gesendet werden.

 Die Verwendung von IKEv2-IPSec anstelle von SSL führt dazu, dass sich Tunnelgruppen auf eine bestimmte Benutzergruppenzuordnung im XML-Profil verlassen. Ohne diese XML auf dem Endbenutzercomputer werden die Benutzer automatisch an die standardmäßige Tunnelgruppe gesendet.



Hinweis: Weitere Informationen zur Gruppenalias-Funktion finden Sie im <u>ASA VPN-</u> <u>Konfigurationshandbuch</u> unter "Tabelle 1. Connection Profile Attributes for SSL VPN'.

Identifizierung von Angriffen mithilfe von Protokollierung und Syslog-IDs

Brute-Force-Angriffe stellen die vorherrschende Methode zur Kompromittierung von Remote

Access-VPNs dar. Dabei werden schwache Passwörter ausgenutzt, um sich unbefugten Zugriff zu verschaffen. Es ist wichtig zu wissen, wie man Anzeichen eines Angriffs erkennt, indem man die Verwendung von Protokollierung und Auswertung von Syslogs nutzt. Gängige Syslogs-IDs, die auf einen Angriff hinweisen können, wenn ein ungewöhnliches Volume auftritt, sind:

%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

Der Benutzername wird immer ausgeblendet, bis der Befehl no logging hide username auf der ASA konfiguriert wird.



Hinweis: Hinweis: Dies gibt Aufschluss darüber, ob gültige Benutzer von IP-Adressen mit Sicherheitsverletzungen erstellt wurden oder bekannt sind. Seien Sie jedoch vorsichtig, da die Benutzernamen in den Protokollen angezeigt werden.

Cisco ASA-Protokollierung:

Benutzerhandbuch zur sicheren ASA-Firewall Protokollierung des Kapitels Cisco Secure Firewall ASA-Serie Allgemeiner CLI-Konfigurationsleitfaden für den Betrieb

Cisco FTD-Protokollierung:

Konfigurieren der Protokollierung auf FTD über FMC

Konfigurieren Sie den Abschnitt Syslog im Kapitel "Plattform-Einstellungen" des Cisco Secure Firewall Management Center Gerätekonfigurationsleitfadens. Konfiguration und Überprüfung des Syslog im FirePOWER Geräte-Manager Konfigurieren der Systemprotokollierungseinstellungen im Kapitel "Systemeinstellungen" des Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager

Überprüfung des Angriffs

Melden Sie sich zur Überprüfung bei der ASA- oder FTD-Befehlszeilenschnittstelle (CLI) an, führen Sie den Befehl show aaa-server aus, und untersuchen Sie die Anzahl der Authentifizierungsanforderungen, die an einen der konfigurierten AAA-Server gesendet wurden, auf ungewöhnlich viele, versucht oder abgelehnt wurden:

<#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

Beispiele für FMC-Konfiguration

Deaktivieren Sie die AAA-Authentifizierung in den Verbindungsprofilen DefaultWEBVPNGroup und DefaultRAGroup.

Navigieren Sie zu Geräte > Remotezugriff.

Firev	vall Manage ew / Dashboard	ement Center s / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration		
Summar Provides a summa Network	mary Dashboard (switch dashboard) summary of activity on the appliance ork Threats Intrusion Events Status Geolocation QoS		Device M NAT QoS Platform FlexConf	lanagement Settings īg	VPN Site To Site Remote Access Dynamic Access P Troubleshooting	olicy	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture			
► Top Zero	Trust Applicatio	ons			- ×	Certificat	les			Upgrade Threat Defense Upgrade Chassis Upgrade

Zeigt an, wie Sie in der FMC-GUI zur Konfiguration der VPN-Richtlinie für den Remote-Zugriff navigieren.

Bearbeiten Sie die vorhandene VPN-Richtlinie für den Remote-Zugriff, und erstellen Sie ein Verbindungsprofil mit dem Namen "DefaultRAGroup".

Fir Dev	ewall Management Center ices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 📀	¢ 0	admin ~	citco SECURE
													Add
Name					Status			Last Modified					
RAVPN					Targeting 1 d	devices on all targeted		2024-03-07 10:58:20 Modified by "admin"			9	/1	

Zeigt, wie die VPN-Richtlinie für den Remotezugriff in der FMC-Benutzeroberfläche bearbeitet wird.

Bearbeiten Sie die Verbindungsprofile 'DefaultWEBVPNGroup' und 'DefaultRAGroup'.

Firewall Management Center Devices / VPN / Edit Connection Profile	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q (admin 🗸 🙁 🕹 🕹
RAVPN								Save
Enter Description								
								Policy Assignments (1)
							Local Realm: LOCAL-REALM	Dynamic Access Policy: None
Connection Profile Access Interfaces A	dvanced							
Name			AAA				Group Policy	
DefaultWEBVPNGroup			Authentication: Authorization: Accounting:	LOCAL None None			DittGrpPolicy	

Zeigt, wie die DefaultWEBVPNGroup in der FMC-Benutzeroberfläche bearbeitet wird.

Navigieren Sie zur Registerkarte AAA, und wählen Sie das Dropdown-Menü Authentication

Method aus. Wählen Sie 'Nur Client-Zertifikat' und dann Speichern.

Edit Connection Profile		0
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	ve

Ändern der Authentifizierungsmethode in ein Clientzertifikat nur für die DefaultWEBVPNGroup innerhalb der FMC-Benutzeroberfläche.

Bearbeiten Sie DefaultRAGroup, und navigieren Sie zur Registerkarte AAA, und wählen Sie das Dropdown-Menü Authentication Method (Authentifizierungsmethode) aus. Wählen Sie 'Nur Client-Zertifikat' und dann Speichern aus.

Edit Connection Profile		
Connection Profile:*	DefaultRAGroup	
Group Policy:*	DfltGrpPolicy +	
Ed 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	ive

Ändern der Authentifizierungsmethode in ein Clientzertifikat nur für die DefaultRAGroup innerhalb der FMC-Benutzeroberfläche.



Hinweis: Bei der Authentifizierungsmethode kann es sich auch um einen Sinkhole-AAA-Server handeln. Wenn diese Methode verwendet wird, ist die AAA-Serverkonfiguration gefälscht und verarbeitet keine Anforderungen. Außerdem muss auf der Registerkarte "Client Address Assignment" (Client-Adressenzuweisung) ein VPN-Pool definiert werden, um die Änderungen zu speichern.

Deaktivieren Sie Hostscan/Secure Firewall Posture auf der DefaultWEBVPNGroup und DefaultRAGroup (optional).

Dies ist nur erforderlich, wenn Sie Hostscan/Secure Firewall Posture in Ihrer Umgebung haben. Dieser Schritt verhindert, dass Angreifer die durch den Endpunkt-Scanvorgang verursachte Ressourcennutzung auf der Firewall erhöhen. Im FMC wird dies durch das Erstellen eines FlexConfig-Objekts mit dem Befehl without-csd erreicht, um die Endpunkt-Scanfunktion zu deaktivieren.

Navigieren Sie zu Objekte > Objektverwaltung > FlexConfig-Objekt > FlexConfig-Objekt hinzufügen.

Cipiects / Object Management	t Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 🕢 admin 🗸	cisco SECURE
 AAA Server Access List Address Pools Application Filters 	FlexConfig Object PlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in RexConfig polices.	Add RescConfig Object	
AS Path	Name	Description	
BFD Template Circher Suite List	Anyconnect_route_litering		6/ €^
Community List	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNS	¶aq ≣
DHCP IPv6 Pool	Default_Inspection_Protocol_Disable	Disable Default Inspection.	¶∎ Q ⊕
Distinguished Name DNS Sequer Group	Default_Inspection_Protocol_Enable	Enable Default Inspection.	¶a q ≣
> External Attributes	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recip	¶a q ≣
File List	DHCPv6_Prefix_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 Q ⊕
Text Object	DNS_UnConfigure	Remove the DNS configurations.	¶a Q ⊕
Geolocation	Egrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-su	G Q ⊕
Interface Key Chain	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authent	6 Q ⊕
Network	Eigr_UnConfigure	Clears eigrp configuration for an AS	G Q =

Navigieren in der FMC-Benutzeroberfläche zum Erstellen eines FlexConfig-Objekts

Nennen Sie das FlexConfig-Objekt, und legen Sie die Bereitstellung auf Everytime mit dem Typ Append fest. Geben Sie dann die Syntax genau wie dargestellt ein, und speichern Sie das Objekt.

Edit FlexConfig Object						0
Name: Wtihout-CSD Description: Copy-pasting any rich text might int	troduce line breaks wh	ille generating CLI. Pleas	e verify the	CLI before deployn	nent.	
Insert - 🔣 Deployment	Everytime	•	Type:	Append	•	
tunnel-group DefaultWEBVPNGroup w without-csd tunnel-group DefaultRAGroup webvp without-csd	ebvpn-attributes					
▼ Variables						
Name	Dimension D	efault Value (Typ	erty e:Name)	Override	Description	
		No records to display				
					Cancel	Save

Erstellen eines FlexConfig-Objekts mit "ohne CSD"

Navigieren Sie zu Devices > FlexConfig, und klicken Sie dann auf den Bleistift, um die FlexConfig-

Richtlinie zu bearbeiten.

· didd SECURE	📍 🔅 😧 🛛 admin -	۹ 🔮	Deploy		Integration	Objects	Devices	Policies	Analysis	Overview	Firewall Management Center Devices / FlexConfig	Ū,
New Policy												
				Last Modified		Status					FlexConfig Policy	P
¶ ∠ ∎				2024-04-10 21:54:19 Modified by "admin"	1 devices te on 1 targeted devices	Targeting 1 Out-of-date					Flax-Test	
u 2				2024-04-10 21:54:19 Modified by "admin"	I devices	Targeting 1 Out-of-dat					Fiex-Test	

Bearbeiten der FlexConfig-Richtlinie innerhalb des FMC

Suchen Sie das Objekt, das Sie im Abschnitt Benutzerdefiniert erstellt haben. Klicken Sie anschließend auf den Pfeil, um es zu "Ausgewählte FlexConfigs anhängen" hinzuzufügen. Wählen Sie abschließend Speichern, um die FlexConfig-Richtlinie zu speichern.

Firewall Management Center Devices / Flexcoring Policy Editor	Overvie	w Analysis	Policies	Devices	Objects	Integration	Depkoy Q 🧬 🗱 🌚 🛛 admin 🗸 🖓	
FlexConfig Enter Description							You have unsaved changes Migrate Config Preview Config Save	Cancel
							Policy Assignment	ins (1)
	n Se	lected Prepend F	lexConfigs					
Available FlexConfig C FlexConfig Object		Name			Description			
Vuser Defined	7							
"3 Anyconnect_route_filtering								
"2 Keepout								
"] No_Keepout								
"? Wtihout-CSD								
V System Defined								
" Default_DNS_Configure								
Default_Inspection_Protocol_Disable								
Default_Inspection_Protocol_Enable	Se	lected Append FI	exConfigs					
DHCPv6_Prefx_Delegation_Configure		Namo			Description			
DHCPv6_Prefix_Delegation_UnConfigure		Without-CSD						=
DNS_Configure		Wanton Coo						-
_9 DNS_UnConfigure								
12 Eigrp_Configure								

Hängen Sie das FlexConfig-Objekt an die FlexConfig-Richtlinie an.

Wählen Sie Policy Assignments (Richtlinienzuweisungen) und das FTD aus, auf das Sie diese FlexConfig-Richtlinie anwenden möchten. Wählen Sie anschließend OK. Wählen Sie erneut Speichern, wenn es sich um eine neue FlexConfig-Zuweisung handelt, und stellen Sie die Änderungen bereit. Überprüfen Sie nach der Bereitstellung

Firewall Management Center Devices / Flexcorify Policy Editor	Overview Anal	ysis Policies	Devices 0	Objects Inte	egration		Deploy Q 🧬 🛱 😡	admin ~ duto SECURE
FlexConfig Enter Description								Config Sava Cancel
Available FlexConfig C FlexConfig Object	Selected Prep	end FlexConfigs	Desc	cription				Policy Assignments (1)
V User Defined		Targeted Devices Targeted Devices Select devices to t Available Devices Q. Search by nam FTD1	swhich you want to					
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. 🗑

Weisen Sie die FlexConfig-Richtlinie einem FirePOWER-Gerät zu.

Geben Sie die FTD-CLI ein, und geben Sie den Befehl show run tunnel-group für DefaultWEBVPNGroup und DefaultRAGroup aus. Vergewissern Sie sich, dass "without-csd" in der Konfiguration vorhanden ist.

<#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

Gruppenaliase deaktivieren und Gruppen-URLs aktivieren

Navigieren Sie zu einem Verbindungsprofil und wählen Sie die Registerkarte 'Aliase'. Deaktivieren oder löschen Sie den Gruppenalias, und klicken Sie auf das Pluszeichen, um einen URL-Alias hinzuzufügen.

Edit Connection Profile		e						
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 on web access. If users choose the following URLs, system will automatically log them in via this connection profile.								
URL	Status							

Deaktivieren der Gruppenalias-Option für eine Tunnelgruppe in der FMC-Benutzeroberfläche.

Konfigurieren Sie einen Objektnamen für den URL-Alias, und geben Sie den FQDN und/oder die IP-Adresse der Firewall für die URL ein, gefolgt vom Namen, mit dem Sie das Verbindungsprofil verknüpfen möchten. In diesem Beispiel haben wir 'aaaldap' gewählt. Je obskurer, desto sicherer, da es für Angreifer weniger wahrscheinlich ist, die vollständige URL zu erraten, selbst wenn sie Ihren FQDN erhalten haben. Wählen Sie anschließend Speichern aus.



Erstellen eines URL-Alias-Objekts in der FMC-Benutzeroberfläche

Wählen Sie aus dem Dropdown-Menü den URL-Alias aus, aktivieren Sie das Kontrollkästchen Enabled (Aktiviert), und wählen Sie OK aus.



Stellen Sie sicher, dass der URL-Alias in der FMC-Benutzeroberfläche aktiviert ist.

Stellen Sie sicher, dass der Gruppenalias gelöscht oder deaktiviert ist, und stellen Sie sicher, dass der URL-Alias jetzt aktiviert ist. Wählen Sie anschließend Speichern aus.

Edit Connection Profile		Ø
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. Ali on this device can be turned on or off for display.	ases from all connections conf	igured +
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	ct on web access. If users choo connection profile.	ose the +
URL	Status	
LDAP-ALIAS (https://ftd1 com/aaaldap)	Enabled 💉	1
	Cancel	Save

Aktivieren der Option URL-Alias für eine Tunnelgruppe in der FMC-Benutzeroberfläche.

Bei Bedarf können URL-Aliase auch als Teil des XML-Codes weitergegeben werden. Dies wird durch die Bearbeitung des XML-Codes mit dem VPN Profile Editor oder dem ASA Profile Editor erreicht. Navigieren Sie zu diesem Zweck zur Registerkarte "Serverliste", und stellen Sie sicher, dass das Feld "Benutzergruppe" bei Verwendung von SSL mit dem URL-Alias des Verbindungsprofils übereinstimmt. Stellen Sie bei IKEv2 sicher, dass das Feld User Group (Benutzergruppe) mit dem genauen Namen des Verbindungsprofils übereinstimmt.

Server List Entry X
Primary Server Connection Information Display Name (required) FTD1-SSL Primary Protocol SSL FQDN or IP A User Group Add piteway Add Method During IKE Negotilition Group URL IKE Identity (IOS gateway only)
Backup Servers
Host Address Add

Bearbeiten des XML-Profils mit einem URL-Alias für SSL-Verbindungen.

Zertifikatszuordnung

Navigieren Sie zur Registerkarte Advanced (Erweitert) in der VPN-Richtlinie für den Remote-Zugriff. Wählen Sie je nach Präferenz eine allgemeine Einstellungsoption aus. Wählen Sie anschließend Zuordnung hinzufügen aus.

RAVPN Enter Description		Ye	a have unsaved changes Save Cancel
Connection Profile Access Inter	aces Advanced	Local Realm: None	Dynamic Access Policy: None
Secure Client Images ~ Secure Client Customization GUI Text and Messages loons and Images Scripts Binaries Custom Installer Transforms	General Settings for Connection Profile Mapping The divice processes the policies in the order lated below until it finds a match Use group URL if group URL and Centificate Map match different Connection Profile Use the configured rules to match centificate Mapping Client request is checked against each Centificate Map, asociated Connection Profile will be used when rules are m Please provide at least one Centificate Mapping.	tched. If none of the Certificate Map is matched, default connection profile will be chosen.	Add Mapping
Localized Installer Transforms	Certificate Map	Connection Profile	
Address Assignment Policy Certificate Maps		No Records Found	
Group Policies LDAP Attribute Mapping Load Balancing UPsec Crypto Maps			
IKE Policy IPsec/IKEv2 Parameters	Default Connection Profile: This Connection Profile will be applied when more of the Cortificate Map's code in matched.		•

Navigieren Sie zur Registerkarte Erweitert in der FMC-Benutzeroberfläche, um ein Zertifikatzuordnungsobjekt in der FMC-Benutzeroberfläche zu erstellen.

Geben Sie dem Zertifikatzuordnungsobjekt einen Namen, und wählen Sie Regel hinzufügen aus. Definieren Sie in dieser Regel die Eigenschaften des Zertifikats, das Sie identifizieren möchten, um den Benutzer einem bestimmten Verbindungsprofil zuzuordnen. Wählen Sie anschließend OK und anschließend Speichern.

Add Certificate Map				0		
Map N Cer Mapp Config	Name*: tificate-Map-CN ing Rule gure the certificate ma	atching rule			Add Rule	
#	Field	Component	Operator	Value		
1	Subject 🔻	CN (Common Name -	Equals 🔻	customval	ue	
	OK Cancel					
				Cance	Save	•

Erstellen Sie eine Zertifikatszuordnung, und fügen Sie Kriterien für die Zuordnung innerhalb der FMC-Benutzeroberfläche hinzu.

Wählen Sie aus dem Dropdown-Menü das Zertifikatzuordnungsobjekt und das Verbindungsprofil aus, dem die Zertifikatzuordnung zugeordnet werden soll. Wählen Sie dann OK aus.

Add Connection Profile to Certificate Map	
Choose a Certificate Map and associate Connection Profiles to selected Certficate Map.	
Certificate Map Name*:	
Certificate-Map-CN +	
Connection Profile*:	
LDAP-TG 🔹	
Cancel	

Verknüpfen Sie das Zertifikatzuordnungsobjekt mit der gewünschten Tunnelgruppe in der FMC-Benutzeroberfläche.

Vergewissern Sie sich, dass das Standardverbindungsprofil als DefaultWEBVPNGroup konfiguriert ist. Wenn ein Benutzer die Zuordnung nicht bekommt, wird er an DefaultWEBVPNGroup gesendet. Wählen Sie anschließend Speichern und verteilen Sie die Änderungen.



Ändern Sie das Standardverbindungsprofil für die Zertifikatszuordnung in die DefaultWEBVPNGroup innerhalb der FMC-Benutzeroberfläche.



Wählen Sie das gewünschte IPsec-IKEv2-Verbindungsprofil aus, und navigieren Sie zu Gruppenrichtlinie bearbeiten.

Edit Connection Profile		0	
Connection Profile:*	IKEV2		
Group Policy:*	IKEV2-IPSEC + idit Group Policy 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.			
Name	IP Address Range		
AnyConnect_Pool	10.50.50.1-10.50.50.6		
DHCD Soquere			
Name	DHCP Server IP Address	+	
	Cancel	ve 🗸	

Bearbeiten einer Gruppenrichtlinie in der FMC-Benutzeroberfläche

Navigieren Sie auf der Registerkarte General (Allgemein) zum Abschnitt VPN Protocols (VPN-Protokolle), und stellen Sie sicher, dass das Kontrollkästchen IPsec-IKEv2 aktiviert ist.

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 Psec-IKEv2

Aktivieren Sie IPsec-IKEv2 innerhalb einer Gruppenrichtlinie in der FMC-Benutzeroberfläche.

Navigieren Sie im VPN Profile Editor oder ASA Profile Editor zur Registerkarte Server List (Serverliste). Der Benutzername für die Benutzergruppe MUSS exakt mit dem Namen des Verbindungsprofils auf der Firewall übereinstimmen. In diesem Beispiel war IKEV2 der Name des Verbindungsprofils/der Benutzergruppe. Das primäre Protokoll wird als IPsec konfiguriert. Der Anzeigename in wird dem Benutzer in der Secure Client-Benutzeroberfläche angezeigt, wenn eine Verbindung mit diesem Verbindungsprofil hergestellt wird.

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 ftd1com / IKEV2 Group URL	Connection Information Primary Protocol IPsec ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only)		
Backup Servers Host Address	Add Move Up Move D		
	Delete		
OK Cancel			

Bearbeiten Sie das XML-Profil so, dass das primäre Protokoll IPsec ist und die Benutzergruppe mit dem Namen des Verbindungsprofils übereinstimmt.



Vorsicht: Eine SSL-Verbindung ist erforderlich, um XML-Profile von der Firewall an den Client zu übertragen. Wenn nur IKEV2-IPsec verwendet wird, müssen die XML-Profile über eine Out-of-Band-Methode an die Clients übertragen werden.

Sobald das XML-Profil an den Client übertragen wurde, verwendet der sichere Client die Benutzergruppe aus dem XML-Profil, um eine Verbindung mit dem IKEV2-IPsec-Verbindungsprofil herzustellen.

🕱 Cisco Secur	e Client	_		×
	AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC	~	Connect	_
Cisco Se	cure Client FTD1-IPSEC		×	-drafte cisco
Usi Pa:	ername: nroche ssword:			
	OK	Cano	al	

Sichere Client-UI-Ansicht des IPsec-IKEv2 RAVPN-Verbindungsversuchs.

ASA-Konfigurationsbeispiele

Deaktivieren Sie die AAA-Authentifizierung in den Verbindungsprofilen DefaultWEBVPNGroup und DefaultRAGroup.

Geben Sie den Abschnitt "webvpn-attribute" für die Tunnelgruppe "DefaultWEBVPNGroup" ein, und geben Sie die Authentifizierung als zertifikatbasiert an. Wiederholen Sie diesen Vorgang für die DefaultRAGroup. Benutzer, die auf diesen Standard-Verbindungsprofilen landen, müssen ein Zertifikat für die Authentifizierung vorlegen. Sie erhalten keine Möglichkeit, Benutzernamen und Kennwörter einzugeben. Deaktivieren Sie Hostscan/Secure Firewall Posture auf der DefaultWEBVPNGroup und DefaultRAGroup (optional).

Dies ist nur erforderlich, wenn Sie Hostscan/Secure Firewall Posture in Ihrer Umgebung haben. Dieser Schritt verhindert, dass Angreifer die durch den Endpunkt-Scanvorgang verursachte Ressourcennutzung auf der Firewall erhöhen. Öffnen Sie den Abschnitt "webvpn-attribute" für die DefaultWEBVPNGroup- und DefaultRAGroup- sowie die Verbindungsprofile, und implementieren Sie without-csd, um die Funktion zum Scannen von Endpunkten zu deaktivieren.

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

Gruppenaliase deaktivieren und Gruppen-URLs aktivieren

Geben Sie die Tunnelgruppe(n) ein, mit der Benutzer eine Verbindung herstellen. Wenn bereits ein Gruppenalias vorhanden ist, deaktivieren oder entfernen Sie ihn. In diesem Beispiel ist sie deaktiviert. Erstellen Sie anschließend eine Gruppen-URL, die den FQDN oder die IP-Adresse der RAVPN-Terminierungsschnittstelle verwendet. Der Name am Ende der Gruppen-URL muss unklar sein. Vermeiden Sie gängige Werte wie VPN, AAA, RADIUS oder LDAP, da diese es Angreifern erleichtern, die vollständige URL zu erraten, wenn sie den FQDN erhalten. Verwenden Sie stattdessen intern relevante Namen, mit denen Sie die Tunnelgruppe identifizieren können.

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

Zertifikatszuordnung

Erstellen Sie im globalen Konfigurationsmodus eine Zertifikatszuordnung, und weisen Sie ihr einen Namen und eine Sequenznummer zu. Definieren Sie dann eine Regel, die die Benutzer zur Verwendung der Zuordnung abgleichen müssen. In diesem Beispiel müssen Benutzer die Kriterien eines gemeinsamen Namenswerts erfüllen, der "customvalue" entspricht. Geben Sie dann die WebVPN-Konfiguration ein, und wenden Sie die Zertifikatszuordnung auf die gewünschte Tunnelgruppe an. Geben Sie nach Abschluss des Vorgangs die DefaultWEBVPNGroup (Standard-WEBVPN-Gruppe) ein, und legen Sie diese Tunnelgruppe als Standard für Benutzer fest, die die Zertifikatszuordnung nicht erfüllen. Wenn die Zuordnung für Benutzer fehlschlägt, werden sie an die DefaultWEBVPNGroup weitergeleitet. Während die DefaultWEBVPNGroup mit Zertifikatsauthentifizierung konfiguriert ist, haben Benutzer keine Möglichkeit, Benutzernamen oder Kennwörter weiterzugeben.

```
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

Im globalen Konfigurationsmodus können Sie eine vorhandene Gruppenrichtlinie bearbeiten oder eine neue erstellen und die Attribute für diese Gruppenrichtlinie eingeben. Aktivieren Sie IKEv2 im Attributabschnitt als einziges VPN-Tunnelprotokoll. Stellen Sie sicher, dass diese Gruppenrichtlinie mit einer Tunnelgruppe verknüpft ist, die für IPsec-IKEV2-VPN-Verbindungen für den Remotezugriff verwendet wird. Ähnlich wie bei den FMC-Schritten müssen Sie das XML-Profil über den VPN Profile Editor oder den ASA Profile Editor bearbeiten und das Feld User Group so ändern, dass es mit dem Namen der Tunnelgruppe auf der ASA übereinstimmt, und das Protokoll in IPsec ändern.

```
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
```

Navigieren Sie im VPN Profile Editor oder ASA Profile Editor zur Registerkarte Server List (Serverliste). Der Benutzername für die Benutzergruppe MUSS exakt mit dem Namen des Verbindungsprofils auf der Firewall übereinstimmen. Das primäre Protokoll wird als IPsec konfiguriert. Der Anzeigename wird dem Benutzer in der Secure Client-Benutzeroberfläche angezeigt, wenn eine Verbindung mit diesem Verbindungsprofil hergestellt wird.

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

Bearbeiten Sie das XML-Profil so, dass der primäre Protokollname IPsec lautet und der Benutzername mit dem Tunnelgruppennamen der ASA für IPsec-IKEv2-RAVPN-Verbindungen übereinstimmt.



Vorsicht: Eine SSL-Verbindung ist erforderlich, um XML-Profile von der Firewall an den Client zu übertragen. Wenn nur IKEV2-IPsec verwendet wird, müssen die XML-Profile über eine Out-of-Band-Methode an die Clients übertragen werden.

Schlussfolgerung

Zusammenfassend besteht der Zweck der Härtungspraktiken in diesem Dokument darin, legitime Benutzer benutzerdefinierten Verbindungsprofilen zuzuordnen, während Angreifer zur DefaultWEBVPNGroup und zur DefaultRAGroup gezwungen werden. In einer optimierten Konfiguration verfügen die beiden Standardverbindungsprofile über keine benutzerdefinierte AAA-Serverkonfiguration. Darüber hinaus wird durch das Entfernen von Gruppen-Aliasen verhindert, dass Angreifer auf einfache Weise benutzerdefinierte Verbindungsprofile identifizieren können, indem sie die Dropdown-Sichtbarkeit beim Navigieren zum FQDN oder zur öffentlichen IP-Adresse der Firewall entfernen.

Zugehörige Informationen

Technischer Support und Downloads von Cisco

- Angriffe durch Passwortverbreitung
- Sicherheitslücke bei nicht autorisiertem Zugriff September 2023
- ASA-Konfigurationsanleitungen
- FMC-/FDM-Konfigurationsanleitungen

Informationen zu dieser Übersetzung

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