セキュアクライアントAnyConnect VPNの強化対 策の実装

内容

<u>はじめに</u>

<u>前提条件</u>

要件

<u>使用するコンポーネント</u>

<u>背景説明</u>

コンセプト

<u>Cisco Secure Firewallでのクライアントのセキュリティ強化策:</u>

<u>ロギングとsyslog IDを使用した攻撃の特定</u>

<u>攻撃の検証</u>

<u>FMCの設定例</u>

DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無効化

<u>DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイアウォールポス</u> <u>チャを無効にする(オプション)</u>

グループエイリアスの無効化とグループURLの有効化

<u>証明書マッピング</u>

IPsec-IKEv2

<u>ASAの設定例</u>

<u>DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無効化</u>

<u>DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイアウォールポス</u> チャを無効にする(オプション)

<u>グループエイリアスの無効化とグループURLの有効化</u>

<u>証明書マッピング</u>

IPsec-IKEv2

<u>結論</u>

<u>関連情報</u>

はじめに

このドキュメントでは、リモートアクセスVPN実装のセキュリティを向上させる方法について説 明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Client AnyConnect VPN』を参照してください。
- ASA/FTDリモートアクセス設定。

使用するコンポーネント

ベストプラクティスガイドは、次のハードウェアとソフトウェアのバージョンに基づいています 。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。



注意:このドキュメントには、Firepowerデバイスマネージャ(FDM)の手順は含まれてい ません。FDMは、DefaultWEBVPNGroupの認証方式の変更のみをサポートします。コン トロールプレーンACL、またはFDM UIのリモートアクセスVPNの「グローバル設定」セ クションのカスタムポートを使用してください。必要に応じて、Cisco Technical Assistance Center(TAC)に連絡し、サポートを依頼してください。

背景説明

このドキュメントの目的は、Cisco Secure Client AnyConnect VPNの設定が、サイバーセキュリ ティ攻撃が一般的に見られる現代の世界におけるセキュリティのベストプラクティスに準拠して いることを確認することです。

総当たり攻撃では通常、ユーザ名とパスワードの組み合わせを使用してリソースへのアクセスを 繰り返し試みます。攻撃者は、インターネットブラウザ、セキュアクライアントユーザインター フェイス、またはその他のツールを使用して、複数のユーザ名とパスワードを入力し、それらが AAAデータベース内の正当な組み合わせと一致することを望んでいます。認証にAAAを使用する 場合、接続を確立するために必要であるため、エンドユーザはユーザ名とパスワードを入力する 必要があります。同時に、ユーザがクレデンシャルを入力するまで、ユーザを確認しません。本 質的に、これにより攻撃者は次のシナリオを利用できます。

- 1. Cisco Secure Firewallの公開された完全修飾ドメイン名(特に接続プロファイルでグ ループエイリアスを使用する場合):
 - 攻撃者がVPNファイアウォールのFQDNを検出した場合、ブルートフォースアタックを開始するグループエイリアスを使用してトンネルグループを選択するオプションがあります。
- 2. AAAまたはローカルデータベースで設定されたデフォルト接続プロファイル:
 - ○攻撃者は、VPNファイアウォールのFQDNを見つけると、AAAサーバまたはロー カルデータベースに対してブルートフォースアタックを試みることができます。 これは、グループエイリアスが指定されていない場合でも、FQDNへの接続がデ フォルト接続プロファイルに到達するために発生します。

3. ファイアウォールまたはAAAサーバでのリソース枯渇:

攻撃者は、大量の認証要求を送信し、Denial of Service(DoS;サービス拒否)状態を発生させることで、AAAサーバまたはファイアウォールリソースに過大な負荷を与える可能性があります。

コンセプト

グループエイリアス:

 ファイアウォールが接続プロファイルを参照するための代替名。ファイアウォールへの接続 を開始した後、ユーザが選択できるように、これらの名前がセキュアクライアントUIのドロ ップダウンメニューに表示されます。group-aliasesを削除すると、セキュアクライアント UIのドロップダウン機能が削除されます。 グループURL:

 着信接続が目的の接続プロファイルに直接マッピングされるように、接続プロファイルに関 連付けることができるURL。ユーザがセキュアクライアントUIで完全なURLを入力するか、 XMLプロファイルでURLを「表示名」と統合してユーザにURLを表示しないようにできるた め、ドロップダウン機能はありません。

ここで異なるのは、グループエイリアスを実装する場合、ユーザが接続 to vpn_gateway.example.comを開始し、エイリアスを表示して接続プロファイルへのドライブを 選択する点です。グループURLを使用すると、ユーザは

vpn_gateway.example.com/example_groupへの接続を開始し、ドロップダウンメニューの必要や オプションなしで接続プロファイルに直接接続できます。

Cisco Secure Firewallでのクライアントのセキュリティ強化策:

これらの方式は、正当なユーザを適切なトンネルグループや接続プロファイルにマッピングする 一方で、悪意のある可能性のあるユーザをトラップトンネルグループに送信します。このトラッ プトンネルグループは、ユーザ名とパスワードの組み合わせを許可しないように設定されていま す。すべての組み合わせを実装する必要はありませんが、グループエイリアスを無効にし、 DefaultWEBVPNGroupおよびDefaultRAGroupの認証方式を変更することで、推奨事項が効果的 に機能するようになります。

- 接続プロファイル設定でグループエイリアスを無効にしてグループURLのみを使用すると、 適切なFQDNを持つクライアントだけが接続を開始できるため、攻撃者が簡単に検出して選 択することのない特定のFQDNを使用できます。たとえば、 vpn_gateway.example.com/example_groupはvpn_gateway.example.comよりも攻撃者にと って発見が困難です。
- DefaultWEBVPNGroupおよびDefaultRAGroupでAAA認証を無効にし、証明書認証を設定します。これにより、ローカルデータベースまたはAAAサーバに対するブルートフォースを回避できます。このシナリオの攻撃者は、接続試行時に即時エラーを表示されます。認証は証明書に基づいているため、ユーザ名またはパスワードのフィールドはありません。そのため、総当たり攻撃は停止されます。もう1つのオプションは、悪意のある要求のシンクホールを作成するためのサポート設定のないAAAサーバを作成することです。
- 接続プロファイルに証明書マッピングを使用します。これにより、クライアントデバイス上の証明書から受信した属性に基づいて、着信接続を特定の接続プロファイルにマッピングできます。適切な証明書を持つユーザは正しくマッピングされますが、マッピング基準に失敗した攻撃者はDefaultWEBVPNGroupに送信されます。
- SSLの代わりにIKEv2-IPSecを使用すると、トンネルグループはXMLプロファイル内の特定 のユーザグループマッピングに依存します。エンドユーザマシンにこのXMLがないと、ユー ザはデフォルトのトンネルグループに自動的に送信されます。



注:グループエイリアス機能の詳細については、『<u>ASA VPNコンフィギュレーションガ</u> <u>イド</u>』と『表1』を参照してください。SSL VPNの接続プロファイル属性』を参照してく ださい。

ロギングとsyslog IDを使用した攻撃の特定

総当たり攻撃は、リモートアクセスVPNを侵害する主要な方法であり、脆弱なパスワードを悪用 して不正なエントリを取得します。ロギングの利用とsyslogの評価によって攻撃の兆候を認識す る方法を知ることは非常に重要です。異常なボリュームに遭遇した場合に攻撃を示す可能性があ る一般的なsyslog IDは次のとおりです。

%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

ユーザ名は、ASAでno logging hide usernameコマンドが設定されるまで、常に非表示になります。



注:有効なユーザが生成されたか、または悪意のあるIPによって認識された場合、これは 情報を提供しますが、ユーザ名がログに表示されるので注意してください。

Cisco ASAロギング:

<u>Secure ASA Firewallユーザガイド</u>

『Cisco Secure Firewall ASAシリーズCLIコンフィギュレーションガイド』の「<u>ロギング</u>」の章

Cisco FTDロギング:

<u>FMC を介して FTD にロギングを設定</u>

『Cisco Secure Firewall Management Center Device Configuration Guide』の「Platform Settings」の章の「<u>Configure Syslog</u>」の項 <u>Firepower Device Manager(FDM)でのsyslogの設定と確認</u>

『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「 System Settings」の章の「<u>Configuring System Logging Settings</u>」の項

攻撃の検証

これを確認するには、ASAまたはFTDのコマンドラインインターフェイス(CLI)にログインして show aaa-serverコマンドを実行し、設定されたAAAサーバのいずれかに対して試行された認証要 求と拒否された認証要求の数が異常でないかどうかを調べます。

<#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 Number of bad authenticators 0 Number of timeouts 1 Number of unrecognized responses 0

FMCの設定例

DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無 効化

Devices > Remote Accessの順に移動します。

	F irewall Mar Overview / Dashb	agement Center oards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration	
Sumr Provides a Netwo	mary Dash summary of activity of prk Threats	board (<u>switch dashboard)</u> on the appliance in Intrusion Events	Status	Geolocation	QoS	Device M NAT QoS Platform FlexCon	Management Settings fig	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture
▶ Тор	Zero Trust Appl	ications			- ×	Certifica	tes		Upgrade Threat Defense Upgrade Chassis Upgrade

が、リモートアクセスVPNポリシー設定に移動するためにFMC GUIをナビゲートしていることを示します。

既存のリモートアクセスVPNポリシーを編集し、「DefaultRAGroup」という名前の接続プロファ イルを作成します。

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 📀	° 0	admin ~	ninde SECURE
												Add
Namo				Status			Last Modified					
RAVPN				Targeting 1 Up-to-date	devices on all targeted		2024-03-07 10:58:20 Modified by "admin"			ę.	/i	

FMC UIでリモートアクセスVPNポリシーを編集する方法を表示します。

「DefaultWEBVPNGroup」および「DefaultRAGroup」という名前の接続プロファイルを編集します。

Firewall Ma Devices / VPN	anagement Center / Edit Connection Profile	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	م	۲	¢ 0	admin ~	isco SECURE
RAVPN														Save Cancel
Enter Description													Policy	y Assignments (1)
Occurrent on Deaths	• •••								Local Realm: LOCAL	REALN			Dynamic Ace	cess Policy: None
Connection Profile	Access interfaces Adv	anced												
Name				***				Group Policy						
DefaultWEBVPNGroup					LOCAL None None			DfltGrpPolicy						

FMC UI内でDefaultWEBVPNGroupを編集する方法を表示します。

AAAタブに移動し、Authentication Methodドロップダウンを選択します。Client Certificate Onlyを選択し、Saveを選択します。

Edit Connection Profile		
Connection Profile:*	DefaultWEBVPNGroup	
Group Policy:*	DfltGrpPolicy +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method:	Client Certificate Only -	
٩	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	e

FMC UI内のDefaultWEBVPNGroupに対してのみ、認証方式をクライアント証明書に変更します。

DefaultRAGroupを編集し、AAAタブに移動して、Authentication Methodドロップダウンを選択します。'Client Certificate Only'を選択し、Saveを選択します。

Edit Connection Profile		
Connection Profile:*	DefaultRAGroup	
Group Policy:*	DfltGrpPolicy +	
E		
Authentication		
Authentication Method:	Client Certificate Only -	
l I	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	/e

FMC UI内のDefaultRAGroupに対してだけ、認証方式をクライアント証明書に変更します。



注:認証方式は、シンクホールAAAサーバにすることもできます。この方法を使用する と、AAAサーバの設定が誤って設定され、実際には要求が処理されません。変更を保存 するには、「Client Address Assignment」タブでVPNプールを定義する必要もあります 。

DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイア ウォールポスチャを無効にする(オプション)

これは、環境内にホストスキャン/セキュアファイアウォールポスチャがある場合にのみ必要です 。このステップにより、攻撃者はエンドポイントスキャンプロセスによってファイアウォールの リソース使用率を上げることができなくなります。FMCでこれを実現するには、without-csdコマ ンドを使用してFlexConfigオブジェクトを作成し、エンドポイントスキャン機能を無効にします 。

Objects > Object Management > FlexConfig Object > Add FlexConfig Objectの順に移動します。

Cipiects / Object Management	nt Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧳 🌣 g admin 🗸	disco SECURE
> AAA Server > Access List > Address Pools Application Filters	FlexConfig Object PlexConfig Object actude device configuration commands, variables, and scripting language instructions. It is used in PlexConfig polices.	Add FlexConfig Object Q, Filter	
AS Path	Name	Description	
BFD Template Cipher Suite List	Anyconnect_route_Mering		9/7 [*]
> 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.	¶a Q ⊕
> Distinguished Name DNS Server Group	Default_Inspection_Protocol_Enable	Enable Default Inspection.	¶∎ Q 🗑
> External Attributes	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recip	¶aq ⊕
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 ⊂ ≣
Text Object	DNS_UnConfigure	Remove the DNS configurations.	¶aq
Geolocation	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-su	¶_q =
Key Chain	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authent	¶a Q ⊒
Network	Elgrp_UnConfigure	Clears eigrp configuration for an AS	5 α ⊒

FMC UIでFlexConfigオブジェクトを作成する。

FlexConfigオブジェクトに名前を付け、タイプがAppendのデプロイメントをEverytimeに設定し ます。次に、表示されたとおりに構文を入力し、オブジェクトを保存します。

Edit FlexConfig Object						Ø
Name: Wtihout-CSD Description: Copy-pasting any rich text might int	roduce line breaks w	ile generating CLI. Pleas	e verify the	CLI before deployr	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 (Ty	perty pe:Name)	Override	Description	
		No records to display				
					Cancel	Save

Devices > FlexConfigの順に移動し、PencilをクリックしてFlexConfigポリシーを編集します。

^{&#}x27;without-csd'でFlexConfigオブジェクトを作成しています

þ	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	° 0	0	admin \vee	-dude SECURE
														New Policy
	FlexConfig Policy					Status		Last Modified						
	Flox-Test					Targeting 1 Out-of-dat	devices on 1 targeted devices	2024-04-10 21:54:19 Modified by "admin"						9 🖊 î

FMC内でFlexConfigポリシーを編集します。

「ユーザー定義」セクションで作成したオブジェクトを検索します。次に、矢印を選択して、 Selected Append FlexConfigsに追加します。最後に、Saveを選択してFlexConfigポリシーを保存 します。

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🥩 🔅 🛛 admin 🗸 👘 secure
FlexConfig							You have unaxwed changes Migrate Config Preview Config Save Cancel
Enter Description							Policy Assignments (1)
	" Select	ed Prepend F	lexConfigs				
Available FlexConfig C FlexConfig Object	# Na	me			Description		
V User Defined							
"? Anyconnect_route_filtering							
"? No_Keepout							
"∄ Without-CSD ✓ System Defined							
"? Default_DNS_Configure							
Default_Inspection_Protocol_Disable							
"] Default_Inspection_Protocol_Enable	Select	ed Append F	lexConfigs				
** DHCPv6_Prefix_Delegation_Configure	I Na	ime			Description		
.] DHCPv6_Prefix_Delegation_UnConfigure	1 W1	ihout-CSD					93
DNS_Configure							~•
*7 Eloro Configure							
"2 Egrp_Interface_Configure							

FlexConfigオブジェクトをFlexConfigポリシーにアタッチします。

Policy Assignmentsを選択して、このFlexConfigポリシーを適用するFTDを選択してから、OKを 選択します。これが新しいFlexConfigの割り当てである場合は、再度Saveを選択して、変更を適 用します。導入後の検証

Firewall Management Center Devices / Flexconfig Policy Editor	Overview Ar	nalysis Policies	Devices Obj	jects Integration			Deploy Q 🧬 🌣 😡	admin ~ dudo SECURE
FlexConfig Enter Description								Config Swe Cancel
Available FlexConfig C FlexConfig Object	" Selected Pr	epend FlexConfigs	Descrip	otion				POICY Assignments (1)
Viser Defined Nerconnect_route_filtering Necepout Ne_Keepout Ne_Keepout Ne_Keepout Ne_Keepout Ne_Keepout Otherwork SD System Defined Default_DNS_Configure J Default_Inspection_Protocol_Disable		Targeted Device Select devices to Available Devices Q. Search by na	s which you want to ap me or value	Add to Policy	•			
Default_Inspection_Protocot_Enable DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure DNS_Configure Egrp_Configure Egrp_Configure Egrp_Interface_Configure Egrp_Interface_Configure	Selected Ap	2				Cancel		Q. 🗑

FlexConfigポリシーをFirePOWERデバイスに割り当てます。

FTD CLIに入り、DefaultWEBVPNGroupおよびDefaultRAGroupに対してshow run tunnel-groupコマンドを発行します。without-csdが設定に含まれていることを確認します。

<#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

グループエイリアスの無効化とグループURLの有効化

接続プロファイルに移動し、「エイリアス」タブを選択します。グループエイリアスを無効また

は削除し、プラス(+)アイコンをクリックしてURLエイリアスを追加します。

Edit Connection Profile		
Connection Profile:* LDAP-TG		
Group Policy:* DfltGrpPolicy	• +	
Edit Group Policy		
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 content of the second	on web access. If users onnection profile.	choose the
URL	Status	

FMCのUIでトンネルグループのgroup-aliasオプションを無効にする

URLエイリアスのオブジェクト名を設定し、URLのファイアウォールのFQDNまたはIPアドレス を入力し、続いて接続プロファイルを関連付ける名前を入力します。この例では、「aaaldap」を 選択します。FQDNを取得した攻撃者が完全なURLを推測する可能性が低いため、不明瞭なほど 、安全性が高くなります。終了したら、Saveを選択します。

Edit URL Objects		9
Name LDAP-ALIAS		
Description		
URL https://ftd1	.com/aaalda	
Allow Overrides		
	Cancel	Save

FMC UI内でのURLエイリアスオブジェクトの作成

ドロップダウンからURLエイリアスを選択し、Enabledボックスにチェックマークを入れて、 OKを選択します。



URLエイリアスがFMC UI内で有効になっていることを確認します。

group-aliasが削除されているか無効になっているかを確認し、URL Aliasが有効になっていること を確認して、Saveを選択します。

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. Ali on this device can be turned on or off for display.	ases from all connections confi	igured +
Name	Status	
LDAP	Disabled ,	7
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 🖉	T
	Cancel	Save

FMCのUIでトンネルグループのURLエイリアスオプションを有効にする

必要に応じて、URLエイリアスをXMLの一部としてプッシュすることもできます。これは、 VPNプロファイルエディタまたはASAプロファイルエディタを使用してXMLを編集することで実 現されます。これを行うには、Server Listタブに移動し、SSLを使用する場合はUser Groupフィ ールドが接続プロファイルのURLエイリアスと一致することを確認します。IKEv2では、User Groupフィールドが接続プロファイルの正確な名前と一致することを確認します。

Edt Det		
	Server List Entry Server List Entry	×
	Primary Server Corrise Display Name (required) FIDI-SSL Prim FIDI-SSL FQDN or IP A User Group ftd1 com Group URL IR ftd1 com/asaldap	ction Information any Protocol SSL ··································
	Badup Servers Host Address	Add Move Ub Move D Delete
	OK Cancel	

SSL接続用のURLエイリアスを持つようにXMLプロファイルを編集します。

証明書マッピング

リモートアクセスVPNポリシー内のAdvancedタブに移動します。基本設定に基づいて一般設定オ プションを選択します。選択したら、Add Mappingを選択します。

RAVPN	You have unneved by	inges Save	Cancel
Enter Description			
		Policy Assignr	ments (1)
	Local Realm: None Dr	namic Access Poli	icy: None
Connection Profile Access Inter	Hrisos 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 inf group URL and Certificate Map in Consistion Profiles		
Icons and Images	Vuse the configured rules to match a certificate to a Connection Protee		
Scripts	Certificate to Connection Profile Mapping Client results is checked seased such clients Man seasched Connection Profile will be used when rules are matched. If none of the Certificate Man is matched default connection profile will be chosen		
Binaries	Please provide at least one Certificate Mapping.	Add M	anning
Custom Installer Transforms			opping
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	Datas Casarda - Datas		_
IPsec/IKEv2 Parameters	United Defendent Poths will be applied when none of the Certificate May's rade in matched,		· .

FMC UI内でAdvancedタブに移動して、FMC UI内に証明書マップオブジェクトを作成します。

証明書マップオブジェクトに名前を付け、Add Ruleを選択します。このルールでは、ユーザを特定の接続プロファイルにマッピングするために識別する証明書のプロパティを定義します。終了したら、OKを選択してからSaveを選択します。

Add	Certificate Map					0
Map Ce Mapı Conf	Name*: rtificate-Map-CN ping Rule igure the certificate ma	atching rule			Add Ruk	e
#	Field	Component	Operator	Value		
1	Subject •	CN (Common Name -	Equals 🔻	customval	ue	
	OK Cancel					
				Cance	el Sa	ve

証明書マップを作成し、FMCのUIでマップの基準を追加します。

ドロップダウンから、証明書マップオブジェクトと、証明書マップを関連付ける接続プロファイ ルを選択します。次にOKを選択します。

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 OK

証明書マップオブジェクトをFMC UI内の目的のトンネルグループに関連付けます。

ユーザがマッピングに失敗するとDefaultWEBVPNGroupに送信されるように、デフォルト接続プ ロファイルがDefaultWEBVPNGroupとして設定されていることを確認します。完了したら、 Saveを選択して、変更を適用します。

RAVPN Enter Description Connection Profile Access Inter	faces Advanced	Yeu Ia Local Realm: None	ne unsaved changes Save Cancel Policy Assignments.(1) Dynamic Access Policy: None
Secure Client Images Secure Client Customization GUI Text and Messages Icons and Images Scripts Binaries Custom Installer Transforms	General Settings for Connection Profile Mapping The device processes the policies in the order lated below until it finds a match Use group URL if group URL and Certificate Map match different Connection Profiles Set Use the configured rules to match a certificate to a Connection Profile Certificate to Connection Profile Mapping Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are match Certificate to Connection Profile Certificate Map, associated Connection Profile will be used when rules are matched Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched Certificate Connection Profile Mapping	sched. If none of the Certificate Map is matched, default connection profile will be chosen.	Add Mepping
Localized Installer Transforms	Certificate Map	Connection Profile	
Address Assignment Policy	Certificate-Map-CN	LDAP-TG	/1
Certificate Maps Group Policies LDAP Attribute Mapping Load Balancing > IPsec Crypto Maps IKE Policy			
IPsec/IKEv2 Parameters	Default Connection Profile: This Connection Profile will be applied when none of the Contheate Map's rule is matched.		DefaultWEBVPNGroup

証明書マッピングのデフォルト接続プロファイルをFMC UI内のDefaultWEBVPNGroupに変更します。

IPsec-IKEv2

目的のIPsec-IKEv2接続プロファイルを選択し、Edit Group Policyに移動します。

Edit Connection Profile	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	
	Cancel	Save

FMC UI内でグループポリシーを編集します。

Generalタブで、VPN Protocolsセクションに移動し、IPsec-IKEv2ボックスにチェックマークが付いていることを確認します。

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

FMC UIのグループポリシー内でIPsec-IKEv2を有効にします。

VPNプロファイルエディタまたはASAプロファイルエディタで、Server Listタブに移動します。 ユーザグループ名は、ファイアウォール上の接続プロファイル名と完全に一致している必要があ ります。この例では、IKEV2は接続プロファイル/ユーザグループ名です。プライマリプロトコル がIPsecとして設定されている。の「表示名」は、この接続プロファイルへの接続を確立するとき に、セキュアクライアントUIでユーザに表示されます。

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certific	ate Pinning
Primary Server Display Name (required) FTD1-IPSEC FQDN or IP A ftd1com / 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
ОК	Cancel

プライマリプロトコルがIPsecで、ユーザグループが接続プロファイル名と一致するようにXMLプロファイルを編集します。



注意:ファイアウォールからクライアントにXMLプロファイルをプッシュするには、 SSL接続が必要です。IKEV2-IPsecのみを使用している場合、XMLプロファイルはアウト オブバンド方式でクライアントにプッシュする必要があります。

XMLプロファイルをクライアントにプッシュすると、セキュアクライアントはXMLプロファイル のユーザグループを使用して、IKEV2-IPsec接続プロファイルに接続します。

🕱 Cisco Secur	re Client	_		×
	AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC		Connect	_
Cisco Se	ecure Client FTD1-IPSEC		×	-dhalla cisco
Us Pa	ername: nroche ssword:			
			_	

IPsec-IKEv2 RAVPN接続のセキュアクライアントUIビュー。

ASAの設定例

DefaultWEBVPNGroupおよびDefaultRAGroup接続プロファイルでのAAA認証の無効化

tunnel-group DefaultWEBVPNGroupにwebvpn-attributesセクションを入力し、証明書ベースとし て認証を指定します。DefaultRAGroupに対してこのプロセスを繰り返します。これらのデフォル トの接続プロファイルを使用するユーザは、認証用の証明書を提示することを強制され、ユーザ 名とパスワードのクレデンシャルを入力する機会は与えられません。

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# authentication certificate DefaultWEBVPNGroupおよびDefaultRAGroupでホストスキャン/セキュアファイア ウォールポスチャを無効にする(オプション)

これは、環境内にホストスキャン/セキュアファイアウォールポスチャがある場合にのみ必要です 。このステップにより、攻撃者はエンドポイントスキャンプロセスによってファイアウォールの リソース使用率を上げることができなくなります。DefaultWEBVPNGroup、DefaultRAGroup、 および接続プロファイルのwebvpn-attributesセクションに入り、without-csdを実装して、エンド ポイントスキャン機能を無効にします。

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

グループエイリアスの無効化とグループURLの有効化

ユーザが接続するトンネルグループを入力します。既存のグループエイリアスがある場合は、無 効にするか、削除します。この例では無効になっています。これが完了したら、RAVPN終端イン ターフェイスのFQDNまたはIPアドレスを使用してグループURLを作成します。グループURLの 末尾の名前は分かりにくい必要があります。VPN、AAA、RADIUS、LDAPなどの一般的な値は、 攻撃者がFQDNを取得する際に完全なURLを推測しやすくなるため、使用しないでください。代 わりに、トンネルグループの識別に役立つ内部的に有意な名前を使用します。

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

証明書マッピング

グローバルコンフィギュレーションモードで、証明書マップを作成し、名前とシーケンス番号を 割り当てます。次に、マッピングを利用するためにユーザが照合する必要があるルールを定義し ます。この例では、ユーザは「customvalue」と等しい共通名の値の基準に一致する必要があり ます。次に、webvpn設定を入力し、目的のトンネルグループに証明書マップを適用します。完了 したら、DefaultWEBVPNGroupを入力し、証明書マッピングに失敗したユーザのデフォルトをこ のトンネルグループにします。ユーザがマッピングに失敗すると、DefaultWEBVPNGroupにリダ イレクトされます。DefaultWEBVPNGroupに証明書認証が設定されている場合、ユーザはユーザ 名またはパスワードのクレデンシャルを渡すオプションを使用できません。

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

グローバルコンフィギュレーションモードから、既存のグループポリシーを編集したり、新しい グループポリシーを作成して、そのグループポリシーの属性を入力したりできます。属性セクシ ョンに移動したら、IKEv2を唯一のVPNトンネルプロトコルとして有効にします。このグループ ポリシーが、IPsec-IKEV2リモートアクセスVPN接続に使用されるトンネルグループに関連付け られていることを確認します。FMCの手順と同様に、VPNプロファイルエディタまたはASAプロ ファイルエディタを使用してXMLプロファイルを編集し、User GroupフィールドをASAのトンネ ルグループの名前に一致するように変更し、プロトコルをIPsecに変更する必要があります。

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

VPNプロファイルエディタまたはASAプロファイルエディタで、Server Listタブに移動します。 ユーザグループ名は、ファイアウォール上の接続プロファイル名と完全に一致している必要があ ります。プライマリプロトコルがIPsecとして設定されている。表示名は、この接続プロファイル への接続を確立するときに、セキュアクライアントUIでユーザに表示されます。

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certific	ate Pinning
Primary Server Display Name (required) ASA-IPsec FQDN or IP A User Group FQDN Group URL FQDN/TG-NAME	Connection Information Primary Protocol IPsec
Backup Servers Host Address	Add Move Up Move D Delete
ОК	Cancel

プライマリプロトコル名がIPsecで、ユーザグループ名がIPsec-IKEv2 RAVPN接続用ASAのトンネルグループ名と一致するように、XMLプロファイルを編集します。



注意:ファイアウォールからクライアントにXMLプロファイルをプッシュするには、 SSL接続が必要です。IKEV2-IPsecのみを使用している場合、XMLプロファイルはアウト オブバンド方式でクライアントにプッシュする必要があります。

結論

要約すると、このドキュメントの強化策の目的は、攻撃者がDefaultWEBVPNGroupと DefaultRAGroupに強制されている間に、正当なユーザをカスタム接続プロファイルにマッピング することです。最適化された設定では、2つのデフォルトの接続プロファイルに正規のカスタム AAAサーバ設定はありません。また、グループエイリアスを削除すると、ファイアウォールの FQDNまたはパブリックIPアドレスに移動するときにドロップダウンの表示が削除されるため、 攻撃者がカスタム接続プロファイルを簡単に識別できなくなります。

関連情報

<u>シスコテクニカルサポートとダウンロード</u>

<u>パスワードスプレー攻撃</u>

<u> 不正アクセスの脆弱性2023年9月</u>

<u>ASA設定ガイド</u>

<u>FMC/FDM構成ガイド</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。