实施安全客户端AnyConnect VPN的强化措施

目录	
<u>简介</u>	
<u>先决条件</u>	
<u>要求</u>	
<u>使用的组件</u>	
<u>背景信息</u>	
<u>概念</u>	
<u>思科安全防火墙</u>	的安全客户端强化实践:
使用日志记录和	<u>ISyslog ID识别攻击</u>
<u>攻击验证</u>	
<u>FMC配置示例</u>	
<u>禁用DefaultW</u>	EBVPNGroup和DefaultRAGroup连接配置文件中的AAA身份验证
<u>在DefaultWEE</u>	WPNGroup和DefaultRAGroup上禁用Hostscan/安全防火墙状态(可选)
<u>禁用Group-alia</u>	ases并启用Group-URL
<u>证书映射</u>	
IPsec-IKEv2	
<u>ASA配置示例</u>	
<u>禁用DefaultW</u>	EBVPNGroup和DefaultRAGroup连接配置文件中的AAA身份验证
<u>在DefaultWEE</u>	WPNGroup和DefaultRAGroup上禁用Hostscan/安全防火墙状态(可选)
<u>禁用Group-alia</u>	ases并启用Group-URL
<u>证书映射</u>	
IPsec-IKEv2	
<u>结论</u>	
<u>相关信息</u>	

简介

本文档介绍如何提高远程访问VPN实施的安全性。

先决条件

要求

思科建议您了解以下主题:

- 思科安全客户端AnyConnect VPN。
- ASA/FTD远程访问配置。

使用的组件

最佳实践指南基于以下硬件和软件版本:

- 思科ASA 9.x
- Firepower威胁防御7.x/FMC 7.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。



注意:本文档不包含Firepower设备管理器(FDM)的步骤。FDM仅支持更改 DefaultWEBVPNGroup上的身份验证方法。请在FDM UI中的远程访问VPN"全局设置 "(Global Settings)部分中使用控制平面ACL或自定义端口。如果需要,请与思科技术支持中 心(TAC)联系以获取进一步帮助。

背景信息

本文档的目的是确保Cisco安全客户端AnyConnect VPN配置符合网络安全攻击常见的现代环境中的 最佳安全实践。 暴力攻击通常涉及使用用户名和密码组合反复尝试获取对资源的访问权限。攻击者尝试使用其 Internet浏览器、安全客户端用户界面或其他工具输入多个用户名和密码,希望它们与AAA数据库中 的合法组合匹配。使用AAA进行身份验证时,我们希望最终用户输入其用户名和密码,因为这对建 立连接是必要的。同时,我们不会验证用户是谁,直到他们输入其凭证。从本质上讲,这使得攻击 者能够利用以下场景:

- 已公开的Cisco安全防火墙的完全限定域名(特别是在连接配置文件中使用组别名时):
 如果攻击者发现VPN防火墙的FQDN,则他们可以选择使用要在其中启动暴力攻击 的组别名来选择隧道组。
- 2. 使用AAA或本地数据库配置的默认连接配置文件:
 - 如果攻击者找到VPN防火墙的FQDN,他们可能会尝试对AAA服务器或本地数据库 进行暴力攻击。出现这种情况是因为与FQDN的连接位于默认连接配置文件上,即 使未指定组别名也是如此。
- 3. 防火墙或AAA服务器上的资源耗尽:
 - 攻击者可以通过发送大量身份验证请求和创建拒绝服务(DoS)条件来淹没AAA服务
 器或防火墙资源。

概念

组别名:

 防火墙可用来引用连接配置文件的备用名称。启动与防火墙的连接后,这些名称将显示在 Secure Client UI的下拉菜单中,以供用户选择。删除group-aliases会删除Secure Client UI中 的下拉功能。

组URL:

 可与连接配置文件绑定的URL,以便传入的连接直接映射到所需的连接配置文件。没有下拉功能,因为用户可以在安全客户端UI中输入完整的URL,或者可以将URL与XML配置文件中的 "显示名称"集成,以向用户隐藏URL。

此处的区别在于,当实施group-aliases时,用户发起连接to vpn_gateway.example.com,并显示别 名以选择将其驱动到连接配置文件。使用组URL,用户可启动到 vpn_gateway.example.com/example_group的连接,并将它们直接驱动到连接配置文件,而无需或 选择下拉菜单。

思科安全防火墙的安全客户端强化实践:

这些方法依靠将合法用户映射到正确的隧道组/连接配置文件,而将潜在的恶意用户发送到我们配置 为不允许用户名和密码组合的陷阱隧道组。虽然并非必须实现所有组合,但要使建议有效发挥作用 ,需要禁用group-aliases并更改DefaultWEBVPNGroup和DefaultRAGroup的身份验证方法。

• 禁用组别名并仅使用连接配置文件配置中的group-url,这样您就拥有了特定FQDN,攻击者无

法轻易发现和选择该FQDN,因为只有具有正确FQDN的客户端才能启动连接。例如 vpn_gateway.example.com/example_group比vpn_gateway.example.com更难被攻击者发现 。

- 在DefaultWEBVPNGroup和DefaultRAGroup中禁用AAA身份验证并配置证书身份验证,这样 可避免对本地数据库或AAA服务器实施暴力攻击。此场景中的攻击者在尝试连接时会立即看到 错误。由于身份验证基于证书,因此没有用户名或密码字段,从而停止暴力尝试。另一种选 择是创建不支持配置的AAA服务器,为恶意请求创建漏洞。
- 对连接配置文件使用证书映射。这允许根据从客户端设备上的证书接收的属性将传入连接映射 到特定连接配置文件。具有正确证书的用户会被正确映射,而未能满足映射条件的攻击者会被 发送到DefaultWEBVPNGroup。
- 使用IKEv2-IPSec而不是SSL会导致隧道组依赖于XML配置文件中的特定用户组映射。如果最终用户计算机上没有此XML,用户将自动发送到默认隧道组。



注意:有关组别名功能的详细信息,请参阅<u>ASA VPN配置指南</u>并观察"表1"。SSL VPN的连 接配置文件属性"(Connection Profile Attributes for SSL VPN)。

使用日志记录和Syslog ID识别攻击

暴力攻击是破坏远程访问VPN的主要方法,它利用弱密码来获得未经授权的访问。了解如何使用日志记录和评估syslog来识别攻击迹象至关重要。如果遇到异常卷,可能指示攻击的常见Syslog ID如下:

%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

在ASA上配置no logging hide username命令之前,用户名始终处于隐藏状态。



注意:注意:这提供了有效用户是否由违规的IP生成或知晓的信息,但请谨慎注意,因为用 户名在日志中可见。

Cisco ASA日志记录:

<u>安全ASA防火墙用户指南</u>

《Cisco安全防火墙ASA系列常规操作CLI配置指南》的<u>日志记录</u>一章

思科FTD日志记录:

通过 FMC 在 FTD 上配置日志记录

Cisco Secure Firewall Management Center Device Configuration Guide的Platform Settings一章中 的<u>Configure Syslog</u>部分

<u>配置并验证Firepower设备管理器中的系统日志</u>

<u>配置系统日志记录设置</u>部分(适用于Firepower设备管理器的Cisco Firepower威胁防御配置指南的 系统设置章节中)

攻击验证

要进行验证,请登录到ASA或FTD命令行界面(CLI),运行show aaa-server命令,并调查尝试到任何 已配置AAA服务器的身份验证请求数以及拒绝的身份验证请求数是否异常:

<#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配置示例

禁用DefaultWEBVPNGroup和DefaultRAGroup连接配置文件中的AAA身份验证

导航到设备>远程访问。

	Firewa Overview	all Manage //Dashboards	ment Center	Overview	Analysis	Policies	Devices	Objects	Integration			
Sum Provides Netw	nmary a summary vork	Dashboa of activity on the a Threats	ard (<u>switch dashboard)</u> appliance Intrusion Events	Status	Geolocation	QoS	Device M NAT QoS Platform FlexConf Certificat	lanagement Settings ig	VPN Site To Site Remote Access Dynamic Access Troubleshooting	s Policy	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	
► To	p Zero Tr	ust Application	ns			- ×					Upgrade Threat Defense Upgrade Chassis Upgrade	

显示导航FMC GUI以访问远程访问VPN策略配置。

编辑现有远程访问VPN策略并创建名为"DefaultRAGroup"的连接配置文件

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (• • •	admin \sim	citco SECURE
												Add
Name				Status			Last Modified					
RAVPN				Targeting 1 Up-to-date	devices on all targeted		2024-03-07 10:58:20 Modified by "admin"				1 1	

显示如何在FMC UI中编辑远程访问VPN策略。

编辑名为"DefaultWEBVPNGroup"和"DefaultRAGroup"的连接配置文件

Firewall Management Center Devices / VPN / Edit Connection Profile	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	९ 💿 🌣 🔞	admin ~ deaths SECURE
RAVPN									Save Cancel
Enter Description									
									Policy Assignments (1)
							Local Realm: LOCAL-RE/	ALM	Dynamic Access Policy: None
Connection Profile Access Interfaces Adva	anced								
Name			AAA				Group Policy		
DefaultWEBVPNGroup				LOCAL None None			DfltGrpPolicy		

显示如何在FMC UI中编辑DefaultWEBVPNGroup。

导航到AAA选项卡并选择Authentication Method下拉列表。选择Client Certificate Only并选择 Save。

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

在FMC UI中将DefaultWEBVPNGroup的身份验证方法更改为仅客户端证书。

编辑DefaultRAGroup并导航到AAA选项卡并选择Authentication Method下拉列表。选择"仅客户端 证书",然后选择保存。

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	ent certificate	
Authorization		
Authorization Server:	▼	
	Allow connection only if user exists in authorization database	
Accounting		
Accounting Server:	▼	
	Cancel	<i>i</i> e

在FMC UI中将DefaultRAGroup的身份验证方法更改为仅客户端证书。



注意:身份验证方法也可以是Sinkhole AAA服务器。如果使用此方法,则AAA服务器配置 是虚假的,实际上不会处理任何请求。还必须在"Client Address Assignment"(客户端地址 分配)选项卡中定义VPN池以保存更改。

在DefaultWEBVPNGroup和DefaultRAGroup上禁用Hostscan/安全防火墙状态(可选)

仅在您的环境中具有Hostscan/安全防火墙状态时才需要这样做。此步骤可防止攻击者通过终端扫描 进程增加防火墙上的资源利用率。在FMC中,这通过用命令without-csd创建FlexConfig对象以禁用 终端扫描功能来实现。

导航到"对象">"对象管理">"FlexConfig对象">"添加FlexConfig对象"。

Firewall Manageme Objects / Object Manageme	nt Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 🎯 admin 🗸	disce 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 RexConfig Object	
AS Path	Name	Description	
BFD Template Circher Suite List	Anyconnect_route_filtering		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.	F a Q
Distinguished Name DNS Server 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_Prefx_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside i	¶a q ⊒
 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	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_UnCentgure	Clears eigrp configuration for an AS	¶aα ≣

导航FMC用户界面以创建FlexConfig对象。

为FlexConfig对象命名,并将部署设置为Everytime,类型为Append。然后,完全按照所示输入语 法并保存对象。

Edit FlexConfig Object								0
Name: Wtihout-CSD Description: Copy-pasting any rich text might int	roduce line breaks	s while generating C	I Please	a verify the	: CLI before deplo	vment.		
Insert v 🔣 Deployment:	Everytime		•	Туре:	Append	,	•	
tunnel-group DefaultWEBVPNGroup w without-csd tunnel-group DefaultRAGroup webvp without-csd	ebvpn-attributes	3						
▼ Variables			Pror	ertv				
Name	Dimension	Default Value	(Тур	e:Name)	Override	Descript	ion	
		No records to	display					
							Cancel	Save

使用"without-csd"创建FlexConfig对象

导航到设备 > FlexConfig,然后点击铅笔以编辑FlexConfig策略。

D	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	? <	÷ 0	admin ~	esce SECURE
														New Policy
F	lexConfig Policy					Status		Last Modified						
	Flex-Test					Targeting 1 Out-of-date	devices on 1 targeted devices	2024-04-10 21:54:19 Modified by "admin"						¶∠i

编辑FMC中的FlexConfig策略。

找到您从用户定义部分创建的对象。然后,选择箭头将其添加到所选附加FlexConfigs。最后,选择 保存以保存FlexConfig策略。

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🧳 🔅 🛛 🛛 admin 🗸 👘 SECURE
FlexConfig							You have unsaved changes Migrate Config Preview Config Save Cancel
chier Description							Policy Assignments (1)
	"i Selec	ted Prepend F	lexConfigs				
Available FlexConfig C FlexConfig Object	# N	ame			Description		
	_						
Vuser Defined	·]						
"? Anyconnect_route_filtering							
"? Keepout							
1 No_Keepout							
System Defined							
"? Default_DNS_Configure							
Default_Inspection_Protocol_Disable							
2 Default_Inspection_Protocol_Enable	Selec	ted Append F	lexConfigs				
2 DHCPv6_Prefix_Delegation_Configure					B a contraction		
. DHCPv6_Prefix_Delegation_UnConfigure		ame			Description		
"? DNS_Configure	1 W	tihout-CSD					٩.3
DNS_UnConfigure							
"Eligrp_Configure							
"2 Elorp Interface Configure							

将FlexConfig对象附加到FlexConfig策略。

选择策略分配,并选择要应用此FlexConfig策略的FTD,然后选择确定。如果这是新的FlexConfig分 配,请再次选择保存并部署更改。部署完成后,验证

Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	९ ピ 🌣 ।	admin	
FlexConfig Enter Description														
													Po	olicy Assignments (1)
	3 Selecter	d Prepend	FlexConfigs											
Available FlexConfig C FlexConfig Object	# Nam				Description									
^		Tar	geted Devic	es										
V User Defined		т	argeted Device:	5										
* Keepout		-		_										
"? No_Keepout		Se	lect devices to	which you wa	int to apply thi	s policy.	Selected Devices							
"? Wthout-CSD			Search by nan	ne or value			FTD1	ì	7					
V System Defined			FTD1											
Default_DNS_Configure Default_Inspection_Protocol_Disable														
"? Default_Inspection_Protocol_Enable	I Selecter	1 Apr												
Therefore the the test of														
DHCPv6_Prefix_Delegation_UnConfigure	• Nam	•												
") DNS_Configure	1 With	out-C!												۹ 🖥
.9 DNS_UnConfigure										Cancel				
"i Egrp_interface_Configure														
.9 Eigrp_UnConfigure														

将FlexConfig策略分配到FirePOWER设备。

输入FTD CLI并为DefaultWEBVPNGroup和DefaultRAGroup发出命令show run tunnel-group。验证 配置中现在是否存在without-csd。

<#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

禁用Group-aliases并启用Group-URL

导航到连接配置文件并选择"别名"选项卡。禁用或删除组别名,然后单击加号图标以添加URL别名

0

Edit Connection Profil	е			
Connection Profile:*	LDAP-TG			
Group Policy:*	DfltGrpPolic	ÿ	• +	
Client Address Assignmen	t AAA	Aliases		

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

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	

在FMC UI中禁用隧道组的group-alias选项。

为URL别名配置对象名称,并为URL填写防火墙FQDN和/或IP地址,后跟您要与连接配置文件关联 的名称。在本例中,我们选择"aaaldap"。越模糊,就越安全,因为即使攻击者已经获取你的 FQDN,也很难猜到完整的URL。完成后,选择Save。

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

在FMC UI中创建URL别名对象。

从下拉列表中选择URL别名,选中Enabled框,然后选择OK。



确保在FMC UI中启用URL别名。

确保删除或禁用了组别名,并检查您的URL别名当前是否已启用,然后选择保存。

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 co	nfigured +
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 of the select s	t on web access. If users ch connection profile.	oose the +
URL	Status	
LDAP-ALIAS (https://ftd1 com/aaaldap)	Enabled	/1
	Cancel	Save

在FMC UI中启用隧道组的URL-Alias选项。

如果需要,还可以将URL别名作为XML的一部分推送。这通过使用VPN配置文件编辑器或ASA配置 文件编辑器编辑XML来实现。为此,请导航到Server List选项卡,并确保使用SSL时User Group字 段与连接配置文件的URL别名匹配。对于IKEv2,确保User Group字段与连接配置文件的确切名称 匹配。

Server List Entry X
Primary Server Connection Information Display Name (reguined) FTD1-SSL PGDN or IP A Dara Group Intil com AsA gateway Group URL INE Identity (IOS gateway only)
Badup Servers Host Address Add
Move Up Move D Delete
OK Cancel

编辑XML配置文件,使其具有SSL连接的URL别名。

证书映射

导航到"Remote Access VPN Policy"内的Advanced选项卡。根据首选项选择常规设置选项。选择后 ,请选择Add Mapping。

RAVPN Enter Description			You have unsaved changes Save	Cancel
Connection Profile Access Inter	aces Advanced		Policy Assic Local Realm: None Dynamic Access P	anments (1) 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 divice processes the policies in the order listed below unit it finds a match Use group URL if group URL and Certificate Map match different Connection Profiles Its the configured rules to match a certificate to 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 Please provide at least one Certificate Mapping	hed. If none of the Certificate Map is matched, default connection profile will	be chosen.	Mapping
Localized Installer Transforms	Certificate Map	Connection Profile		
Address Assignment Policy		No Records Found		
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 Certificate Map's rule is matched.			•

导航到FMC UI中的Advanced选项卡,以在FMC UI中创建证书映射对象。

为证书映射对象命名并选择Add Rule。在此规则中,定义要标识的证书的属性,以便将用户映射到 特定连接配置文件。完成后,选择OK,然后选择Save。

Add	l Certificate Map					6
Map C Map Cor	p Name*: Certificate-Map-CN pping Rule nfigure the certificate ma	atching rule			Add Rule	
#	Field	Component	Operator	Value		
1	Subject -	CN (Common Namer	Equals 🔻	customvalu	le	
	OK Cancel					
				Cance	Save	2

在FMC UI中创建证书映射并为映射添加条件。

从下拉列表中,选择证书映射对象以及您希望证书映射与之关联的连接配置文件。然后选择OK。

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	

将证书映射对象绑定到FMC UI中的所需隧道组。

确保将默认连接配置文件配置为DefaultWEBVPNGroup,这样,如果用户映射失败,则会将其发送 到DefaultWEBVPNGroup。完成后,选择Save并部署更改。

RAVPN		You I	we unsaved changed Save Cancel
Enter Description.			Policy Assignments (1)
		Local Realm: None	Dynamic Access Policy: None
Connection Profile Access Inte	rfaces Advanced		
Secure Client Images	General Settings for Connection Profile Mapping		
Secure Client Customization	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 Certificate Map, associated Connection Profile will be used when rules are ma	ched. If none of the Certificate Map is matched, default connection profile will be chosen.	
Custom Installer Transforms			Add Mapping
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:		DefaultWEBVPNGroup *

在FMC UI中将证书映射的默认连接配置文件更改为DefaultWEBVPNGroup。

IPsec-IKEv2

选择所需的IPsec-IKEv2连接配置文件,并导航到Edit Group Policy。

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

在FMC UI中编辑组策略。

在常规选项卡中,导航到VPN Protocols部分并确保IPsec-IKEv2框已选中。

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

在FMC UI的组策略中启用IPsec-IKEv2。

在VPN配置文件编辑器或ASA配置文件编辑器中,导航至Server List选项卡。用户组名称必须与防 火墙上的连接配置文件名称完全匹配。在本示例中,IKEV2是连接配置文件/用户组名称。主协议配 置为IPsec。当建立与此连接配置文件的连接时,"Display Name"(显示名称)会在安全客户端UI中 显示给用户。

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 IKE Identity (IOS gateway only)			
Backup Servers Host Address	Add Move Up Move D Delete			
OK Cancel				

编辑XML配置文件,使主要协议为IPsec,用户组与连接配置文件名称匹配。



注意:需要SSL连接才能将XML配置文件从防火墙推送到客户端。当仅使用IKEV2-IPsec时 ,必须通过带外方法将XML配置文件推送到客户端。

将XML配置文件推送到客户端后,安全客户端会使用XML配置文件中的用户组连接到IKEV2-IPsec连接配置文件。

🕲 Cisco Secu	re Client	_		×
	AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC	~	Connect	_
Cisco Se	ecure Client FTD1-IPSEC		×	-ijiaja cisco
Username: nroche Password:				
		,		

IPsec-IKEv2 RAVPN连接尝试的安全客户端UI视图。

ASA配置示例

禁用DefaultWEBVPNGroup和DefaultRAGroup连接配置文件中的AAA身份验证

输入tunnel-group DefaultWEBVPNGroup的webvpn-attributes部分并将身份验证指定为基于证书。 对DefaultRAGroup重复此过程。登录这些默认连接配置文件的用户必须提供用于身份验证的证书 ,而没有机会输入用户名和密码凭证。

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# authentication certificate

ASA# configure terminal ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes ASA(config-tunnel-webvpn)# authentication certificate 在DefaultWEBVPNGroup和DefaultRAGroup上禁用Hostscan/安全防火墙状态(可选)

仅在您的环境中具有Hostscan/安全防火墙状态时才需要这样做。此步骤可防止攻击者通过终端扫描 进程增加防火墙上的资源利用率。输入DefaultWEBVPNGroup和DefaultRAGroup的webvpnattributes部分以及连接配置文件,并实施without-csd以禁用终端扫描功能。

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

禁用Group-aliases并启用Group-URL

输入用户连接到的隧道组。如果存在现有的组别名,请将其禁用或删除。在本示例中,该选项处于 禁用状态。完成后,使用RAVPN终端接口的FQDN或IP地址创建group-url。group-url末尾的名称需 要隐藏。避免使用常用值,例如VPN、AAA、RADIUS和LDAP,因为这些值使攻击者更容易猜出完 整的URL(如果他们获取了FQDN)。请改用有助于识别隧道组的内部有效名称。

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

证书映射

在全局配置模式下,创建证书映射并为其分配名称和序列号。然后定义用户必须匹配才能使用映射 的规则。在本示例中,用户必须匹配等于"customvalue"的公用名称值的条件。接下来,输入 webvpn配置并将证书映射应用于所需的隧道组。完成后,输入DefaultWEBVPNGroup并将此隧道 组设置为证书映射失败用户的默认值。如果用户映射失败,则会将其定向到 DefaultWEBVPNGroup。虽然DefaultWEBVPNGroup配置了证书身份验证,但用户没有传递用户名 或密码凭据的选项。

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

IPsec-IKEv2

在全局配置模式下,您可以编辑现有组策略或创建新组策略并输入该组策略的属性。进入 attributes部分后,启用IKEv2作为唯一的vpn隧道协议。确保此组策略绑定到将用于IPsec-IKEV2远 程访问VPN连接的隧道组。与FMC步骤类似,您必须通过VPN配置文件编辑器或ASA配置文件编辑 器编辑XML配置文件,并更改User Group字段以匹配ASA上隧道组的名称,然后将协议更改为 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

在VPN配置文件编辑器或ASA配置文件编辑器中,导航至Server List选项卡。用户组名称必须与防 火墙上的连接配置文件名称完全匹配。主协议配置为IPsec。建立与此连接配置文件的连接时,将在 安全客户端UI中向用户显示显示显示名称。

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 FQDN FQDN FQDN FQDN/TG-NAME FQDN/TG-NAME	Connection Information Primary Protocol IPsec
Backup Servers	Add Move Up Move D Delete
ОК	Cancel

编辑XML配置文件,使主协议名称为IPsec,并且用户组名称与ASA的IPsec-IKEv2 RAVPN连接的隧道组名称匹配。



注意:需要SSL连接才能将XML配置文件从防火墙推送到客户端。当仅使用IKEV2-IPsec时 ,必须通过带外方法将XML配置文件推送到客户端。

结论

总之,本文档中的强化做法的目的是将合法用户映射到自定义连接配置文件,同时攻击者被迫使用 DefaultWEBVPNGroup和DefaultRAGroup。在优化配置中,两个默认连接配置文件没有任何合法 的自定义AAA服务器配置。此外,删除组别名可防止攻击者通过删除导航到防火墙的FQDN或公共 IP地址的下拉可视性来轻松识别自定义连接配置文件。

相关信息

<u>Cisco技术支持和下载</u>

<u>密码喷雾攻击</u>

未经授权的访问漏洞2023年9月

<u>ASA配置指南</u>

<u>FMC/FDM配置指南</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。