Implementar medidas de proteção para Secure Client AnyConnect VPN

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Conceitos
Práticas de fortalecimento do cliente seguro no Cisco Secure Firewall:
Identificar ataques usando IDs de registro e syslog
Verificação de ataque
Exemplos de configuração do FMC
Desative a autenticação AAA nos perfis de conexão DefaultWEBVPNGroup e DefaultRAGroup
<u>Desative a verificação de host/postura de firewall seguro em DefaultWEBVPNGroup e</u> <u>DefaultRAGroup (opcional)</u>
Desabilitar aliases de grupo e Habilitar URLs de grupo
Mapeamento de certificado
IPsec-IKEv2
Exemplos de configuração do ASA
Desative a autenticação AAA nos perfis de conexão DefaultWEBVPNGroup e DefaultRAGroup
<u>Desative a verificação de host/postura de firewall seguro em DefaultWEBVPNGroup e</u> <u>DefaultRAGroup (opcional)</u>
Desabilitar aliases de grupo e Habilitar URLs de grupo
Mapeamento de certificado
IPsec-IKEv2
Conclusão
Informações Relacionadas

Introdução

Este documento descreve como melhorar a segurança da implementação da VPN de acesso remoto.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Client AnyConnect VPN
- Configuração de acesso remoto ASA/FTD.

Componentes Utilizados

O guia de práticas recomendadas baseia-se nas seguintes versões de hardware e software:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.



Cuidado: este documento não contém etapas do Firepower Device Manager (FDM). O FDM só oferece suporte à alteração do método de autenticação no DefaultWEBVPNGroup. Use ACLs de plano de controle ou uma porta personalizada na

seção 'Configurações Globais' da VPN de Acesso Remoto na interface do usuário do FDM. Entre em contato com o Cisco Technical Assistance Center (TAC) para obter assistência adicional, se necessário.

Informações de Apoio

A finalidade deste documento é garantir que a configuração do AnyConnect VPN do Cisco Secure Client esteja aderindo às melhores práticas de segurança em um mundo moderno onde os ataques de segurança cibernética são comuns.

Os ataques de força bruta geralmente envolvem tentativas repetidas de obter acesso a um recurso usando combinações de nome de usuário e senha. Os invasores tentam usar seu navegador da Internet, a interface de usuário de cliente seguro ou outras ferramentas para inserir vários nomes de usuário e senhas, esperando que correspondam a uma combinação legítima em um banco de dados AAA. Ao usar AAA para autenticação, esperamos que o usuário final insira seu nome de usuário e senha, já que isso é necessário para estabelecer a conexão. Ao mesmo tempo, não estamos verificando quem é o usuário até que ele insira suas credenciais. Por natureza, isso permite que os invasores aproveitem os seguintes cenários:

- 1. Nomes de domínio totalmente qualificados expostos para o Cisco Secure Firewall (especialmente ao usar aliases de grupo no perfil de conexão):
 - Se o invasor descobrir o FQDN do seu firewall VPN, ele terá a opção de selecionar o grupo de túneis usando o alias de grupo no qual deseja iniciar o ataque de força bruta.
- 2. Perfil de Conexão Padrão configurado com AAA ou Banco de Dados Local:
 - Se o invasor encontrar o FQDN do firewall VPN, ele poderá tentar atacar de forma forçada o servidor AAA ou o banco de dados local. Isso ocorre porque a conexão com o FQDN cai no Perfil de Conexão Padrão, mesmo que nenhum alias de grupo seja especificado.
- 3. Esgotamento de recursos no firewall ou em servidores AAA:
 - Os invasores podem sobrecarregar os servidores AAA ou os recursos de firewall enviando grandes quantidades de solicitações de autenticação e criando uma condição de negação de serviço (DoS).

Conceitos

Apelidos de grupo:

 Um nome alternativo pelo qual o firewall pode se referir a um perfil de conexão. Depois de iniciar uma conexão com o firewall, esses nomes aparecem em um menu suspenso na IU do Secure Client para que os usuários selecionem. A remoção de aliases de grupo remove a funcionalidade suspensa na IU do Secure Client. URLs de grupo:

 Uma URL que pode ser vinculada a um perfil de conexão para que as conexões de entrada sejam mapeadas diretamente para um perfil de conexão desejado. Não há nenhuma funcionalidade suspensa, pois os usuários podem inserir a URL completa na IU do Secure Client ou a URL pode ser integrada a um 'Nome de exibição' no perfil XML para ocultar a URL do usuário.

A diferença aqui é quando os aliases de grupo são implementados, um usuário inicia uma conexão to vpn_gateway.example.com e é apresentado com aliases para selecionar a unidade para um perfil de conexão. Com URLs de grupo, um usuário inicia uma conexão com vpn_gateway.example.com/example_group e os direciona diretamente ao perfil de conexão sem a necessidade ou opção de um menu suspenso.

Práticas de fortalecimento do cliente seguro no Cisco Secure Firewall:

Esses métodos dependem do mapeamento de usuários legítimos para perfis de conexão/grupos de túneis apropriados, enquanto usuários potencialmente mal-intencionados são enviados para um grupo de túneis de interceptação que configuramos para não permitir combinações de nome de usuário e senha. Embora nem todas as combinações devam ser implementadas, a desabilitação de aliases de grupo e a alteração do método de autenticação de DefaultWEBVPNGroup e DefaultRAGroup são necessárias para que as recomendações funcionem de forma eficaz.

- Desabilite os aliases de grupo e use apenas group-url na configuração Perfil de Conexão; isso permite que você tenha um FQDN específico que não será fácil para um invasor descobrir e selecionar, já que apenas os clientes com o FQDN apropriado podem iniciar a conexão. Por exemplo, vpn_gateway.example.com/example_group é mais difícil para um invasor descobrir do que vpn_gateway.example.com.
- Desabilite a autenticação AAA no DefaultWEBVPNGroup e no DefaultRAGroup e configure a autenticação de certificado; isso evita uma possível força bruta contra o banco de dados local ou o servidor AAA. O invasor nesse cenário seria apresentado com erros imediatos ao tentar se conectar. Não há nenhum campo de nome de usuário ou senha, pois a autenticação é baseada em certificados, interrompendo, assim, tentativas de força bruta. Outra opção é criar um servidor AAA sem configuração de suporte para criar um sinkhole para solicitações mal-intencionadas.
- Utilize o mapeamento de certificado para o perfil de conexão. Isso permite que as conexões de entrada sejam mapeadas para perfis de conexão específicos com base nos atributos recebidos de certificados no dispositivo cliente. Os usuários que têm os certificados apropriados são mapeados corretamente, enquanto os invasores que falham nos critérios de mapeamento são enviados para o DefaultWEBVPNGroup.

 O uso de IKEv2-IPSec em vez de SSL faz com que os grupos de túneis dependam de um mapeamento de grupo de usuários específico no perfil XML. Sem esse XML na máquina do usuário final, os usuários são enviados automaticamente para o grupo de túneis padrão.



Observação: para obter mais informações sobre a funcionalidade de alias de grupo, consulte o <u>ASA VPN Configuration Guide</u> e observe a 'Tabela 1. Atributos do perfil de conexão para VPN SSL'.

Identificar ataques usando IDs de registro e syslog

Os ataques de força bruta representam o método predominante de comprometer as VPNs de acesso remoto, explorando senhas fracas para obter entrada não autorizada. É crucial saber como reconhecer os sinais de um ataque aproveitando o uso de registro e avaliando syslogs. Os IDs de syslogs comuns que podem indicar um ataque se encontrados com volume anormal são:

%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

O nome de usuário está sempre oculto até que o comando no logging hide username seja configurado no ASA.



Observação: Observação: isso fornece informações sobre usuários válidos gerados ou conhecidos por IPs ofensivos. No entanto, tenha cuidado, pois os nomes de usuário são visíveis nos logs.

Registro do Cisco ASA:

Guia do usuário para proteger o firewall ASA

Capítulo <u>Registro</u> do Guia de configuração da CLI de operações gerais do Cisco Secure Firewall ASA Series

Registro do Cisco FTD:

Configurar o registro no FTD usando o FMC

Seção <u>Configurar Syslog</u> no capítulo Configurações de plataforma do Guia de Configuração de Dispositivos do Cisco Secure Firewall Management Center <u>Configurar e verificar o Syslog no Gerenciador de dispositivos do Firepower</u>

<u>Seção Definindo as configurações de registro do sistema</u> no capítulo Configurações do sistema do Guia de configuração do Cisco Firepower Threat Defense para o Firepower Device Manager

Verificação de ataque

Para verificar, faça login no ASA ou na Interface de Linha de Comando (CLI) do FTD, execute o comando show aaa-server e investigue se há um número incomum de solicitações de autenticação tentadas e rejeitadas para qualquer um dos servidores AAA configurados:

<#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

Exemplos de configuração do FMC

Desative a autenticação AAA nos perfis de conexão DefaultWEBVPNGroup e DefaultRAGroup

Navegue até Devices > Remote Access.

	Firewall N Overview / Da	Janage i ashboards	ment Center / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration	
Sumi Provides a Netwo	mary Da summary of act ork Thr	ashboa tivity on the aj reats	ard (switch dashboard) ppliance Intrusion Events	Status	Geolocation	QoS	Device M NAT QoS Platform FlexCon Certifica	Aanagement Settings fig tes	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture
▶ Тор) Zero Trust #	Application	S			- ×				Upgrade Threat Defense Upgrade Chassis Upgrade

Exibe a navegação na GUI do FMC para acessar a configuração da política de VPN de acesso remoto.

Edite a Política de VPN de Acesso Remoto existente e crie um perfil de conexão chamado 'DefaultRAGroup'

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (• • •	admin ~	the SECURE
												Add
Namo				Status			Last Modified					
RAVPN				Targeting 1 o	devices on all targeted		2024-03-07 10:58:20 Modified by "admin"			q	/ i	

Exibe como editar a política de VPN de acesso remoto na interface do usuário do FMC.

Edite os perfis de conexão denominados 'DefaultWEBVPNGroup' e 'DefaultRAGroup'

Firewall Management Center Devices / VPN / Edit Connection Profile	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (• • •	admin ~	disce SECURE
RAVPN Enter Description												Cancel
								Level Dealers LOCAL	CALM		Policy.	Assignments (1)
Connection Profile Access Interfaces	Advanced							Local Realm. LOCAL-P	EALM		Cynamic Acci	ess Policy. None
Namo			AAA				Group Policy					
DefaultWEBVPNGroup				None None			DfltGrpPolicy					

Exibe como editar o DefaultWEBVPNGroup na interface do FMC.

Navegue até a guia AAA e selecione o menu suspenso Authentication Method. Selecione 'Somente certificado do cliente' e selecione Salvar.

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

Alterando o método de autenticação para certificado de cliente somente para DefaultWEBVPNGroup na interface do usuário do FMC.

Edite o DefaultRAGroup e navegue até a guia AAA e selecione o menu suspenso Authentication Method. Selecione 'Somente certificado do cliente' e Salvar.

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

Alterar o método de autenticação para certificado de cliente somente para DefaultRAGroup na interface do usuário do FMC.



Observação: o método de autenticação também pode ser um servidor AAA sinkhole. Se esse método for usado, a configuração do servidor AAA será falsa e não processará nenhuma solicitação. Um pool de VPNs também deve ser definido na guia "Client Address Assignment" (Atribuição de endereço de cliente) para salvar as alterações.

Desative a verificação de host/postura de firewall seguro em DefaultWEBVPNGroup e DefaultRAGroup (opcional)

Isso só é necessário se você tiver o Hostscan / Secure Firewall Posture em seu ambiente. Essa etapa impede que os invasores aumentem a utilização de recursos no firewall causada pelo processo de verificação de endpoint. No FMC, isso é obtido com a criação de um objeto FlexConfig com o comando without-csd para desabilitar a funcionalidade de verificação de endpoint.

Navegue até Objetos > Gerenciamento de objetos > Objeto FlexConfig > Adicionar objeto FlexConfig.

Cipects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🏟 admin 🗸	disco 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_litering		9/7 [*]
Community List	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNS	¶∎ Q ≣
DHCP IPv6 Pool	Default_Inspection_Protocol_Disable	Disable Default Inspection.	¶∎ ⊂, ;;;
> Distinguished Name DNS Server Group	Default_Inspection_Protocol_Enable	Enable Default Inspection.	¶∎ Q ≣
> External Attributes	DHCPv6_Prefx_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	¶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	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-su	¶_a ⊂, ≣
Key Chain	Eigrp_interface_Configure	Configures interface parameters for eigrp. 1. Configures authent	¶aq
Network	Eigrp_UnConfigure	Clears eigrp configuration for an AS	¶aq ⊒

Navegação na interface do usuário do FMC para criar um objeto FlexConfig.

Nomeie o objeto FlexConfig, defina a implantação como Everytime com o tipo Append. Em seguida, insira a sintaxe exatamente como mostrada e salve o objeto.

Edit FlexConfig Object						Ø
Name: Wtihout-CSD Description: Copy-pasting any rich text might info	roduce line breaks v	while generating CLI. Plea	se verify the	e CLI before deployr	nent.	
Insert 🔻 🔣 Deployment	Everytime	•	Туре:	Append	•]
tunnel-group DefaultWEBVPNGroup w without-csd tunnel-group DefaultRAGroup webvp without-csd	ebvpn-attributes					
▼ Variables		Dr	operty			
Name	Dimension	Default Value (T	ype:Name)	Override	Description	
		No records to display				
					Cancel	Save

Criando um objeto FlexConfig com 'without-csd'

Navegue até Devices > FlexConfig e clique no Pencil para editar a Política FlexConfig.

Ð	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	°	0	admin v	-dude SECURE
													New Policy
Be	exConfig 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"					9 🖊 î

Edição da política FlexConfig no FMC.

Localize o objeto criado na seção Definido pelo usuário. Em seguida, selecione a seta para adicioná-la ao Seleted Append FlexConfigs. Por fim, selecione Salvar para salvar a política FlexConfig.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Depkoy Q 🦆 🏠 🕢 admin 🗸 👘 SECURE
FlexConfig							You have unaseed changes Migrate Conting Preview Conting Save Cancel
							Policy Assignments (1)
	" Select	ed Prepend F	lexConfigs				
Available FlexConfig C FlexConfig Object	# Na	me			Description		
V User Defined							
**: Anyconnect_route_filtering **: Keepout							
입 No_Keepout 암 Without-CSD							
V System Defined							
"? Default_DNS_Configure							
Default_Inspection_Protocol_Disable							
? Default_Inspection_Protocol_Enable	Select	ed Append F	lexConfigs				
"? DHCPv6_Prefx_Delegation_Configure	I No	me			Description		
.) DHCPv6_Prefx_Delegation_UnConfigure	1 W1	hout-CSD					93
DNS UnConfigure							
12 Eigrp_Configure							
"} Eigrp_interface_Configure							

Anexe o objeto FlexConfig à política FlexConfig.

Selecione Policy Assignments e escolha o FTD ao qual você deseja aplicar esta política FlexConfig e, em seguida, selecione OK. Selecione Salvar novamente se esta for uma nova atribuição FlexConfig e implante as alterações. Após a implantação, verifique

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	apply this policy	y. Selected Devices FTD1	Selected Devices FTD1			
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. 🗑

Atribua a política FlexConfig a um dispositivo FirePOWER.

Insira o FTD CLI e emita o comando show run tunnel-group para o DefaultWEBVPNGroup e o DefaultRAGroup. Verifique se without-csd agora está presente na configuração.

<#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

Desabilitar aliases de grupo e Habilitar URLs de grupo

Navegue até um perfil de conexão e selecione a guia 'Aliases'. Desative ou exclua o alias de

grupo e clique no ícone de adição para adicionar um alias de 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. 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 following URLs, system will automatically log them in via this c	on web access. If users	choose the							
		_							
URL	Status								

Desabilitando a opção group-alias para um grupo de túneis na interface do usuário do FMC.

Configure um nome de objeto para o alias de URL e preencha o FQDN e/ou o endereço IP do firewall para o URL, seguido do nome ao qual você deseja associar o perfil de conexão. Neste exemplo, escolhemos 'aaldap'. Quanto mais obscuro, mais seguro, pois é menos provável que os invasores adivinhem o URL completo, mesmo que tenham obtido seu FQDN. Quando terminar, selecione Salvar.

Edit URL Objects		9
Name LDAP-ALIAS		
Description		
URL https://ftd1co	m/aaaldaj	
Allow Overrides		
	Cancel	Save

Criação de um objeto URL-Alias na interface do usuário do FMC.

Selecione o Alias de URL no menu suspenso, marque a caixa Enabled e selecione OK.



Verifique se o URL-Alias está habilitado na interface do usuário do FMC.

Verifique se o alias de grupo foi excluído ou desabilitado e se o Alias de URL está habilitado e selecione Salvar.

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.	iases from all connections configu	red ¹
Name	Status	
LDAP	Disabled	
URL Alias: Configure the list of URL alias which your endpoints can sele	ct 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	
		-
	Cancel	Save

Ativação da opção URL-Alias para um grupo de túneis na interface do usuário do FMC.

Se desejar, os aliases de URL também podem ser enviados como parte do XML. Isso é obtido editando o XML usando o VPN Profile Editor ou o ASA Profile Editor. Para fazer isso, navegue até a guia Lista de servidores e verifique se o campo Grupo de usuários corresponde ao Alias de URL do perfil de conexão ao usar SSL. Para IKEv2, certifique-se de que o campo User Group (Grupo de usuários) corresponda ao nome exato do perfil de conexão.

Server List Entry X
Primary Server Connection Information Display Name (required) FTD1-SSL FQDN or IP A Der Group asaidap ftb1 com Group URL IXE Identity (IOS gateway only)
Badup Servers Host Address Add Move Lb Move D Delete
OK Cancel

Editando o perfil XML para ter um URL-Alias para conexões SSL.

Mapeamento de certificado

Navegue até a guia Advanced dentro da Política de VPN de acesso remoto. Escolha uma opção de configuração geral com base na preferência. Depois de selecionado, selecione Adicionar Mapeamento.

RAVPN			You have unsaved changes Save Cancel
Enter Description			
			Policy Assignments (1)
Overseller Derfle Averselsted	hour Advanced	Local Re	alm: None Dynamic Access Policy: None
Connection Prome Access Inten	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	Lient request is checked against each Certificate Map, associated Connection Prome will be used when rules are matc Please provide at least one Certificate Mapping.	neo. Il none ol une Certilicate Map is matcheo, detauti connection prolle will be chose	
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			
IPsec/IKEv2 Parameters	Denaux Connection Profile will be avoided when none of the Certificate Mar's rule is matched.		· · · ·

Navegar até a guia Avançado na interface do usuário do FMC para criar um objeto de mapa de certificado na interface do usuário do FMC.

Nomeie o objeto de mapa do certificado e selecione Adicionar Regra. Nesta regra, defina as propriedades do certificado que você deseja identificar para mapear o usuário para um determinado perfil de conexão. Quando terminar, selecione OK e, em seguida, Salvar.

Add	Certificate Map					Ø
Map Ce Mapp Confi	Name*: rtificate-Map-CN ping Rule igure the certificate m	atching rule			Add Rul	e
#	Field	Component	Operator	Value		
1	Subject 🔻	CN (Common Name -	Equals 🔹	customval	ue	
	OK Cancel					
				Cance	el Sa	ve

Crie um mapa de certificado e adicione critérios para o mapa na interface do usuário do FMC.

No menu suspenso, selecione o objeto de mapa de certificado e o perfil de conexão ao qual deseja que o mapa de certificado seja associado. Em seguida, selecione OK.

Add Connection Profile to Certificate N	lap 🕜
Choose a Certificate Map and associate Connecti selected Certficate Map.	on Profiles to
Certificate Map Name*:	
Certificate-Map-CN +	
Connection Profile*:	
LDAP-TG 🔻	
Canc	el OK

Vincule o objeto de mapa do certificado ao grupo de túneis desejado na interface do usuário do FMC.

Verifique se o Perfil de Conexão Padrão está configurado como DefaultWEBVPNGroup para que, se um usuário falhar no mapeamento, ele seja enviado para o DefaultWEBVPNGroup. Quando terminar, selecione Save e implante as alterações.

RAVPN Enter Description			You have unsaved changes Save Cancel
			Policy Assignments (1)
Connection Profile Access Inter	faces Advanced		Local Realm: None Dynamic Access Policy: None
Secure Client Images Secure Client Customization GUI Text and Messages Icons and Images Scripts Binaries	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 Vest 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 with Certificate to Connection Profile Mapping	hen rules are matched. If none of the Certificate Map is matched, defaul	t 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: This Connection Profile will be applied when none of the Certificate Map's rule is matched.		DefaultWEBVPNGroup

Altere o perfil de conexão padrão do mapeamento de certificado para DefaultWEBVPNGroup na interface do usuário do FMC.

IPsec-IKEv2

Selecione o perfil de conexão IPsec-IKEv2 desejado e navegue para Editar política de grupo.

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	
	Cance	Save

Edite uma política de grupo na interface do usuário do FMC.

Na guia General, navegue até a seção VPN Protocols e verifique se a caixa IPsec-IKEv2 está marcada.

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

Habilite IPsec-IKEv2 em uma política de grupo na interface do usuário do FMC.

No Editor de perfis VPN ou no Editor de perfis ASA, navegue até a guia Lista de servidores. O nome do grupo de usuários DEVE corresponder exatamente ao nome do perfil de conexão no firewall. Neste exemplo, IKEV2 era o perfil de conexão / nome do grupo de usuários. O protocolo primário está configurado como IPsec. O 'Nome de exibição' no é exibido para o usuário na interface do usuário do Secure Client ao estabelecer uma conexão com este perfil de conexão.

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
OK	Move D Delete

Edite o perfil XML para que o protocolo principal seja IPsec e o Grupo de usuários corresponda ao nome do perfil de conexão.



Cuidado: uma conexão SSL é necessária para enviar perfis XML do firewall para o cliente. Ao usar apenas IKEV2-IPsec, os perfis XML devem ser enviados aos clientes por meio de um método fora de banda.

Depois que o perfil XML é enviado ao cliente, o Secure Client usa o Grupo de Usuários do perfil XML para se conectar ao perfil de conexão IKEV2-IPsec.

🕲 Cisco Secur	re Client	_		×
	AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC	~	Connect	_
🔅 🕕 🕲 Cisco Se	ecure Client FTD1-IPSEC		×	altalta cisco
	ername: nroche			

Exibição da interface do usuário do cliente seguro da tentativa de conexão IPsec-IKEv2 RAVPN.

Exemplos de configuração do ASA

Desative a autenticação AAA nos perfis de conexão DefaultWEBVPNGroup e DefaultRAGroup

Insira a seção webvpn-attributes para grupo de túnel DefaultWEBVPNGroup e especifique a autenticação como baseada em certificado. Repita esse processo para o DefaultRAGroup. Os usuários que chegam a esses perfis de conexão padrão são forçados a apresentar um certificado para autenticação e não têm a oportunidade de inserir credenciais de nome de usuário e senha.

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

Desative a verificação de host/postura de firewall seguro em DefaultWEBVPNGroup e DefaultRAGroup (opcional)

Isso só é necessário se você tiver o Hostscan / Secure Firewall Posture em seu ambiente. Essa etapa impede que os invasores aumentem a utilização de recursos no firewall causada pelo processo de verificação de endpoint. Insira a seção webvpn-attributes para os perfis de conexão e DefaultWEBVPNGroup e DefaultRAGroup e implemente without-csd para desabilitar a funcionalidade de verificação de ponto de extremidade.

```
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
```

Desabilitar aliases de grupo e Habilitar URLs de grupo

Digite o grupo de túneis ao qual os usuários estão se conectando. Se houver um alias de grupo existente, desabilite-o ou remova-o. Neste exemplo, ele está desativado. Quando estiver concluído, crie um group-url usando o FQDN ou o endereço IP da interface de terminação RAVPN. O nome no final da url de grupo precisa ser obscuro. Evite valores comuns, como VPN, AAA, RADIUS e LDAP, pois eles facilitam para os invasores adivinharem a URL completa se obtiverem o FQDN. Em vez disso, use internamente nomes significativos que ajudem a identificar o grupo de túneis.

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

Mapeamento de certificado

No modo de configuração global, crie um mapa de certificado e atribua a ele um nome e um número de sequência. Em seguida, defina uma regra que os usuários devem corresponder para utilizar o mapeamento. Neste exemplo, os usuários teriam que corresponder aos critérios de um valor de nome comum igual a "valor personalizado". Em seguida, insira a configuração de webvpn

e aplique o mapa de certificado ao grupo de túneis desejado. Depois de concluído, insira DefaultWEBVPNGroup e torne este grupo de túneis o padrão para usuários que falharem no mapeamento de certificado. Se os usuários falharem no mapeamento, eles serão direcionados para o DefaultWEBVPNGroup. Enquanto o DefaultWEBVPNGroup estiver configurado com autenticação de certificado, os usuários não terão a opção de passar credenciais de nome de usuário ou senha.

```
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

No modo de configuração global, você pode editar uma diretiva de grupo existente ou criar uma nova e inserir os atributos dessa diretiva de grupo. Quando estiver na seção de atributos, ative IKEv2 como o único protocolo de túnel VPN. Certifique-se de que essa política de grupo esteja vinculada a um grupo de túneis que será utilizado para conexões VPN de acesso remoto IPsec-IKEV2. Semelhante às etapas do FMC, você deve editar o perfil XML através do VPN Profile Editor ou do ASA Profile Editor e alterar o campo User Group para corresponder ao nome do grupo de túneis no ASA, e alterar o protocolo para 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

No Editor de perfis VPN ou no Editor de perfis ASA, navegue até a guia Lista de servidores. O nome do grupo de usuários DEVE corresponder exatamente ao nome do perfil de conexão no firewall. O protocolo primário está configurado como IPsec. O nome de exibição é mostrado ao usuário na interface do usuário do Secure Client ao estabelecer uma conexão com este perfil de conexão.

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 Group URL FODN/TG-NAME	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	

Edite o perfil XML para que o nome do protocolo primário seja IPsec e o nome do Grupo de Usuários corresponda ao nome do grupo de túneis do ASA para conexões IPsec-IKEv2 RAVPN.



Cuidado: uma conexão SSL é necessária para enviar perfis XML do firewall para o cliente. Ao usar apenas IKEV2-IPsec, os perfis XML devem ser enviados aos clientes por meio de um método fora de banda.

Conclusão

Em resumo, a finalidade das práticas de proteção neste documento é mapear usuários legítimos para perfis de conexão personalizados, enquanto os invasores são forçados para o DefaultWEBVPNGroup e o DefaultRAGroup. Em uma configuração otimizada, os dois perfis de conexão padrão não têm nenhuma configuração de servidor AAA personalizada legítima. Além disso, a remoção de aliases de grupo impede que os invasores identifiquem facilmente perfis de conexão personalizados, removendo a visibilidade suspensa ao navegar para o FQDN ou o endereço IP público do firewall.

Informações Relacionadas

Suporte técnico e downloads da Cisco

Ataques de borrifo de senha

Vulnerabilidade de acesso não autorizado setembro de 2023

Guias de configuração do ASA

Guias de configuração do FMC/FDM

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.