Configuración de las políticas de control de acceso del plano de control para Secure Firewall Threat Defence y ASA

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Configuraciones
Configuración de una ACL de plano de control para FTD gestionada por FMC
Configuración de una ACL de plano de control para FTD gestionada por FDM
Configuración de una ACL de plano de control para ASA mediante CLI
Configuración alternativa para bloquear los ataques de firewall seguro mediante el comando <u>'shun'</u>
<u>Verificación</u>
Errores relacionados

Introducción

Este documento describe el proceso para configurar las reglas de acceso del plano de control para Secure Firewall Threat Defense y Adaptive Security Appliance (ASA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protección frente a amenazas de firewall (FTD)
- Administrador de dispositivos de firewall seguro (FDM)
- Centro de gestión de firewall seguro (FMC)
- ASA de firewall seguro
- · Lista de control de acceso (ACL)
- FlexConfig

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Secure Firewall Threat Defence versión 7.2.5
- Secure Firewall Manager Center versión 7.2.5
- Secure Firewall Device Manager versión 7.2.5
- Secure Firewall ASA versión 9.18.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El tráfico normalmente atraviesa un firewall y se enruta entre interfaces de datos; en algunas circunstancias, es beneficioso denegar el tráfico destinado al firewall seguro. El firewall seguro de Cisco puede utilizar una lista de control de acceso (ACL) del plano de control para restringir el tráfico "listo para usar". Un ejemplo de cuándo una ACL del plano de control puede ser útil sería controlar qué peers pueden establecer un túnel VPN (VPN de sitio a sitio o de acceso remoto) al firewall seguro.

Tráfico "mediante el dispositivo" de firewall seguro

El tráfico normalmente atraviesa los firewalls de una interfaz (entrante) a otra interfaz (saliente), lo que se conoce como tráfico 'mediante el dispositivo' y lo gestionan tanto las políticas de control de acceso (ACP) como las reglas de prefiltrado.



Imagen 1. Ejemplo de tráfico listo para usar

Tráfico "listo para usar" de firewall seguro

Hay otros casos en los que el tráfico está destinado directamente a una interfaz FTD (VPN de sitio a sitio o de acceso remoto), esto se conoce como tráfico "a la caja" y es administrado por el plano de control de esa interfaz específica.



Imagen 2. Ejemplo de tráfico To-the-box

Consideraciones Importantes sobre las ACL del Plano de Control

- A partir de la versión 7.0 de FMC/FTD, se debe configurar una ACL del plano de control mediante FlexConfig, utilizando la misma sintaxis de comandos utilizada en el ASA.
- La palabra clave control-plane se agrega a la configuración del grupo de acceso, que aplicará el tráfico 'a' la interfaz de firewall segura. Sin la palabra del plano de control anexada al comando, la ACL restringiría el tráfico a 'través' del firewall seguro.
- Una ACL de plano de control no restringirá SSH, ICMP o TELNET entrante a una interfaz de firewall segura. Se procesan (se permiten o deniegan) según las directivas de configuración de la plataforma y tienen mayor prioridad.
- Una ACL del plano de control restringe el tráfico "al" propio firewall seguro, mientras que la política de control de acceso para el FTD o las ACL normales para el ASA, controla el tráfico "a través" del firewall seguro.
- A diferencia de una ACL normal, no hay una 'deny' implícita al final de la ACL.
- En el momento de la creación de este documento, la función de geolocalización de FTD no se puede utilizar para restringir el acceso al FTD.

Configurar

En el siguiente ejemplo, un conjunto de direcciones IP de un país determinado intenta aplicar fuerza bruta VPN a la red al intentar iniciar sesión en el RAVPN FTD. La mejor opción para proteger el FTD contra estos ataques de fuerza bruta VPN es configurar una ACL de plano de control para bloquear estas conexiones a la interfaz FTD externa.

Configuraciones

Configuración de una ACL de plano de control para FTD gestionada por FMC

Este es el procedimiento que debe seguir en un FMC para configurar una ACL del plano de control para bloquear los ataques de fuerza bruta de VPN entrantes a la interfaz FTD externa:

Paso 1. Abra la interfaz gráfica de usuario (GUI) de FMC mediante HTTPS e inicie sesión con sus

credenciales.



Imagen 3. Página de inicio de sesión de FMC

Paso 2. Necesita crear una ACL extendida. Para ello, navegue hasta Objetos > Gestión de objetos.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q <mark>6</mark> 🌣 🕜 admi	n - diada SECURE
Summary Dashboard (switch.dashboard) Provides a summary of activity on the spolance					Object N Intrusion	lanagement Rules			Reporting
Network $ imes$ Threats Intrusion Events	Status (Geolocation	QoS					Show the Last 1 hour	• 11
 Unique Applications over Time 		-× •	Top Web App	lications Seen				Top Client Applications Seen	
No Data Last updated 2 minutes ago				utes ago	No Data			No Data Last updated 2 minutes ago	
 Traffic by Application Risk 			Top Server A	pplications See	n		- ×	Top Operating Systems Seen	

Imagen 4. Gestión de objetos

Paso 2.1. En el panel izquierdo, navegue hasta Lista de acceso > Extendida para crear una ACL extendida.

Firewall Managemen	t Center _{Overview}	Analysis Policies	Devices O	bjects Integration	Dep	olay Q 🧬 🌣 🛛	admin -
> AAA Server Access List Extended Standard 	Network A network object represents o network discovery rules, event	ne or more IP addresses. N searches, reports, and so	letwork objects are on.	used in various places,	Add Network including access control policies, n	Filter Show etwork variables, intrusio	Unused Objects n rules, identity rules,
> Address Pools	Name				Value	Туре	Override
Application Filters AS Path	any				0.0.0.0/0 ::/0	Group	Q ≣ ₿
Cipher Suite List	any-ipv4				0.0.0.0/0	Network	Q ≣ ₿
> Community List	any-ipv6				::/0	Host	Q ≣ ₩
 Distinguished Name DNS Server Group 	IPv4-Benchmark-Tests				198.18.0.0/15	Network	Q ≣ ₿
> External Attributes	IPv4-Link-Local				169.254.0.0/16	Network	Q 🗑 👪
File List	IPv4-Multicast				224.0.0.0/4	Network	Q. () ₿
Geolocation	IPv4-Private-10.0.0.0-8				10.0.0/8	Network	Q ≣ ₩
Interface	IPv4-Private-172.16.0.0-12				172.16.0.0/12	Network	ବ ≣ ଈ
Key Chain	IPv4-Private-192.168.0.0-16				192.168.0.0/16	Network	Q 🗎 👪
Network	IPv4-Private-All-RFC1918				10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	ଦ 🗎 ୫
Policy List Port					Display	ing 1 - 14 of 14 rows 🔣	< Page 1 of 1 > > C

Imagen 5. Menú ACL extendido

Paso 2.2. A continuación, seleccione Agregar lista de acceso ampliada.

Firewall Managemen Objects / Object Managemen	nt Center _{Overview}	Analysis F	Policies Devi	ces Objects	Integration	Deploy	Q 🧬 🌣 🔞	admin • ·	elsee SECURE
> AAA Server	Extended					Add Extended Acces	s List ् २ Filter		
✓ Access List	An access list object, also k	nown as an access	control list (ACI)	selects the traffic to	which a service will apply. Sta	andard-Identifies traffic ha	sed on destination :	address only 1	dentifies
Extended	traffic based on source and	destination address	and ports. Supp	orts IPv4 and IPv6 a	dresses. You use these object	s when configuring partic	ular features, such a	s route maps.	
Standard									
> Address Pools	Name					Value		Override	
Application Filters									
AS Path									
Community List									
Distinguished Name									
DNS Server Group									
> External Attributes									
File List									
> FlexConfig									
Geolocation									
Interface									
Key Chain									
Network									
> ркі									
Policy List									
Port						No	data to display	Page 1	of 1 > > C
> Prefix List									

Imagen 6. Agregar ACL extendida

Paso 2.3. Escriba un nombre para la ACL extendida y, a continuación, haga clic en el botón Agregar para crear una entrada de control de acceso (ACE):

Firewall Mana Objects / Object M	agement Ce anagement	nter	Overview	Analysis Policie	s Devices Ob	jects Integration		Deploy Q	🧐 🌣 🔞	admin • •	the SECURE
> AAA Server	New Exte	nded Acc	cess List Obj	ect							
Extended	Name ACL-UNW	ANTED-CO	UNTRY							dress only. In oute maps.	dentifies
> Address Pools Application Filters	Entries (0)								Artel	Override	
AS Path Cipher Suite List	Sequence	Action	Source	Source Port	Destinat	on Destinat	tion Port Applicatio	n	Add		
Community List Distinguished Name											
DNS Server Group											
File List FlexConfig Configence											
Interface	Allow Ot	errides									
Network									Save		
Policy List Port								No data t	o display 🖂 <	Page 1	of 1 > > C
> Deather Link											

Imagen 7. Entradas de ACL extendidas

Paso 2.4. Cambie la acción ACE a Block (Bloquear), luego agregue la red de origen para que coincida con el tráfico que debe ser denegado al FTD, mantenga la red de destino como Any (Cualquiera) y haga clic en el botón Add (Agregar) para completar la entrada ACE:

- En este ejemplo, la entrada ACE configurada bloqueará los ataques de fuerza bruta VPN que provienen de la subred 192.168.1.0/24.

Firewa Objects /	Action: Block			cisco SECURE
> AAA Server	Logging: Default			
Extended	Log Level:			Identifies 3.
Standard Address Pools	Log Interval:			
Application Filt AS Path	300 Sec. Network Port () Application			/ ≣ 88
Cipher Suite Lis	Available Networks C +	Source Networks (1)	Destination Networks (0)	
> Distinguished N	Q Search by name or value	192.168.1.0/24	any	
DNS Server Gro	any Add to Source			
> External Attribu	any-ipv4 Add to Destination			
File List	any-ipv6			
> FlexConfig	IPv4-Benchmark-Tests			
Geolocation	IPv4-Link-Local			
Interface	IPv4-Multicast			
Key Chain	IPv4-Private-10.0.0.0-8			
Network	IPv4-Private-172.16.0.0-12	Enter an IP address Add	Enter an IP address Add	
> ркі				
Policy List				
Port			Cancel	
> Prefix List			Calleer	

Imagen 8. Redes denegadas

Paso 2.5. En caso de que necesite agregar más entradas ACE, vuelva a hacer clic en el botón Add (Agregar) y repita el paso 2.4. Después de esto, haga clic en el botón Save (Guardar) para completar la configuración de ACL.

Firewall Managemen Objects / Object Management	Edit Exten	nded Acc	ess List Object					0	cisco SECURE
➢ AAA Server ✓ Access List	Name ACL-UNW	ANTED-CC	PUNTRY						
Extended	Entries (1)								Identifies
Standard								Add	
> Address Pools									
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		人主体
AS Path	1	Block	192.168.1.0/24					11	
Cipher Suite List									
> Community List									
> Distinguished Name									
DNS Server Group									
> External Attributes									
File List	Allow Ov	verrides							
> FlexConfig									
Geolocation									
Interface								Save	
Key Chain									
Network									
> ркі									
Policy List									
Port							Displaying 1 - 1 of 1 rows	I< < Page 1	of 1 $>$ $>$ C
> Prefix List									

Imagen 9. Entradas de ACL extendidas completadas

Paso 3. A continuación, debe configurar un objeto Flex-Config para aplicar la ACL del plano de control a la interfaz FTD externa. Para ello, desplácese al panel izquierdo y seleccione la opción FlexConfig > Objeto FlexConfig.

P	Firewall Management Objects / Object Management	t Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	¢ 🔮	🕴 🕜 admin 🔻	cisco SECURE
> AA	A Server	Extende	d						Add Extended Acces	s List ् ९	ilter	
✓ Acc	Extended	An access list traffic based o	object, also known source and d	own as an acc lestination add	ess control lis ress and ports	t (ACL), select s. Supports IPv	s the traffic to 4 and IPv6 ad	which a service will apply. S dresses. You use these obje	Standard-Identifies traffic be ects when configuring partic	ased on destin ular features, :	ation address only such as route map	y. Identifies ps.
> Ad	dress Pools	Name							Value		Override	
Ap) AS	plication Filters Path	ACL-UNWANT	TED-COUNTRY									1 1 6
Cip	her Suite List											
> Coi	mmunity List											
DIS	S Server Group											
> Ext	ernal Attributes											
File	List											
Y Fle	xConfig											
	FlexConfig Object											
Ge	plocation											
Inte	erface											
Key	/ Chain											
Net	work											
> ркі									Displaying	1 - 1 of 1 rows	K < Page 1	of 1 > > C
Del	inst link											



Paso 3.1. Haga clic en Agregar objeto FlexConfig.

Firewall Manageme	It Center Overview Analysis Policies Devices Objects Integ	pration Deptoy Q 🥩 🌣 🕜 admin 🔻 🖞
 AAA Server Access List Extended Standard 	FlexConfig Object FlexConfig Object include device configuration commands, variables, and scripting language	Add FlexConfig Object
> Address Pools	Name	Description
Application Filters AS Path	Default_DNS_Configure	Configure Default DNS with the help of TextObj ${f F_2}$ Q, $\ \widehat{\ }$
Cipher Suite List	Default_Inspection_Protocol_Disable	Disable Default Inspection. 📲 🔍 🗎
> Community List	Default_Inspection_Protocol_Enable	Enable Default Inspection. 😼 Q 🗎
Distinguished Name DNS Segrer Group	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one insid 📲 Q 🗎
External Attributes	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client 🛛 🖥 🔍 🗎
File List	DNS_Configure	Configure DNS with the help of TextObjects dn ${f P} \ {f Q} \ $
 FlexConfig FlexConfig Object 	DNS_UnConfigure	Remove the DNS configurations. 🖥 Q 📄
Text Object	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. co 📲 Q 🗎
Geolocation	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1, C 🖥 🔍 🗎
Interface	Eigrp_UnConfigure	Clears eigrp configuration for an AS
Key Chain	Eigra Llaconfigura All	Close elementation in O
> ркі		Displaying 1 - 20 of 48 rows I < < Page 1 of 3 > I C

Imagen 1. Agregar Objeto Flexconfig

Paso 3.2. Agregue un nombre para el objeto FlexConfig y, a continuación, inserte un objeto de directiva ACL. Para ello, seleccione Insertar > Insertar objeto de directiva > Objeto ACL extendido.

AAA Server AAA Server Cathodical Standard A doress Lat Standard Aca Cosy-pasting any rich text might introduce line breaks while generating CLL Please verify the CLI before deployment. Impert Polyney Object A cogr-pasting any rich text might introduce line breaks while generating CLL Please verify the CLI before deployment. Impert Polyney Object A cogr-pasting any rich text might introduce line breaks while generating CLL Please verify the CLI before deployment. Impert Polyney Object Intert Strete Key Scattard ACL Object Intert Matrixbutes Fiel Lat Variables Variables Impert Polyney Object Intert Dimension Default Value Property To records to display Intert Strete Key Intert Dimension Default Value Property To records to display Intert Strete Key Intert Dimension Default Value Property To records to display Intert Strete Key Intert Dimension Default Value Property To records to display Intert Strete Key Intert Dimension Default Value Property To records to display Intert Strete Key Intert Dimension Default Value Property To records to display Intert Dimension Default Value Property To records to display Intert Dimension Default Value Property To records to display Intert Dimension Default Value Property To records to display Intert Dimension Default Value Property To records to display Intert Dimension Default Value Property To records to display Intert Dimension Default Value Property To records to display Intert Dimension Default Value Property To records to display Intert	Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE						🏄 👩 admin 🔻 讨	
AAA Server AAA Server AAA Server Access Lit Standard A docess Lot Standard A docess Pools Application Filters Application Filters Application Filters As Path Cipher Suite List Distinguished Name Distinguished Name PiexConfig • Variables • File List • Variables • Nore ords to display File List • Name Dimension Default Value Property (Type: Name) Override Description • Nore ords to display • Pid • Converting • Pid • Converting • Converting • Converting • Converting • Pid • Converting • Pid • Converting		Description:							
Access Lat Extended Standard Address Pools Applications Filters As Path Cipher Suite List Community Lat Community Lat Community Lat Community Lat Statenaided Act Object Text Object Text Object Text Object Text Object Name Dimension Default Value Property No records to display Override Description No records to display (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 (X < Page 1 di < 2 < 2000 </td <td>> AAA Server</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Filter</td> <td></td>	> AAA Server							Filter	
Extended Sundard > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Attributes File List • Config Object • Variables • Name Dimension Default Value No records to display interface Koy Chain Network > PK1									
Standard > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Attributes File List Variables Name Dimension Default Value Property (Override Description intert Sort Cope > PKi	Extended	Copy-pasting any rich to	ext might introduce line break	s while generating CLI.	. Please verify the	e CLI before deploy	ment.		
Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Atributes File List Variables Name Network No records to display	Standard	locart -	Deployment:		- Tree	Annend			
Application Filters AS Path Cipher Suite List Community Community Community List Community	> Address Pools	Insert Policy Object	Taut Object		Type.	Append	•		
AS Path Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Attributes File List Variables File List Variables File Config Object Text Object Geolocation Interface Key Chain Network > Kil	Application Filters	Insert System Variable N	Network					the help of TextObi	Fa a T
Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Attributes File List > FlexConfig • Variables Name Dimension Default Value Property Override Description interface key Chain Network > PKi	AS Path	Insert Secret Key	Security Zenes						
Community List Distinguished Name DNS Server Group External Attributes File List • Variables • Variables • Variables • Route Map • Override Discription • Route Map • Override Discription • Route Map • Override Discription • resconfig • Anne Dimension Default Value Property (TypesName) • Override Description • resconfig • override • Discription • resconfig • Anne Dimension Default Value • Property • No records to display • terride • override • Description • override • override • Description • override • overide • override • override • overrid	Cipher Suite List		Standard ACL Object						η α -
> Distinguished Name DNS Server Group > External Attributes File Llat • FlexConfig • Variables • Variables • Name Dimension Default Value Property (TypesName) Override Description interface Key Chain Network > PKi	> Community List		Extended ACL Object						¶∎ Q =
DNS Server Group > External Attributes File List • Variables • Variables • Variables • Variables • Name Dimension Default Value Property (TypesName) Override Description interface key Chain Network > PKi	> Distinguished Name		Route Map					lient) and one insid	Faq =
> External Attributes File List a outside (PD client	DNS Server Group		Route Map						
Flie List	> External Attributes							e outside (PD client	<u>н</u> с –
✓ FlexConfig ↓ Variables on s. Image: Second								of TextObjects dn	¶∎ q =
FlexConfig Object Name Dimension Default Value Property (Type:Name) Override Description Text Object Interface	✓ FlexConfig	▼ Variables						lions	Ra ⊇
Text Object Interface Geolocation No records to display Interface Interface Key Chain Interface Network Interface > PKI Interface		Name	Dimension	Default Value	Property (Type:Name)	Override	Description	0115.	
Geolocation NoticeUsia to display Interface ters for eigrp. 1. C I a Q i Key Chain ran AS Network Image: Constant Con	Text Object			No records to d	(Type:rume)			res next hop. 2. co	П О, П
Interface Key Chain r an AS Fa Q i Network Fa Q i Fa Q i Vertice Fa Q i Fa Q i Vertice Vertice Fa Q i Vertice Vertice Fa Q i	Geolocation			No Tecolas to a	врнау			sters for eigrp. 1. C	₽ Q →
Key Chain Pair As Image: Chain Network Image: Chain Image: Chain > PKI Image: Chain Image: Chain	Interface							A ne x	E o =
Network Fig.q. > PKI K < Page 1 of 3 > >IC	Key Chain							pi all AS	
> PKI	Network								Fi Q
	> ркі							s IC < Page 1	of 3 > > C

Imagen 12. Variable de objeto FlexConfig

Paso 3.3. Agregue un nombre para la variable de objeto ACL y, a continuación, seleccione la ACL extendida que se creó en el paso 2.3; después de esto, haga clic en el botón Save (Guardar).

Firewall Managemen	Name: OBJ-FC-CONTROL-PLANE	:			⊁ 🥑 admin ▾ 🏻 🖞	sco SECURE
> AAA Server ~ Access List	Description:	Insert Extended Access List Object Var	iable 🛛 🔞		Filter	
Extended Standard > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Attributes	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY Description: Available Objects C Q Search C C UNWANTED COUNTRY	Selected Object FlacL-UNWANTED-COUNTRY		the help of TextObj ;lient) and one insid a outside (PD client	
File List Y FlexConfig	▼ Variables				> of TextObjects dn	¶ ¶ 10
FlexConfig Object Text Object Geolocation Interface Key Chain Network	Name		Cancel	ription	Ions. Ires next hop. 2. co Iters for eigrp. 1. C In AS	
> PKI Policy List				Cancel	s I< < Page 1	of 3 > > C

Imagen 13. Asignación de ACL de variable de objeto FlexConfig

Paso 3.4. Luego, configure la ACL del plano de control como entrante para la interfaz externa de la siguiente manera.

Sintaxis de la línea de comandos:

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

Esto se traduce en el siguiente ejemplo de comando, que utiliza la variable ACL creada en el paso anterior 2.3 'VAR-ACL-UNWANTED-COUNTRY' de la siguiente manera:

```
access-group $VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Así se debe configurar en la ventana de objetos de FlexConfig. A continuación, seleccione el botón Guardar para completar el objeto de FlexConfig.

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE						≵ 🥝 admin v "≵	secure
> AAA Server	Description:						Filter	
✓ Access List								
Extended	A Copy-pasting any rich text might in	troduce line breaks	s while generating CLI.	Please verify the	CLI before deploy	ment.		
Standard								
> Address Pools	Insert V 🔢 Deployment	Once		Type:	Append	•		
Application Filters	access-group \$VAR-ACL-UNWANTED-COUN	TRY in interface outsid	e control-plane				the help of TextObj	₽ _ 0,]
AS Path								Bo =
Cipher Suite List								
> Community List								¶∎ Q
> Distinguished Name							lient) and one insid	Ela Q ≣
DNS Server Group								
> External Attributes							e outside (PD client	Г а ()
							of TextObjects dn	₽ a ⊂
✓ FlexConfig	▼ Variables							B. A. E
	Name	Dimension	Default Value	Property	Override	Description	lons.	
Text Object				(Type:Name)			ires next hop. 2. co	¶∎ Q
Geolocation	VAR-ACL-UNWANTED-COUNTRY	SINGLE	ACL-UNWANTED	EXD_ACL:A	false		eters for eigro. 1. C	En α ⊒
Interface								
Key Chain							or an AS	Fi Q 📄
Network								¶a q =
> ркі							s IK < Page 1	of 3 > > C
Policy List						Cancel Save		

Imagen 14. Línea de comandos completa del objeto Flexconfig

Paso 4. Debe aplicar la configuración del objeto FlexConfig al FTD. Para ello, vaya a Dispositivos > FlexConfig.

Circle Cobjects / Object Management	Center _{Overview Analysis} Policies	Devices Objects	Integration	Deploy Q 🤩 🛔	🌣 🕝 admin v 🏻	SECURE
AAA Server Access List Extended Standard Address Pools	FlexConfig Object FlexConfig Object include device configuration command: Name	Device Management Device Upgrade NAT QoS Platform Settings FlexConfig	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting Site to Site Monitoring	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	ilter	
Application Filters AS Path	Defaul	Certificates			he help of TextObj	¶∎ Q
Cipher Suite List	Default_Inspo	action_Protocol_Disable		Disable Default Inspection.		¶∎ Q,
> Community List	Default_Insp	ection_Protocol_Enable		Enable Default Inspection.		₽ 0,
> Distinguished Name	DHCPv6_Pref	ix_Delegation_Configure		Configure one outside (PD c	lient) and one insid	Fa Q =
DNS Server Group						
> External Attributes	DHCPv6_Prefix	_Delegation_UnConfigure		Remove configuration of one	e outside (PD client	a ⊲ ∥
File List	DN	S_Configure		Configure DNS with the help	o of TextObjects dn	₽ 0, ``
✓ FlexConfig	DNS	S UnConfigure		Remove the DNS configurat	ions	R q
FlexConfig Object		_onooningalo		nonore ine onto comgarae	iono.	
Text Object	Eig	rp_Configure		Configures eigrp. 1. Configu	ires next hop. 2. co	R Q
Geolocation	Eigrp_In	terface_Configure		Configures interface parame	aters for eigrp. 1. C	₽ q
Interface	Figu	n UnConfigure		Clears eigrn configuration fr	ar an AS	R a =
Key Chain				chaine engrip deringeretren it		
Network	Eigrp_	Unconfigure_All		Clears eigrp configuration.		
> ркі				Displaying 1 - 20 of 49 row	s I< < Páge 1	of 3 > > C



Paso 4.1. A continuación, haga clic en New Policy (Nueva política) si aún no hay una FlexConfig creada para el FTD o edite la política FlexConfig existente.

Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	م 🧬	🗘 🕜 admin	cisco SECURE
											New Policy
FlexConfig Policy			Status				Last Modified				
					created. Add	a new policy					

Imagen 16. Creación de la política FlexConfig

Paso 4.2. Agregue un nombre para la nueva política FlexConfig y seleccione el FTD al que desea aplicar la ACL del plano de control creada.

Firewall Management Center	Overview Analysis Policies	Devices Objects Integration		play Q 🔮 🌣 🕜 admin 🛛 🔤 🐯 SECURE
FlexConfig Policy	New Policy		0	
	Name: FLEXCONFIG-POLICY Description: Targeted Devices Select devices to which you want to Available Devices Q. Search by name or value FTD-CONTROL-PLANE	Add to Policy		
			Save	

Imagen 17. Asignación de dispositivo de política FlexConfig

Paso 4.3. En el panel izquierdo, busque el objeto FlexConfig creado en el paso 3.2 anterior y, a continuación, agréguelo a la directiva FlexConfig haciendo clic en la flecha derecha situada en el centro de la ventana. A continuación, haga clic en el botón Save (Guardar).

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🤩 🎝 🔞 admin 🕇 🥲 SECUR	εE
FLEXCONFIG-POLICY							You have unsaved changes Preview Config Save Cance	al
							Policy Assignments (1	
	"3 Selecte	d Prenend F	FlexConfigs					
Available FlexConfig C FlexConfig Object	# Nan	ne			Description			
V User Defined								
BOBJ-FC-CONTROL-PLANE								
System Denned								
Default_DNS_Configure								
Default_Inspection_Protocol_Disable								
Default_Inspection_Protocol_Enable	Selecte	d Append F	lexConfigs					
DHCPv6_Prefix_Delegation_Configure	# Nan	ne			Description			
9 DHCPv6_Prefix_Delegation_UnConfigure								
DNS_Configure	1 OBJ	-FC-CONTROL	L-PLANE				۲. ۲.	
DNS_UnConfigure								
n Eigrp_Configure								
"i Eigrp_Interface_Configure								
Eigrp_UnConfigure								
⁰ Eigrp_Unconfigure_All								

Imagen 18. Asignación de objeto de política FlexConfig

Paso 5. Continúe con la implementación del cambio de configuración en el FTD. Para ello, navegue hasta Deploy > Advanced Deploy .

FLEXCONFIG-POLICY Enter Description Advanced Deploy FDCONTROL-PLANE * Selected Prepend FlexConfigs * Name Description * OB-I-ECONTROL-PLANE * Selected Append FlexConfigs * OB-I-ECONTROL-PLANE * OB-I-ECONTROL-PLANE * Selected Append FlexConfigs * OB-I-ECONTROL-PLANE * OB-I-I-ECONTROL-PLANE * OB-I-I-ECONTROL-PLANE * OB-I-I-ECONTROL-PLANE * OB-I-I-ECONTROL-PLANE * OB-I-I-E	cies Devices Objects Integration Deploy Q 🥩 🌣 🕢 admin 🕶 🖓	Firewall Management Center Overview Analysis Policies Devices Objects
Enter Description Available FlexConflg C FID-CONTROL-PLANE * Selected Prepend FlexConflgs * Name * OBJ-FC-CONTROL-PLANE * OBJ-FC-CONTROL-PLANE * Objection * Objection <td>Q Advanced Deploy All neel</td> <td>FLEXCONFIG-POLICY</td>	Q Advanced Deploy All neel	FLEXCONFIG-POLICY
Available FlexConfig C FlexConfig Object Available FlexConfig C FlexConfig Object * User Defined * Obfault_Inspection_Protocol_Disable * Default_Inspection_Protocol_Enable * Obfault_Inspection_Protocol_Enable * ObfAuble FlexConfigure * Obfault_Inspection_Protocol_Enable * ObfAuble Sconfigure * Obfault_Inspection_Protocol_Enable * ObfAuble Sconfigure * ObfAuble Sconfigure * Obfault_Inspection_Protocol_Enable * ObfAuble Sconfigure	FTD-CONTROL-PLANE Ready for Deployment	Enter Description
Available PrexConfig C FexConfig Object X Y Vuser Defined Description * OBJ-FC-CONTIROL-PLANE Image: Configure of the state	nfigs	Selected Prepend FlexConfigs
✓ User Defined ♥ Obs-FC-CONTROL-PLANE ♥ System Defined * Default_Inspection_Protocol_Disable * Default_Inspection_Protocol_Enable * DNS_Configure * DNS_Configure * DNS_Configure * DNS_UnConfigure * DNS_UnConfigure * DNS_UnConfigure * DNS_UnConfigure * DNS_UnConfigure	Description	Available PiexComing C FlexComing Object # Name Description
• User Defined • Default_DNS_Configure • Default_Inspection_Protocol_Disable • Default_Inspection_Protocol_Enable • DHCPv6_Prefx_Delegation_Configure • DNS_Configure • DNS_Configure • DNS_Configure • DNS_Configure • DNS_Configure		
✓ System Defined □ Default_DNS_Configure □ Default_Inspection_Protocol_Disable □ Default_Inspection_Protocol_Enable □ Default_Inspection_Protocol_Enable □ DHCPv6_Prefx_Delegation_Configure □ DHCPv6_Prefx_Delegation_UnConfigure □ DNS_Configure □ DNS_Configure □ DNS_Configure □ DNS_UnConfigure		Oser Denned Oser Denned
In Default_DNS_Configure In Default_Inspection_Protocol_Disable In device is available for deployment Image: Image		V System Defined
Configure Configure		"∄ Default_DNS_Configure
Image: Default_Inspection_Protocol_Enable Image: Selected Append FlexConfigs Image: DHCPv6_Prefix_Delegation_Configure Image: Selected Append FlexConfigs Image: DHCPv6_Prefix_Delegation_UnConfigure Image: Selected Append FlexConfigs Image: DhCPv6_Prefix_Delegation_UnConfigure Image: Selected Append FlexConfigs Image: DhCPv6_Prefix_Delegation_UnConfigure Image: Description	0 1 device is available for deployment 腔 🕫	. Default_Inspection_Protocol_Disable
Image: DHCPv6_Prefx_Delegation_Configure Image: Name Description Image: DHCPv6_Prefx_Delegation_UnConfigure Image: Name Description	hfgs	Default_Inspection_Protocol_Enable
"DNS_Configure 1 OBJ-FC-CONTROL-PLANE "DNS_UnConfigure 1 OBJ-FC-CONTROL-PLANE	Description	DHCPv6_Prefix_Delegation_Configure
DNS_UnConfigure		2 DNS Configure 1 OB LEC-CONTROL -PLANE
		DNS UnConfigure
"il Eigrp_Configure		"il Eigrp_Configure
		-® Firm Lloconfigure All

Imagen 19. Implementación avanzada de FTD

Paso 5.1. A continuación, seleccione el FTD al que desea aplicar la política FlexConfig. Si todo es correcto, haga clic en Deploy (Implementar).

þ	Fi	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🇳	🌣 🕜 admin -	cisco SECURE
1 devic	e sek Q	ected Search using device name, user name, type,	, group or statu	15								Deploy time: Esti	nate Deploy
_		Device	Modified by		Inspect Inte	erruption	Туре	Group	Last Deploy Time		Preview	Status	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:0	5 PM	B	Ready for Deploy	ment
:: •		Flex Configuration Template Policy: FLEXCONFIG-POLICY											
https://10	88 243	8.5843013/dd/#Context5mionee											

Imagen 20. Validación de implementación de FTD

Paso 5.2. A continuación, aparecerá una ventana de confirmación de implementación, agregará un comentario para realizar un seguimiento de la implementación y continúe con la implementación.

	Fir	rewall Management Center									🔅 🕜 admin 🕶 🖞	
1 devia												
			Modified by									
Ý	>	FTD-CONTROL-PLANE	admin						Sep	5, 2023 12:05 PM	Ready for Deployment	
÷.		 Flex Configuration Template Policy: FLEXCONFIG-POLICY 		Deploy	ment Con	firmation			×			
				You have	selected 1 c	levice to depl	loy					
				Deploym	ent Notes:							
				You can	optionally a	dd notes abou	ut the configur	ation changes				
									Deploy			

Imagen 21. Comentarios de implementación de FTD

Paso 5.3. Puede aparecer un mensaje de advertencia al implementar los cambios de FlexConfig. Haga clic en Implementar sólo si está completamente seguro de que la configuración de la política es correcta.



Imagen 2. Advertencia de Flexconfig de implementación de FTD

Paso 5.4. Confirme que la implementación de la política es correcta para el FTD.

	Fir	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	ৎ 🤞	🗘 🗘 adm	in ▼
	۹	Search using device name, user name, type,	, group or statu	IS									Deploy
		Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time	1	Preview	Status	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:05	5 PM		Completed	
:: •		 Flex Configuration Template Policy: FLEXCONFIG-POLICY 											



Paso 6. Si crea una nueva ACL de plano de control para el FTD o si editó una existente que está en uso activamente, es importante resaltar que los cambios de configuración realizados no se aplican a las conexiones ya establecidas al FTD; por lo tanto, debe borrar manualmente los intentos de conexión activos al FTD. Para ello, conéctese a la CLI del FTD y borre las conexiones activas de la siguiente manera.

Para borrar la conexión activa para una dirección IP de host específica:

> clear conn address 192.168.1.10 all

Para borrar las conexiones activas para una red de subred completa:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Para borrar las conexiones activas para un rango de direcciones IP:

> clear conn address 192.168.1.1-192.168.1.10 all

Nota: Se recomienda utilizar la palabra clave 'all' al final del comando clear conn address para forzar la eliminación de los intentos de conexión de fuerza bruta VPN activos al firewall seguro, principalmente cuando la naturaleza del ataque de fuerza bruta VPN está lanzando una ráfaga de intentos de conexión constantes.

Configuración de una ACL de plano de control para FTD gestionada por FDM

Este es el procedimiento que debe seguir en un FDM para configurar una ACL del plano de control para bloquear los ataques de fuerza bruta de VPN entrantes a la interfaz FTD externa:

Paso 1. Abra la GUI de FDM mediante HTTPS e inicie sesión con sus credenciales.



cisco SECURE

Cisco Secure Firewall Device Manager

Username	
Password	
	LOG IN

© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2, 1 and 3" provided with ABSCULTEY NO WARRANTY under the terms of "GNU Lesser General Public License, versions 2, 2, and version 3, 2, C

Firewall Device Manager Monitoring	Image: Constraint of the second sec	() (i) (i) (i) (i) (i) (i) (i) (i) (i) (
Model Cisco Firepower Threat Defen	Software VDB Intrusion Ruli se for VMwa 7.2.5-208 353.0 20220511-1	e Update Cloud Services High Availability State Not Registered Register Not Configured CONFIGURE
r Inside Net	0/1 Cisco Firepower Threat Defense for VMware () 0/0 0/1 () 0/0 0/1	MGMT MGMT
Interfaces Connected Enabled 3 of 3 View All Interfaces	Routing There are no static routes yet View Configuration	Updates System Settings Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds Management Access Logging Settings View Configuration > Troubleshoot No files created yet Management Interface Hostname

Paso 2. Debe crear una red de objetos. Para ello, vaya a Objetos:

Imagen 25. Panel principal de FDM

Paso 2.1. En el panel izquierdo, seleccione Redes y, a continuación, haga clic en el botón '+' para crear un nuevo objeto de red.

Firewall Device Manager	Monitoring Policies Objects Device: fireport	wer (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)
Object Types ←	Network Objects and Groups	
C Networks	6 objects	▼ Filter + 💭
S Ports		Preset filters: System defined, User defined
🔒 Security Zones	# NAME	TYPE VALUE ACTIONS
Application Filters	1 IPv4-Private-10.0.08	NETWORK 10.0.0/8
	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12
C URLS	3 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16
Geolocations	4 any-ipv4	NETWORK 0.0.0.0/0
Syslog Servers	5 any-ipv6	NETWORK ::/0
🔑 IKE Policies	6 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-
👍 IPSec Proposals		192.100.0.0~10
Secure Client Profiles		
State Identity Sources		
🔒 Secret Keys		

Imagen 26. Creación de objetos

Paso 2.2. Agregue un nombre para el objeto de red, seleccione el tipo de red para el objeto, agregue la dirección IP, la dirección de red o el rango de IP para que coincidan con el tráfico que debe denegarse al FTD. A continuación, haga clic en el botón Aceptar para completar la red de objetos.

- En este ejemplo, la red de objetos configurada está pensada para bloquear los ataques de fuerza bruta de VPN que provienen de la subred 192.168.1.0/24.

Firewall Device Manager	Monitoring Polici	Add Network Object
Object Types 🤟	Network Obje	Name
C Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY
Security Zones	N NAME	Description Actions
🐔 Application Filters	1 IPv4-Private-Al	e=172.16.0.0-12, IPv4-Private=
C ² URLs	2 IPv4-Private-10	Туре
Geolocations	3 IPv4-Private-11	Network Host FQDN Range
Syslog Servers	4 IPv4-Private-19	Network 1923 Fe 1 0/24
IKE Policies	5 any-ipv4	e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60
🐴 IPSec Proposals	6 any-ipv6	
Secure Client Profiles		CANCEL OK
Surces		
L Users		
A Certificates		
🔒 Secret Keys		

Imagen 27. Agregar objeto de red

Paso 3. A continuación, debe crear una lista de control de acceso ampliada; para ello, vaya a la ficha Device (Dispositivo) del menú superior.

Firewall Device Manager	Monitoring Policies Objects Device: firepov	ver	cisco SECURE
Object Types ←	Network Objects and Groups		
C Networks	7 objects	Tilter	+ 🔍
S Ports		Preset filters: System.defined, User.defined	
Security Zones	H NAME	TYPE VALUE	ACTIONS
Application Filters	1 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private- 192.168.0.0-16	
🖉 URLs	2 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8	
Geolocations	3 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12	
Svslog Servers	4 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16	
	5 any-ipv4	NETWORK 0.0.0.0/0	
INE POlicies	6 any-ipv6	NETWORK ::/0	
IPSec Proposals	7 OBJ-NET-UNWANTED-COUNTRY	NETWORK 192.168.1.0/24	
Secure Client Profiles			
Surces			
👤 Users			
🙎 Certificates			
Secret Keys			

Imagen 28. Página Configuración del dispositivo

Paso 3.1. Desplácese hacia abajo y seleccione Ver configuración en el cuadro Configuración avanzada como se indica a continuación.

Firewall Device Manager Monitoring	Image: Specific constraints Policies Objects Device: firepower	 (2) (3) (4) (4) (5) (6) (7) (7)	admin Administrator ~ tisto SECURE
	оло С		
Interfaces Connected Enabled 3 of 3 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service
Smart License Evaluation expires in 89 days Tier: Not selected (Threat Defense Virtual - Variable)	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	DNS Server Management Interface Hostname Time Services See more
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Requires RA VPN license No connections 1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

Imagen 29. Configuración avanzada de FDM

Paso 3.2. A continuación, en el panel izquierdo, navegue hasta CLI inteligente > Objetos y haga clic en CREAR OBJETO CLI INTELIGENTE.

Firewall Device Manager	Monitoring	Policies	Objects	Device: firepower	6) 🚑	2	* * *	admin Administrator	 dialla secure 	
Advanced ← Configuration	Device Summa Objects	ary									
Smart CLI										+	
Objects	•	NAME		ТҮРЕ	DESCRIPTION				ACTIONS		
FlexConfig					There are no Smart CLI of	objects yet.	act				
FlexConfig Objects						BIECT	1				
FlexConfig Policy					CREATE SMART GETO	DJEGI	1				

Imagen 30. Objetos CLI inteligentes

Paso 3.3. Agregue un nombre para la ACL extendida que desea crear, seleccione Lista de acceso extendida en el menú desplegable de la plantilla CLI y configure las ACE requeridas mediante el objeto de red creado en el paso anterior 2.2. A continuación, haga clic en el botón Aceptar para completar la ACL.

Firewall Devic			sco SECURE
Advanced Configuration	Name	Description	
Smart CLI	ACL-UNWANTED-COUNTRY CLI Template		ACTIONS
FlexConfig	Extended Access List	Show disabled	Reset
FlexConfig Objects	1 access-list ACL-UMAWITED-COUNTRY extended 2 configure access-list-entry deny v 3 deny network source [083-MET-UMAMITED-COUNTRY x v] destine 4 configure deny port any v	nation [<u>any-lpu4 X</u> ~]	
	○ 5 deny port source NNY destination NNY ○ 6 configure logging default ∨ ○ 7 default log set log-level INFORMATIONAL log-interval	300	
		CANCEL	

Imagen 31. Creación de ACL ampliada

Nota: Si necesita agregar más ACE para la ACL, puede hacerlo pasando el ratón sobre la izquierda de la ACE actual; luego aparecerán tres puntos en los que se puede hacer clic. Haga clic en ellos y seleccione Duplicar para agregar más ACE.

Paso 4. A continuación, debe crear un objeto FlexConfig; para ello, vaya al panel izquierdo, seleccione FlexConfig > Objetos FlexConfig y haga clic en CREAR OBJETO FLEXCONFIG.

Firewall Device Mana	ger Monitoring	Ø Policies	Objects	Device: firepower	(Σ_{-})) (?)	:	admin Administrator	~	cisco SECURE	
Advanced ← Configuration	Device Summ FlexCor	nary Ifig Object	S									
Smart CLI						T	Filter				+	
Objects	•	NAME		DESCRIPTION				ACTI	ONS			
FlexConfig FlexConfig Objects FlexConfig Policy				There a Start by cn	re no FlexConfig obj lating the first FlexCo	iects yet. onfig object. IECT						

Imagen 32. Objetos FlexConfig

Paso 4.1. Agregue un nombre para el objeto FlexConfig para crear y configurar la ACL del plano de control como entrante para la interfaz externa de la siguiente manera.

```
Sintaxis de la línea de comandos:
```

```
access-group "ACL-name" in interface "interface-name" control-plane
```

Esto se traduce en el siguiente ejemplo de comando, que utiliza la ACL extendida creada en el paso anterior 3.3 'ACL-UNWANTED-COUNTRY' de la siguiente manera:

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Así se debe configurar en la ventana de objetos de FlexConfig. A continuación, seleccione el botón Aceptar para completar el objeto de FlexConfig.

Firewall Device Mana	ager Monitoring					admin Administrator Cisco SECURE
Advanced ← Configuration	Device Sur FlexCo	Name	ect		U ×	
Smart CLI		OBJ-FC-CONTROL-PLANE				+
Objects	8 - C	Description			1	CTIONS
FlexConfig		Variables				
FlexConfig Objects		ADD VARIABLE				
The only		Template	TED-COUNTRY in interface outsid	Expand control-plane	🗘 Reset	
					- D. Barris	
		no access-group ACL-UN	WANTED-COUNTRY in interface out	side control-plane	Çî Reset	
				CANCEL	OK	
				OF OTHER		

Imagen 3. Creación de objetos FlexConfig

Paso 5. Proceda a crear una política FlexConfig. Para ello, navegue hasta Flexconfig > Política FlexConfig, haga clic en el botón '+' y seleccione el objeto FlexConfig que se creó en el paso 4.1 anterior.



Imagen 34. Política FlexConfig

Paso 5.1. Verifique que la vista previa de FlexConfig muestre la configuración correcta para la ACL del plano de control creada y haga clic en el botón Save (Guardar).

Firewall Device Manager	Monitoring Policies Objects Device: firepower	() () () () () () () () () () () () () (
Advanced ← Configuration	Device Summary FlexConfig Policy	
Smart CLI	Group List	Preview
Objects	OBJ-FC-CONTROL-PLANE	1 access-group ACL-UMWANTED-COUNTRY in interface outside control-plane
FlexConfig FlexConfig Objects		
FlexConfig Policy		
	OWE	

Imagen 35. Vista previa de política FlexConfig

Paso 6. Implemente los cambios de configuración en el FTD que desee proteger contra los ataques de fuerza bruta VPN. Para ello, haga clic en el botón Implementación del menú superior, valide que los cambios de configuración que desea implementar son correctos y, a continuación, haga clic en IMPLEMENTAR AHORA.

Firewall Device Manager		istrator v ulturle SECURE	
Advanced ← Configuration	Pending Changes Last Deployment Completed Successfully 05 Sep 2023 02:27 PM. <u>See Deployment History</u>	• ×	
Smart CLI	Deployed Version (05 Sep 2023 02:27 PM)	Pending Version C LEGEND	
Objects	Network Object Added: OBJ-NET-UNWANTED-COUNTRY		
FlexConfig		subType: Network CLAND value: 2.2.2.0/24 isSystemDefined: false dmsResolution: IPV4_ND_IPV6 description:	
FlexConfig Objects	-	name: 083-NET-UNMANTED-COUNTRY	
FlexConfig Policy	SelexConfig Policy Edited: default-group		
	flexConfigObjects: -	083-FC-CONTROL-PLANE	
	Extended Access List Added: ACL-UNWANTED-COUNTRY		
	- - - entries[0].sourceNetworks:	entries[0].logging: DEFAULT entries[0].action: DENY name: ACL-UNWANTED-COUNTRY	
	MORE ACTIONS V	CANCEL DEPLOY NOW	

Imagen 36. Implementación pendiente

Pasc	6.1.	Valide of	oue la im	plementación	de la	política se	realice	correctamente.
1 450	, 0	vanaci	que la litt	picificitic	uc iu		realiee	concolumente.

Firewall Device Ma	Manager Pending Changes @ X	n vibidi SECURE
Advanced ← Configuration	*	
Smart CLI		
Objects	There are no Pending Changes yet. Nothing to deploy.	<> Expand
FlexConfig	List sussessful deployment upp on 05 Cap 2022 11:00 AM	in interface outside
FlexConfig Objects	You can see what was deployed in previous jobs in the Deployment History	
FlexConfig Policy		
	ox Contraction of the second se	
	SAVE	

Imagen 37. Implementación correcta

Paso 7. Si crea una nueva ACL de plano de control para el FTD o si editó una existente que está en uso activamente, es importante resaltar que los cambios de configuración realizados no se aplican a las conexiones ya establecidas al FTD; por lo tanto, debe borrar manualmente los intentos de conexión activos al FTD. Para ello, conéctese a la CLI del FTD y borre las conexiones activas de la siguiente manera.

Para borrar la conexión activa para una dirección IP de host específica:

> clear conn address 192.168.1.10 all

Para borrar las conexiones activas para una red de subred completa:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Para borrar las conexiones activas para un rango de direcciones IP:

> clear conn address 192.168.1.1-192.168.1.10 all

Nota: Se recomienda utilizar la palabra clave 'all' al final del comando clear conn address para forzar la eliminación de los intentos de conexión de fuerza bruta VPN activos al firewall seguro, principalmente cuando la naturaleza del ataque de fuerza bruta VPN está lanzando una ráfaga de intentos de conexión constantes.

Configuración de una ACL de plano de control para ASA mediante CLI

Este es el procedimiento que debe seguir en una CLI ASA para configurar una ACL del plano de control para bloquear los ataques de fuerza bruta de VPN entrante a la interfaz externa:

Paso 1. Inicie sesión en el firewall ASA seguro a través de CLI y obtenga acceso al 'configure terminal' de la siguiente manera.

asa# configure terminal

Paso 2. Utilice el siguiente comando para configurar una ACL extendida para bloquear una dirección IP de host o una dirección de red para el tráfico que debe bloquearse en el ASA.

- En este ejemplo, crea una nueva ACL llamada 'ACL-UNWANTED-COUNTRY' y la entrada ACE configurada bloqueará los ataques de fuerza bruta VPN que provienen de la subred 192.168.1.0/24.

asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

Paso 3. Utilice el siguiente comando access-group para configurar la ACL 'ACL-UNWANTED-COUNTRY' como ACL de plano de control para la interfaz externa de ASA.

```
asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Paso 4. Si crea una nueva ACL del plano de control o si editó una existente que está en uso activamente, es importante resaltar que los cambios de configuración realizados no se aplican a las conexiones ya establecidas con el ASA, por lo tanto, necesita borrar manualmente los intentos de conexión activos con el ASA. Para esto, borre las conexiones activas de la siguiente manera.

Para borrar la conexión activa para una dirección IP de host específica:

asa# clear conn address 192.168.1.10 all

Para borrar las conexiones activas para una red de subred completa:

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

Para borrar las conexiones activas para un rango de direcciones IP:

asa# clear conn address 192.168.1.1-192.168.1.10 all

Nota: Se recomienda utilizar la palabra clave 'all' al final del comando clear conn address para forzar la eliminación de los intentos de conexión de fuerza bruta VPN activos al firewall seguro, principalmente cuando la naturaleza del ataque de fuerza bruta VPN está lanzando una ráfaga de intentos de conexión constantes.

Configuración alternativa para bloquear los ataques de firewall seguro mediante el comando 'shun'

En caso de que exista una opción inmediata para bloquear los ataques al firewall seguro, puede utilizar el comando 'shun'. El comando hunpermite bloquear las conexiones de un host atacante.

- Una vez que rechaza una dirección IP, todas las conexiones futuras de la dirección IP de origen

se descartan y se registran hasta que la función de bloqueo se elimina manualmente.

- La función de bloqueo de theshuncommand se aplica independientemente de si una conexión con la dirección de host especificada está actualmente activa o no.

- Si especifica la dirección de destino, los puertos de origen y destino y el protocolo, descartará la conexión coincidente y rechazará todas las conexiones futuras de la IP de origen

dirección; todas las conexiones futuras se rechazan, no sólo las que coinciden con estos parámetros de conexión específicos.

- Solo puede tener uncomando hunpor dirección IP de origen.

- Debido a que el comando hunse utiliza para bloquear ataques dinámicamente, no se muestra en la configuración del dispositivo de defensa contra amenazas.

- Siempre que se elimina una configuración de interfaz, también se eliminan todas las rechazos que están conectados a esa interfaz.

- Sintaxis del comando Shun:

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

- Para inhabilitar un shun, utilice la forma no de este comando:

no shun source_ip [vlan vlan_id]

Para rechazar una dirección IP de host, proceda como se indica a continuación para el firewall seguro. En este ejemplo, el comando 'shun' se utiliza para bloquear los ataques de fuerza bruta de VPN que provienen de la dirección IP de origen 192.168.1.10.

Ejemplo de configuración de FTD.

Paso 1. Inicie sesión en el FTD a través de CLI y aplique el comando shun de la siguiente manera.

<#root>

>

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Paso 2. Puede utilizar los siguientes comandos show para confirmar las direcciones IP rechazadas en el FTD y para monitorear los recuentos de aciertos rechazados por dirección IP:

<#root>

```
>
show shun
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
>
show shun statistics
diagnostic=0FF, cnt=0
outside=0N, cnt=0
Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

Ejemplo de configuración para ASA

Paso 1. Inicie sesión en ASA a través de CLI y aplique el comando shun de la siguiente manera.

<#root>
asa#
shun 192.168.1.10
Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Paso 2. Puede utilizar los siguientes comandos show para confirmar las direcciones IP rechazadas en el ASA y para monitorear los recuentos de aciertos rechazados por dirección IP:

<#root>
asa#
show shun
shun (outside) 192.168.1.10 0.0.0.0 0 0 0

asa#

show shun statistics

outside=ON, cnt=0
inside=OFF, cnt=0
dmz=OFF, cnt=0
outside1=OFF, cnt=0
mgmt=OFF, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:01:39)

Nota: Para obtener más información sobre el comando secure firewall shun, consulte la <u>Referencia de Comandos de Cisco Secure Firewall Threat Defence</u>

Verificación

Para confirmar que la configuración ACL del plano de control está en su lugar para el firewall seguro, proceda de la siguiente manera:

Paso 1. Inicie sesión en el firewall seguro a través de CLI y ejecute los siguientes comandos para confirmar que se ha aplicado la configuración de ACL del plano de control.

Ejemplo de salida del FTD gestionado por el CSP:

<#root>

>

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

>

show running-config access-group

OUTPUT OMITTED FOR BREVITY access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

Ejemplo de salida del FTD gestionado por FDM:

<#root>

> show running-config object id OBJ-NET-UNWANTED-COUNTRY

object network OBJ-NET-UNWANTED-COUNTRY
subnet 192.168.1.0 255.255.255.0

show running-config access-list ACL-UNWANTED-COUNTRY

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default
```

> show running-config access-group

```
***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Ejemplo de salida para ASA:

<#root>

asa#

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

asa#

show running-config access-group

OUTPUT OMITTED FOR BREVITY access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

Paso 2. Para confirmar que la ACL del plano de control está bloqueando el tráfico requerido, utilice el comando packet-tracer para simular una conexión TCP 443 entrante con la interfaz externa del firewall seguro, luego utilice el comando show access-list <acl-name> , el conteo de aciertos de la ACL debe incrementarse cada vez que la ACL del plano de control bloquea una conexión VPN de fuerza bruta con el firewall seguro:

- En este ejemplo, el comando packet-tracer simula una conexión TCP 443 entrante originada en el host 192.168.1.10 y destinada a la dirección IP externa de nuestro firewall seguro. El resultado del 'packet-tracer' confirma que el tráfico se está descartando y el resultado del 'show access-list' muestra los incrementos de conteo de aciertos para nuestra ACL del plano de control en su lugar:

Ejemplo de salida para FTD

<#root>

>

>

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443 Phase: 1 Type: ACCESS-LIST Subtype: log Result: DROP Elapsed time: 21700 ns Config: Additional Information: Result: input-interface: outside(vrfid:0) input-status: up input-line-status: up Action: drop Time Taken: 21700 ns Drop-reason: (acl-drop) Flow is denied by configured rule , Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA > show access-list ACL-UNWANTED-COUNTRY access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (

hitcnt=1

) 0x142f69bf

Ejemplo de salida para ASA

<#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 19688 ns Config: Implicit Rule Additional Information: MAC Access list

Phase: 2

```
Type:
ACCESS-LIST
Subtype: log
Result: DROP
Elapsed time: 17833 ns
Config:
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
Action: drop
Time Taken: 37521 ns
Drop-reason: (acl-drop) Flow is denied by configured rule
, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA
asa#
show access-list ACL-UNWANTED-COUNTRY
access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any
(hitcnt=1)
 0x9b4d26ac
```

Nota: Si se implementa una solución RAVPN como Cisco Secure Client VPN en el firewall seguro, se podría realizar un intento real de conexión al firewall seguro para confirmar que la ACL del plano de control funciona como se esperaba para bloquear el tráfico requerido.

Errores relacionados

 ENH | Conexiones de AnyConnect Client basadas en geolocalización: ID de bug de Cisco CSCvs65322

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).