Konfigurieren von Zugriffskontrollrichtlinien auf Kontrollebene für sicheren Schutz vor Bedrohungen durch Firewalls und ASA

Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
<u>Hintergrundinformationen</u>
Konfigurieren
Konfigurationen
Konfigurieren einer von FMC verwalteten Kontrollebenen-ACL für FTD
Konfigurieren einer von FDM verwalteten Kontrollebenen-ACL für FTD
Konfigurieren einer Kontrollebenen-ACL für ASA mit CLI
Alternative Konfiguration zum Blockieren von Angriffen für eine sichere Firewall mithilfe des Befehls "shun"
Überprüfung
Verwandte Fehler

Einleitung

In diesem Dokument wird der Prozess zur Konfiguration von Zugriffsregeln auf Kontrollebene für die Secure Firewall Threat Defense- und die Adaptive Security Appliance (ASA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sichere Firewall-Bedrohungsabwehr (FTD)
- Sicherer Firewall-Gerätemanager (FDM)
- Secure Firewall Management Center (FMC)
- Sichere Firewall ASA
- Zugriffskontrollliste (ACL)
- FlexConfig

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Secure Firewall Threat Defense Version 7.2.5
- Secure Firewall Manager Center Version 7.2.5
- Secure Firewall Device Manager Version 7.2.5
- Secure Firewall ASA Version 9.18.3

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

Hintergrundinformationen

Der Datenverkehr durchläuft in der Regel eine Firewall und wird zwischen Datenschnittstellen weitergeleitet. In manchen Fällen ist es sinnvoll, den Datenverkehr, der für die sichere Firewall bestimmt ist, zu verweigern. Die sichere Cisco Firewall kann mithilfe einer Zugriffskontrollliste auf Kontrollebene (Control-Plane Access Control List, ACL) den einsatzbereiten Datenverkehr beschränken. Ein Beispiel für den Fall, dass eine Kontrollebenen-ACL nützlich sein kann, wäre die Kontrolle darüber, welche Peers einen VPN-Tunnel (Site-to-Site oder Remote Access VPN) zur sicheren Firewall einrichten können.

Sichere Firewall durch einsatzbereiten Datenverkehr

Der Datenverkehr durchläuft in der Regel Firewalls von einer Schnittstelle (eingehend) zu einer anderen Schnittstelle (ausgehend). Dies wird als Durchgangsverkehr bezeichnet und wird von den Zugriffskontrollrichtlinien (ACP) und den Vorfilterregeln verwaltet.



Bild 1. Beispiel für Datenverkehr durch die Box

Sicherer, sofort einsatzbereiter Firewall-Datenverkehr

Es gibt andere Fälle, in denen der Datenverkehr direkt an eine FTD-Schnittstelle (Site-to-Siteoder Remote Access-VPN) gerichtet ist. Dies wird als einsatzbereiter Datenverkehr bezeichnet und von der Kontrollebene dieser Schnittstelle verwaltet.



Bild 2. Beispiel für standortunabhängigen Datenverkehr

Wichtige Überlegungen zu ACLs auf Kontrollebene

- Ab FMC/FTD Version 7.0 muss eine ACL der Kontrollebene mit FlexConfig konfiguriert werden, wobei dieselbe Befehlssyntax wie für die ASA verwendet wird.
- Das Schlüsselwort "control-plane" wird an die Zugriffsgruppenkonfiguration angefügt, die den Datenverkehr "zur" sicheren Firewall-Schnittstelle erzwingt. Ohne das an den Befehl angehängte Wort für die Kontrollebene würde die ACL den Datenverkehr "durch" die sichere Firewall einschränken.
- Eine Kontrollebenen-ACL schränkt den eingehenden SSH-, ICMP- oder TELNET-Verkehr zu einer sicheren Firewall-Schnittstelle nicht ein. Diese werden gemäß den Plattformeinstellungsrichtlinien verarbeitet (zugelassen/abgelehnt) und haben eine höhere Priorität.
- Eine ACL auf Kontrollebene beschränkt den Datenverkehr "zur" sicheren Firewall selbst, während die Zugriffskontrollrichtlinie für FTD oder die normalen ACLs für ASA den Datenverkehr "durch" die sichere Firewall steuert.
- Im Gegensatz zu einer normalen ACL wird am Ende der ACL kein implizites "deny" (Verweigern) angezeigt.
- Zum Zeitpunkt der Erstellung dieses Dokuments kann die FTD-Standortbestimmung nicht verwendet werden, um den Zugriff auf das FTD einzuschränken.

Konfigurieren

Im nächsten Beispiel versucht eine Gruppe von IP-Adressen aus einem bestimmten Land, VPN-Brute-Force-Angriffe auf das Netzwerk auszuführen, indem sie versucht, sich beim FTD RAVPN anzumelden. Die beste Option zum Schutz des FTD vor diesen VPN-Brute-Force-Angriffen ist die Konfiguration einer Kontrollebenen-ACL, um diese Verbindungen zur externen FTD-Schnittstelle zu blockieren.

Konfigurationen

Konfigurieren einer von FMC verwalteten Kontrollebenen-ACL für FTD

Mit diesem Verfahren müssen Sie in einem FMC eine Kontrollebenen-ACL konfigurieren, um eingehende VPN-Brute-Force-Angriffe auf die externe FTD-Schnittstelle zu blockieren:

Schritt 1: Öffnen Sie die grafische Benutzeroberfläche (GUI) von FMC über HTTPS, und melden Sie sich mit Ihren Anmeldeinformationen an.

	cisco SECURE	
	Secure Firewall	
	Management	
man sa di San	Center	
	Username	
	Password	
	Log In	
		N 0 10 000
*		

Bild 3. FMC-Anmeldeseite

Schritt 2: Sie müssen eine erweiterte Zugriffskontrollliste erstellen. Navigieren Sie dazu zu Objekte > Objektverwaltung.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q <mark>6</mark> 🌣 🥐	admin • •dt+dt+ SECURE
Summary Dashboard (watch.dashboard)					Object M Intrusion	lanagement Rules			Reporting
Provides a summary of activity on the appliance									
Network × Threats Intrusion Events	Status Ge	eolocation	QoS -					Show the Last 1 hour	• 11
Unique Applications over Time		× • T	op Web Applic	ations Seen				Top Client Applications Seen	
No Data				٩	No Data			No Data	
		Last	ipdated 2 minute	is ago				Last updated 2 minutes ago	
Traffic by Application Risk	_	× • T	op Server App	lications See	n		- ×	▶ Top Operating Systems Seen	- ×

Abbildung 4: Objektmanagement

Schritt 2.1: Navigieren Sie im linken Bereich zu Access List > Extended (Zugriffsliste > Erweitert), um eine erweiterte ACL zu erstellen.

Firewall Managemer	nt Center Overview Ana It	lysis Policies Dev	vices Objects	Integration	Deploy	오 🧬 🌣 📀 admin	• dialis SECURE
 AAA Server Access List Extended Standard 	Network A network object represents one or network discovery rules, event sear	more IP addresses. Networl ches, reports, and so on.	k objects are used in	various places, includi	Add Network ng access control policies, network	Filter Show Unused (k variables, intrusion rules, intrusion rules), intrusion rules, intrusion	Dbjects Ientity rules,
> Address Pools	Name			Value	т	ype Over	ide
Application Filters AS Path	any			0.0.0.0	0/0 G	àroup	Q ≣ ₿
Cipher Suite List	any-ipv4			0.0.0.0	0/0 N	letwork	Q ≣ ₿
> Community List	any-ipv6			::/0	н	lost	Q ≣ ₿
 Distinguished Name DNS Server Group 	IPv4-Benchmark-Tests			198.18	8.0.0/15 N	letwork	Q ≣ ₿
> External Attributes	IPv4-Link-Local			169.25	54.0.0/16 N	letwork	۵ 🗑 🚯
File List	IPv4-Multicast			224.0.	.0.0/4 N	letwork	Q ≣ ₿
Geolocation	IPv4-Private-10.0.0.0-8			10.0.0).0/8 N	letwork	۹ 🗑 🕷
Interface	IPv4-Private-172.16.0.0-12			172.10	6.0.0/12 N	letwork	ୟ 🗎 👪
Key Chain	IPv4-Private-192.168.0.0-16			192.10	58.0.0/16 N	letwork	۵ 🗑 🚯
> PKI	IPv4-Private-All-RFC1918			10.0.0 172.16 192.16	0.0/8 5.0.0/12 G 58.0.0/16	Group	ଦ ≣ ୫
Policy List Port					Displaying 1 -	- 14 of 14 rows K < Page	iof 1 > > C

Bild 5. Erweitertes ACL-Menü

Schritt 2.2: Wählen Sie dann Erweiterte Zugriffsliste hinzufügen aus.

Firewall Managemen Objects / Object Management	t Center _{Overview}	Analysis Polie	ies Devices	Objects	Integration	Deploy	९ 🌓 🌣 (🗿 admin 🕶 📔	cisco SECURE
> AAA Server	Extended					Add Extended Access	s List ् २ Filter		
✓ Access List	An essent list chiest clea l		trol list (ACI) color	to the traffic to	udiah a sandaa udil annhi. Cta	andard Identifies troffic be	and on destination	oddraes oshi i	Identifies
Extended	traffic based on source and	destination address an	d ports. Supports IP	v4 and IPv6 ad	dresses. You use these object	s when configuring particu	ular features, such	as route maps.	identines
Standard									
> Address Pools	Name					Value		Override	
Application Filters					o records to display				
AS Path					o records to display				
Cipher Suite List									
> Community List									
Distinguished Name									
DNS Server Group									
> External Attributes									
File List									
> FlexConfig									
Geolocation									
Interface									
Key Chain									
Network									
> ркі									
Policy List									7
Port						No	data to display	< Page 1	of1>>C
> Prefix List									

Bild 6. Erweiterte ACL hinzufügen

Schritt 2.3: Geben Sie einen Namen für die erweiterte Zugriffskontrollliste ein, und klicken Sie dann auf die Schaltfläche Hinzufügen, um einen Zugriffskontrolleintrag (ACE) zu erstellen:

Firewall Mana Objects / Object M	agement Ce anagement	nter	Overview	Analysis Po	licies Device:	s Objects	Integration		Deploy	۹ (6 \$	🛛 admin 🕶 🛛	cisco SECURE
> AAA Server	New Exte	nded Acc	ess List Ob;	ject									
 Access List Extended 	Name											dress only. oute maps	dentifies
Standard Address Pools	Entries (0)	ANTED-CO	UNTRY									Override	
Application Filters AS Path											Add		
Cipher Suite List Community List	Sequence	Action	Source	Source	Port	Destination	Destination I	Port Applic	ation				
Distinguished Name DNS Server Group	No record	s to display											
> External Attributes													
> FlexConfig													
Geolocation	Allow Ov	errides											
Key Chain Network											Save		
> РКІ Policy List													
Port									No	data to	display I<	< Page 1	of 1 > > C

Bild 7. Erweiterte ACL-Einträge

Schritt 2.4: Ändern Sie die ACE-Aktion in Block (Blockieren), fügen Sie dann das Quellnetzwerk hinzu, damit es mit dem Datenverkehr übereinstimmt, der dem FTD verweigert werden muss, und belassen Sie das Zielnetzwerk auf Any (Beliebig), und klicken Sie auf die Schaltfläche Add (Hinzufügen), um den ACE-Eintrag zu vervollständigen:

- In diesem Beispiel blockiert der konfigurierte ACE-Eintrag Brute-Force-VPN-Angriffe aus dem Subnetz 192.168.1.0/24.

Firewa Objects /	Action: Block		
	Logging:		
× Access List	Default 🔻		
Extended	Log Level:		Identifies
Standard	Informational 👻		
> Address Pools	Log Interval:		
Application Filt	300 Sec.		/ = M
AS Path	Network Port 🕕 Application		× • 00
Cipher Suite Lit			
> Community List	Available Networks C + Sou	urce Networks (1) Destination Networks (0)	
> Distinguished N	Q Search by name or value	92.168.1.0/24	
DNS Server Gre	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	inter an IP address Add Enter an IP address Add	
> ркі			
Policy List			
Port			of 1 > > C
> Prefix List		Cancel	

Bild 8. Abgelehnte Netzwerke

Schritt 2.5: Falls Sie weitere ACE-Einträge hinzufügen müssen, klicken Sie erneut auf die Schaltfläche Hinzufügen und wiederholen Sie Schritt 2.4. Klicken Sie anschließend auf Save (Speichern), um die ACL-Konfiguration abzuschließen.

Firewall Managemen Objects / Object Management	Edit Exten	ded Acc	ess List Object					0	cisco SECURE
> AAA Server ~ Access List	Name ACL-UNW/	ANTED-CC	DUNTRY						
Extended	Entries (1)								Identifies
Standard								Add	
> Address Pools									
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		2 E M
AS Path	1	Block	192.168.1.0/24					11	× 00
Cipher Suite List									
> Community List									
> Distinguished Name									
DNS Server Group									
> External Attributes									
File List	Allow Ov	errides							
> FlexConfig									
Geolocation								Save	
Interface									
Key Chain									
Network									
> ркі									
Policy List									
Port							Displaying 1 - 1 of 1 rows	IC < Page 1	of 1 > > C
> Prefix List									

Bild 9. Abgeschlossene erweiterte ACL-Einträge

Schritt 3: Anschließend müssen Sie ein Flex-Config-Objekt konfigurieren, um die Kontrollebenen-ACL auf die externe FTD-Schnittstelle anzuwenden. Navigieren Sie dazu zum linken Bereich, und wählen Sie die Option FlexConfig > FlexConfig Object (FlexConfig > FlexConfig-Objekt) aus.

Ē	Firewall Management	t Center	Overview	Analysis	Policies	Devices	Objects	Integration	De	sploy Q	ې 🍨	🕐 admin 🕶 🛛	cisco SECURE
> aa	A Server	Extended	d						Add Extended	Access Lis	د الع	r	
~ Acc	ess List												
	Extended	An access list traffic based or	object, also kno n source and de	own as an acce estination addr	ess control list ess and ports	t (ACL), select . Supports IPv	s the traffic to 4 and IPv6 ad	which a service will apply. St dresses. You use these objec	tandard-Identifies to ts when configuring	affic based particular f	on destinatio eatures, sucl	n address only h as route maps	. Identifies s.
	Standard												
> Ad	dress Pools	Name							Value			Override	
Ap	olication Filters	ACI-UNWANT	ED-COUNTRY										/ = A
AS	Path	ACE ONTAIN											
Cip	her Suite List												
> co	mmunity List												
> Dis	tinguished Name												
DN	S Server Group												
> Ext	ernal Attributes												
File	List												
~ Fle	Config												
	FlexConfig Object												
	Text Object												
Ge	blocation												
Inte	rface												
Key	Chain												
Net	work												
> ркі									Dis	playing 1 - 1	of 1 rows	C < Page 1	of 1 > > C
Pol	icy List												

Bild 10. Menü "FlexConfig-Objekt"

Schritt 3.1: Klicken Sie auf FlexConfig Objekt hinzufügen.

Firewall Manageme	nt Center Overview	Analysis Po	licies Devices	Objects Integratio	n (eploy Q 🧬 f	⊁ 🕜 admin v │ ;	SECURE
 > AAA Server > Access List Extended Standard 	FlexConfig Object include d	Ct ievice configuration c	ommands, variables, a	nd scripting language instr	Add Flex	Config Object Q ces.	Filter	
> Address Pools	Name				Des	ription		
Application Filters AS Path	Default_DNS_Configure				Con	igure Default DNS with	the help of TextObj	¶∎ Q
Cipher Suite List	Default_Inspection_Protocol	_Disable			Disa	ble Default Inspection.		¶a ()
Community List	Default_Inspection_Protocol	_Enable			Enat	le Default Inspection.		¶∎ Q 🗎
> Distinguished Name	DHCPv6_Prefix_Delegation_	Configure			Con	igure one outside (PD o	lient) and one insid	a q
External Attributes	DHCPv6_Prefix_Delegation_	UnConfigure			Rem	ove configuration of on	e outside (PD client	¶∎ Q 🗎
File List	DNS_Configure				Con	igure DNS with the help	o of TextObjects dn	a Q =
✓ FlexConfig	DNS_UnConfigure				Rem	ove the DNS configurat	ions.	R Q
FlexConfig Object	Firm Orafaura				0		and have 0 and	
Text Object	Eigrp_Configure				Con	igures eigrp. 1. Contigu	ires next hop. 2. co	a d
laterface	Eigrp_Interface_Configure				Con	igures interface param	eters for eigrp. 1. C	α -
Key Chain	Eigrp_UnConfigure				Clea	rs eigrp configuration for	or an AS	¶∎ Q
Network	Eigrp_Unconfigure_All				Clea	rs eigrp configuration.		Pa Q =
> ркі					Disp	laying 1 - 20 of 48 row	s I< < Page 1	of 3 > > C

Bild 11. Flexconfig-Objekt hinzufügen

Schritt 3.2: Fügen Sie einen Namen für das FlexConfig-Objekt hinzu, und fügen Sie dann ein ACL-Richtlinienobjekt ein. Wählen Sie dazu Einfügen > Richtlinienobjekt einfügen > Erweitertes ACL-Objekt.

Firewall Manageme	Name:	s 🙆 admin x 🕙	who are cupr
Objects / Object Manageme	OBJ-FC-CONTROL-PLANE		
> AAA Server	Description:	Filter	
✓ Access List			
Extended	▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.		
Standard	Insert x Denkument: Once x Tune: Annend x		
> Address Pools	Insert Policy Object b Taxt Object		
Application Filters	Insert System Variable Network	the help of TextObj	¶a Q
AS Path	Insert Secret Key Security Zones		E o E
Cipher Suite List	Standard ACL Object		1
> Community List	Extended ACL Object		η α 📄
> Distinguished Name	Route Map	lient) and one insid	₽ 0, 1
DNS Server Group		p outside (PD elient	Bo E
> External Attributes		e outside (PD client	
File List		of TextObjects dn	¶∎ Q
 FlexConfig 	▼ Variables	ions.	¶a ()
Taxt Object	Name Dimension Default Value Property (Type:Name) Override Description	res next hop. 2. co	Fin Q
Geolocation	No records to display		
Interface		aters for eigrp. 1. C	ч с –
Key Chain		or an AS	¶∎ Q 🗎
Network			n a ⊂
> ркі		s K < Page 1	of 3 > > C
	Cancel		

Bild 12. FlexConfig-Objektvariable

Schritt 3.3: Fügen Sie einen Namen für die ACL-Objektvariable hinzu, und wählen Sie dann die erweiterte ACL aus, die in Schritt 2.3 erstellt wurde. Klicken Sie anschließend auf die Schaltfläche Speichern.

Firewall Managemen	Name: OBJ-FC-CONTROL-PLANE	:			⊁ 🕑 admin ▾ 🔤 🖞	sco SECURE
> AAA Server > Access List Extended	Description:	Insert Extended Access List Object Va	iable 🛛 🖓		Filter	
Standard > Address Pools Application Filters	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY				
AS Path Cipher Suite List > Community List		Available Objects C Q. Search	Selected Object		the help of TextObj	
Distinguished Name DNS Server Group External Attributes		CL-UNWANTED-COUNTRY			ilient) and one insid	⊑ α () ■ α ()
File List Y FlexConfig FlexConfig Object	▼ Variables				of TextObjects dn	1
Text Object Geolocation	Name			npuon	ires next hop. 2. co iters for eigrp. 1. C	Ω α () Πα α ()
Interrace Key Chain Network			Cancel		or an AS	■ Q ■ Q ■ Q
> PKI Policy List				Cancel Save	s K < Page 1	of3>>IC

Bild 13. FlexConfig-Objektvariable ACL-Zuweisung

Schritt 3.4: Konfigurieren Sie dann die ACL der Kontrollebene als eingehend für die externe Schnittstelle wie folgt.

Befehlszeilensyntax

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das die ACL-Variable verwendet, die in Schritt 2.3 "VAR-ACL-UNWANTED-COUNTRY" wie folgt erstellt wurde:

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

Auf diese Weise muss sie im FlexConfig-Objektfenster konfiguriert werden. Wählen Sie anschließend die Schaltfläche "Save" (Speichern), um das FlexConfig-Objekt abzuschließen.

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE						⊁ 🕑 admin v ∵	secure
> AAA Server	Description:						Filter	
✓ Access List								
Extended	Copy-pasting any rich text might in	troduce line break	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	le control-plane				the help of TextObj	₽ 0, 1
AS Path								B 0 E
Cipher Suite List								
> Community List								¶∎ Q
> Distinguished Name							lient) and one insid	Faq =
DNS Server Group								
> External Attributes							e outside (PD client	₽ ⊂
File List							of TextObjects dn	₽ _ 0, ``
✓ FlexConfig	▼ Variables							Bh 0 ⊇
FlexConfig Object	Name	Dimension	Default Value	Property (Type:Name)	Override	Description	ons.	
Text Object	VAR-ACL-UNWANTED-COUNTRY	SINGLE	ACL-UNWANTED	EXD_ACL:A	false		ires next hop. 2. co	1 8 Q
Geolocation							sters for eigrp. 1. C	¶a Q
Interface							ZA ne v	En o =
Key Chain							A GILAG	
Network								Γ α -
> ркі							s IC < Page 1	of 3 > > C
Policy List						Cancel Save		

Bild 14. Flexconfig-Objekt - vollständige Befehlszeile

Schritt 4: Sie müssen die Konfiguration des FlexConfig-Objekts auf das FTD anwenden. Gehen Sie dazu zu Devices (Geräte) > FlexConfig (FlexConfig-Objekt).

Cipiects / Object Management	Center Overview Analysis Policies	Devices Objects	Integration	Deploy Q 🤩 🖁	🗘 🕜 admin v 🖓	see SECURE
 > AAA Server > Access List Extended Standard > Address Pools 	FlexConfig Object FlexConfig Object include device configuration commands 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_Insp	ection_Protocol_Disable		Disable Default Inspection.		Γ α 📄
> Community List	Default_Insp	ection_Protocol_Enable		Enable Default Inspection.		₽ 0,
> Distinguished Name	DHCPv6_Pre	fix_Delegation_Configure		Configure one outside (PD o	client) and one insid	₽ Q
DNS Server Group						B. A. D
> External Attributes	DHCPv6_Preh	<_Delegation_UnConfigure		Remove configuration of one	e outside (PD client	• 8 4
File List	D	NS_Configure		Configure DNS with the help	o of TextObjects dn	¶∎ Q
✓ FlexConfig	DN	S_UnConfigure		Remove the DNS configurat	ions.	Elα ⊂
FlexConfig Object						
Text Object	Eig	grp_Configure		Configures eigrp. 1. Configu	ures next hop. 2. co	ча (С
Geolocation	Eigrp_I	nterface_Configure		Configures interface parame	aters for eigrp. 1. C	Ω (
Interface Key Chain	Eigr	p_UnConfigure		Clears eigrp configuration for	or an AS	Fa Q 📄
Network	Eigro	Unconfigure All		Clears eigro configuration.		Elα =
> ркі				Displaying 1 - 20 of 49 row	s K < Page 1	of3>>IC

Bild 15. Menü "FlexConfig Policy"

Schritt 4.1: Klicken Sie dann auf New Policy (Neue Richtlinie), wenn noch keine FlexConfig-Option für Ihr FTD erstellt wurde, oder bearbeiten Sie die bestehende FlexConfig-Richtlinie.

Ę	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						

Bild 16. Erstellung von FlexConfig-Richtlinien

Schritt 4.2: Fügen Sie einen Namen für die neue FlexConfig-Richtlinie hinzu, und wählen Sie das FTD aus, das die erstellte Kontrollebenen-ACL anwenden soll.

Firewall Management Center	Overview Analysis Policies Devices Objects Integration	Deploy Q 🥩 🌣 🍘 admin 🕶 🖓
FlexConfig Policy	New Policy	0
	Name: FLEXCONFIG-POLICY Description: Targeted Devices Select devices to which you want to apply this policy. Available Devices Q. Search by name or value FTD-CONTROL-PLANE Add to Policy	
	Cancel	Save

Bild 17. Zuweisung der FlexConfig-Richtlinie für Geräte

Schritt 4.3: Suchen Sie im linken Bereich nach dem FlexConfig-Objekt, das in Schritt 3.2 oben erstellt wurde, und fügen Sie es anschließend der FlexConfig-Richtlinie hinzu. Klicken Sie dazu auf den rechten Pfeil in der Mitte des Fensters, und klicken Sie anschließend auf die Schaltfläche Speichern.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🥩 🔅 🕢 admin 🔻 👘 secure
FLEXCONFIG-POLICY							You have unsaved changes Preview Config Save Cancel
							Policy Assignments (1)
	- Selecte	d Prepend F	lexConfigs				
Available FlexConfig C FlexConfig Object	# Nam	10			Description		
V Liser Defined							
BOBJ-FC-CONTROL-PLANE							
V System Defined	-						
a Default_DNS_Configure							
Default_Inspection_Protocol_Disable							
Contemporary Conte		d Append Fl	lexConfigs				
DHCPv6_Prefix_Delegation_Configure					Decedation		
DHCPv6_Prefix_Delegation_UnConfigure	# Nam	10			Description		
The DNS_Configure	1 OBJ	-FC-CONTROL	-PLANE				٩ 🖥
DNS_UnConfigure	4						
"i Eigrp_Configure							
"i Eigrp_Interface_Configure							
_9 Eigrp_UnConfigure							
Figrp_Unconfigure_All							

Bild 18. FlexConfig-Richtlinienobjektzuweisung

Schritt 5: Fahren Sie mit der Bereitstellung der Konfigurationsänderung im FTD fort, und navigieren Sie zu Deploy > Advanced Deploy.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🧬 🔅 (admin 🕶 🔤 🖓 admin	SECURE
FLEXCONFIG-POLICY							Advanced	Deploy Deploy All	ncel
Enter Description						FTD-CONTROL-PLANE	Ready for D	ployment	📥 _s (1)
Ausilable ElexConfig	n Selecte	ed Prepend F	lexConfigs						
Available PiexConing C PiexConing Object	# Nar	me			Description				
V Hear Dafinard									
OBJ-FC-CONTROL-PLANE	-								
✓ System Defined									
" Default_DNS_Configure						A device is scallable for device and			
Default_Inspection_Protocol_Disable						I device is available for deployment			
Default_Inspection_Protocol_Enable	Selecte	ed Append F	lexConfigs						
DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure	# Nar	me			Description				
DNS_Configure	1 OB.	J-FC-CONTROL	-PLANE						٩
DNS_UnConfigure									
.9 Eigrp_Unconfigure_All									

Bild 19. FTD - Erweiterte Bereitstellung

Schritt 5.1: Wählen Sie dann das FTD aus, auf das die FlexConfig-Richtlinie angewendet werden soll. Wenn alles korrekt ist, klicken Sie auf Bereitstellen.

Fi or	irewall Management Center eploy / Deployment	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	a 🇬	🔅 🕜 admin 🕇 🔡	🖑 SECURE
1 device se	lected Search using device name, user name, type	, group or statu	15								Deploy time: Estimate	Deploy
	Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time	Pre	eview	Status	
× 🗹	FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:0	5 PM	B	Ready for Deployment	
:: •	Flex Configuration Template Policy: FLEXCONFIG-POLICY											
https://10.88.24	13.58-43013/ddd/#ContextExplorer											

Bild 20. FTD-Bereitstellungsvalidierung

Schritt 5.2: Anschließend wird ein Fenster mit der Bereitstellungsbestätigung angezeigt. Fügen Sie einen Kommentar hinzu, um die Bereitstellung zu verfolgen, und fahren Sie mit der Bereitstellung fort.

P	Firewall Management Center Deploy / Deployment								🔅 🕲 admin 🕶 🖓	
1 devic										
		Modified by								
~	FTD-CONTROL-PLANE	admin					Sep	5, 2023 12:05 PM	Ready for Deployment	
x= •	 Flex Configuration Template Policy: FLEXCONFIG-POLICY 		Deployment Con	ħrmation			×			
			You have selected 1 of	levice to deploy	,					
			Deployment Notes:							
			You can optionally a	id notes about t	the configura	tion changes				
							Deploy			
							Deploy			

Bild 21. FTD-Bereitstellungskommentare

Schritt 5.3: Bei der Bereitstellung von FlexConfig-Änderungen kann eine Warnmeldung angezeigt werden. Klicken Sie auf Deploy (Bereitstellen), wenn Sie absolut sicher sind, dass die Richtlinienkonfiguration korrekt ist.



Bild 22. FTD-Bereitstellungs-Flexconfig-Warnung

Schritt 5.4: Bestätigen Sie, dass die Richtlinienbereitstellung für die FTD erfolgreich war.

	Fi De	irewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deplo	w Q 💰	🗘 🤣 adm	in ▼ disel: SECURE
T	۹	Search using device name, user name, type	e, group or state	us									Deploy
		Device	Modified by		Inspect Inte	erruption	Туре	Group	Last Deploy Tim	10	Preview	Status	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12	2:05 PM		Completed	
* •		 Flex Configuration Template Policy: FLEXCONFIG-POLICY 											

Bild 23. FTD-Bereitstellung erfolgreich

Schritt 6: Wenn Sie eine neue Kontrollebenen-ACL für Ihren FTD erstellen oder eine vorhandene editieren, die aktiv genutzt wird, dann ist es wichtig hervorzuheben, dass die vorgenommenen Konfigurationsänderungen nicht für bereits bestehende Verbindungen zum FTD gelten. Daher müssen Sie die aktiven Verbindungsversuche zum FTD manuell löschen. Stellen Sie dazu die Verbindung mit der CLI des FTD her, und löschen Sie die aktiven Verbindungen wie folgt.

So löschen Sie die aktive Verbindung für eine bestimmte Host-IP-Adresse:

> clear conn address 192.168.1.10 all

So löschen Sie die aktiven Verbindungen für ein ganzes Subnetz:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

So löschen Sie die aktiven Verbindungen für einen IP-Adressbereich:

> clear conn address 192.168.1.1-192.168.1.10 all

Hinweis: Es wird dringend empfohlen, das Schlüsselwort "all" am Ende des Befehls clear conn address zu verwenden, um das Löschen der aktiven VPN-Brute-Force-Verbindungsversuche in die sichere Firewall zu erzwingen, vor allem, wenn die Art des VPN-Brute-Force-Angriffs eine Explosion konstanter Verbindungsversuche auslöst.

Konfigurieren einer von FDM verwalteten Kontrollebenen-ACL für FTD

Mit diesem Verfahren müssen Sie in einem FDM eine Kontrollebenen-ACL konfigurieren, um eingehende VPN-Brute-Force-Angriffe auf die externe FTD-Schnittstelle zu blockieren:

Schritt 1: Öffnen Sie die FDM-GUI über HTTPS, und melden Sie sich mit Ihren Anmeldeinformationen an.



cisco SECURE

Cisco Secure Firewall Device Manager

Username	
Password	ø
	LOG IN



Schritt 2: Sie müssen ein Objektnetzwerk erstellen. Navigieren Sie dazu zu Objekte:

Bild 25. FDM-Haupt-Dashboard

Schritt 2.1: Wählen Sie im linken Bereich "Networks" (Netzwerke) aus, und klicken Sie dann auf die Schaltfläche "+", um ein neues Netzwerkobjekt zu erstellen.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	ver 🔎) (admin Administrator v "lull" SECURE
Object Types ←	Network Objects and Groups		
C Networks	6 objects		▼ Filter + 🗐
S Ports			Preset filters: System defined. User defined
8 Security Zones	H NAME	TYPE VALUE	ACTIONS
🐬 Application Filters	1 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8	
A∂ LIRLs	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12	
	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-10 192.168.0.0-16	0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-
🛖 IPSec Proposals			
Secure Client Profiles			
Sa Identity Sources			
1 Users			
🞗 Certificates			
🔒 Secret Keys			

Bild 26. Objekterstellung

Schritt 2.2: Fügen Sie einen Namen für das Netzwerkobjekt hinzu, wählen Sie den Netzwerktyp für das Objekt aus, fügen Sie die IP-Adresse, die Netzwerkadresse oder den IP-Bereich hinzu, um den Datenverkehr abzugleichen, der dem FTD verweigert werden muss. Klicken Sie dann auf die Schaltfläche OK, um das Objektnetzwerk zu vervollständigen.

- In diesem Beispiel soll das konfigurierte Objektnetzwerk Brute-Force-VPN-Angriffe blockieren, die vom Subnetz 192.168.1.0/24 ausgehen.

Firewall Device Manager	Monitoring Polici	Add Network Object	
Object Types ←	Network Obje		
D Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY	
S Ports	_	defined. User defined	
G Security Zones	H NAME	Description	
🖗 Application Filters	1 IPv4-Private-Al	ie-172.16.0.0-12, IPv4-Private-	
⊘ URLs	2 IPv4-Private-10	Туре	
Geolocations	3 IPv4-Private-1	Network Host FQDN Range	
Syslog Servers	4 IPv4-Private-19	Network	
🔏 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	
Sa Identity Sources			
1 Users			
Q Certificates			
🔒 Secret Keys			

Bild 27. Netzwerkobjekt hinzufügen

Schritt 3: Anschließend müssen Sie eine erweiterte Zugriffskontrollliste erstellen. Navigieren Sie dazu zur Registerkarte Gerät im oberen Menü.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	ver	cisco SECURE
Object Types ←	Network Objects and Groups		
C Networks	7 objects	T Filter	+ 👰
S Ports		Preset filters: System.defined, User.defined	
8 Security Zones	# 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	
Syslog Servers	4 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16	
	5 any-ipv4	NETWORK 0.0.0.0/0	
	6 any-ipv6	NETWORK ::/0	
	7 OBJ-NET-UNWANTED-COUNTRY	NETWORK 192.168.1.0/24	
Secure Client Profiles			
Sea Identity Sources			
1 Users			
🙊 Certificates			
🔒 Secret Keys			

Bild 28. Seite mit Geräteeinstellungen

Schritt 3.1: Blättern Sie nach unten, und wählen Sie im Feld Erweiterte Konfiguration die Option Konfiguration anzeigen aus.

Firewall Device Manager	Policies Objects Device: firepower	> 🚔 @ ?	admin Administrator
	0/0 		
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 DNS Service
Smart License Evaluation expires in 89 days Tier: Not selected (Threat Defense Virtual - Variable) View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	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

Bild 29. Erweiterte FDM-Konfiguration

Schritt 3.2: Navigieren Sie dann im linken Bereich zu Smart CLI > Objects, und klicken Sie auf CREATE SMART CLI OBJECT (SMART CLI-OBJEKT ERSTELLEN).

Firewall Device Manager	Monitoring	Ø Policies	Objects	Device: firepowe		Ø ?	• admin • Administrator	cisco SECURE
Advanced ← Configuration	Device Summa Objects	ary						
Smart CLI								+
Objects	•	NAME		туре	DESCRIPTION		ACTIONS	
FlexConfig					There are no Smart CLI objects yet.	-4		
FlexConfig Objects					CREATE SMART CLIOR IECT	1		
FlexConfig Policy					UREATE SMAAT DEI OBJEUT	1		

Bild 30. Smart CLI-Objekte

Schritt 3.3: Fügen Sie einen Namen für die zu erstellende erweiterte ACL hinzu, wählen Sie im Dropdown-Menü für die CLI-Vorlage die Option "Extended Access List" aus, und konfigurieren Sie die erforderlichen ACEs mithilfe des im obigen Schritt 2.2 erstellten Netzwerkobjekts. Klicken Sie anschließend auf OK, um die ACL abzuschließen.

Firewall Devic	Edit Smort CLI Object		sco SECURE
Advanced Configuration	Name ACL-UNWANTED-COUNTRY	Description	+
Smart CLI Objects	CLI Template Extended Access List \checkmark		ACTIONS
FlexConfig	Template	• Show disabled 🗘 Reset	
FlexConfig Objects	1 access-list ACL-UMANTED-COUNTRY extended 2 configure access-list-entry deny ∨ 3 deny network source [.00].htt-UMANTED-COUNTRY >>] destin 4 configure deny port any ∨ 5 deny port source NNY destination ANY 6 configure logging default ∨ 7 default log set log-level INFORMATIONAL log-interval	nation [<u>amy-ipv4 ×</u>	
		CANCEL OK	

Bild 31. Erstellung erweiterter ACLs

Hinweis: Wenn Sie weitere ACEs für die ACL hinzufügen müssen, können Sie dies tun, indem Sie mit der Maus auf die linke Seite des aktuellen ACE zeigen. Daraufhin werden drei anklickbare Punkte angezeigt. Klicken Sie darauf, und wählen Sie Duplizieren aus, um weitere ACEs hinzuzufügen.

Schritt 4: Anschließend müssen Sie ein FlexConfig-Objekt erstellen. Navigieren Sie dazu zum linken Bereich, wählen Sie FlexConfig > FlexConfig Objects aus, und klicken Sie auf CREATE FLEXCONFIG OBJECT.

Firewall Device Manag	ger Monitoring Policies Objects	Device: firepower	admin Administrator	IRE
Advanced ← Configuration	Device Summary FlexConfig Objects			
Smart CLI			Y Filter	+
Objects	# NAME	DESCRIPTION	ACTIONS	
FlexConfig		There are no FlexConfig object Start by creating the first FlexConf	cts yet. nfig object.	
FlexConfig Objects FlexConfig Policy		CREATE FLEXCONFIG OBJEC	ст	

Bild 32. FlexConfig-Objekte

Schritt 4.1: Fügen Sie einen Namen für das FlexConfig-Objekt hinzu, um die Kontrollebenen-ACL

für die externe Schnittstelle wie folgt als eingehend zu erstellen und zu konfigurieren.

Befehlszeilensyntax

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das die erweiterte ACL verwendet, die in Schritt 3.3 "ACL-UNWANTED-COUNTRY" wie folgt erstellt wurde:

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

So sollte es im FlexConfig-Objektfenster konfiguriert werden. Wählen Sie anschließend die Schaltfläche OK, um das FlexConfig-Objekt abzuschließen.

Advanced Create FlexConfig Object Advanced Device Sur Configuration Dispects Smart CLI Image: Control-PLANE Objects Image: Control-PLANE	Firewall Device Manaç	ger Monitoring	()			<u></u>	admin Administrator	
Advanced Configuration FlexCo Name OBJ-FC-CONTROL-PLANE OBJ-FC-CONTROL-PLANE CTIONS		Device Cu	Create FlexConfig Ob	oject				
Smart CLI OBJ-FC-CONTROL-PLANE Objects	Advanced ← Configuration	FlexCo	Name					
Smart CLI Description Objects Image: Chick State			OBJ-FC-CONTROL-PLANE				+	
Objects Crions	Smart CLI		Description				_	
	Objects	·	boounpion			4	CTIONS	
Elev Coeffe	FloyConfin		Variablee			111.		
Prexioning Valiables There are no variables yet. There are no variables yet.	FlexConfig		There are no variables yet.					
RexConfig Objects Start with adding a new variable.	FlexConfig Objects		ADD VARIABLE					
FlexConfig Policy	FlexConfig Policy		Tree preser					
Template CENTRY is intenface outside control plane			Template	WITED COUNTRY in interface outsi	; Expand	C Reset		
			1 access-group Acc-onno-	ATED-CONTRY IN INCEPTACE OUTSI	de contror-prane			
Negate Template 🛆 🗘 Expand 🛛 🗘 Reset			Negate Template A		Expand	🗘 Reset		
1 no access-group ACL-UNAWNTED-COUNTRY in interface outside control-plane			1 no access-group ACL-U	NMANTED-COUNTRY in interface ou	utside control-plane			
					CANCEL	OK		

Bild 33. Erstellung von FlexConfig-Objekten

Schritt 5: Fahren Sie mit der Erstellung einer FlexConfig-Richtlinie fort. Navigieren Sie dazu zu Flexconfig > FlexConfig Policy, klicken Sie auf die Schaltfläche "+", und wählen Sie das FlexConfig-Objekt aus, das im obigen Schritt 4.1 erstellt wurde.



Bild 34. FlexConfig-Richtlinie

Schritt 5.1: Überprüfen Sie, ob in der FlexConfig-Vorschau die richtige Konfiguration für die erstellte Kontrollebenen-ACL angezeigt wird, und klicken Sie auf die Schaltfläche Speichern.

Firewall Device Manager	Monitoring Policies Objects Device: firepower	S→ S	cisco SECURE
Advanced ← Configuration	Device Summary FlexConfig Policy		
Smart CLI	Group List	Preview	<> Expand
Objects	T OBJ-FC-CONTROL-PLANE	access-group ACL-LMMANTED-COUNTRY in interface control-plane	outside
FlexConfig			
FlexConfig Objects			
FlexConfig Policy			
	SAVE		

Bild 35. Vorschau der FlexConfig-Richtlinie

Schritt 6: Stellen Sie die Konfigurationsänderungen auf dem FTD bereit, das Sie gegen die VPN-Brute-Force-Angriffe schützen möchten. Klicken Sie dazu im oberen Menü auf die Schaltfläche Deployment (Bereitstellung), überprüfen Sie, ob die bereitzustellenden Konfigurationsänderungen richtig sind, und klicken Sie dann auf DEPLOY NOW (JETZT BEREITSTELLEN).

Firewall Device Manage	Pending Changes
Advanced ← Configuration	Last Deployment Completed Successfully 05 Sep 2023 02:27 PM. See Deployment History
Smart CLI	Deployed Version (05 Sep 2023 02:27 PM) Pending Version O LEGEND
Objects	Network Object Added: OBJ-NET-UNWANTED-COUNTRY
FlexConfig	- subTyper Network ↔ Expand - value: 2.2.2.0/24 - in interface outside - dnsResolution: IPV4_N0_IPV6
FlexConfig Objects	- description: - name: 08J-NET-UNMANTED-COUNTRY
FlexConfig Policy	ElayConfig Dallay Edited: default-group
	PrexConing Policy Exited: Default-group flexConing Policy
	C Extended Access List Added: ACL-UNWANTED-COUNTRY
	- entries[0].logging: DEFAULT - entries[0].action: DEINY - name: ACL-UNWANTED-COUNTRY entries[0].sourceNetworks:
	MORE ACTIONS ~ CANCEL DEPLOY NOW ~

Bild 36. Ausstehende Bereitstellung

	مرجع لألبه مسم مالل	مرمامية مستمام مسمامه	Dialattinia and analtata	
SCOULT	Inernriten	der erfoldreichen	Richtliniennereitste	החווי
	Obcipiulon			nung

Firewall Device Ma	hager Pending Changes OX
Advanced ← Configuration	There are no Pending Changes yet
Objects	Nothing to deploy.
FlexConfig	in interface outside
FlexConfig Objects	You can see what was deployed in previous jobs in the <u>Deployment History</u>
FlexConfig Policy	
	ок се
	and a second second Save

Bild 37. Bereitstellung erfolgreich

Schritt 7. Wenn Sie eine neue Kontrollebenen-ACL für Ihren FTD erstellen oder eine vorhandene editieren, die aktiv genutzt wird, dann ist es wichtig hervorzuheben, dass die vorgenommenen Konfigurationsänderungen nicht für bereits bestehende Verbindungen zum FTD gelten. Daher müssen Sie die aktiven Verbindungsversuche zum FTD manuell löschen. Stellen Sie dazu die Verbindung mit der CLI des FTD her, und löschen Sie die aktiven Verbindungen wie folgt.

So löschen Sie die aktive Verbindung für eine bestimmte Host-IP-Adresse:

> clear conn address 192.168.1.10 all

So löschen Sie die aktiven Verbindungen für ein ganzes Subnetz:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

So löschen Sie die aktiven Verbindungen für einen IP-Adressbereich:

> clear conn address 192.168.1.1-192.168.1.10 all

Hinweis: Es wird dringend empfohlen, das Schlüsselwort "all" am Ende des Befehls clear conn address zu verwenden, um das Löschen der aktiven VPN-Brute-Force-Verbindungsversuche in die sichere Firewall zu erzwingen, vor allem, wenn die Art des VPN-Brute-Force-Angriffs eine Explosion konstanter Verbindungsversuche auslöst.

Konfigurieren einer Kontrollebenen-ACL für ASA mit CLI

Mit diesem Verfahren müssen Sie in einer ASA CLI eine Kontrollebenen-ACL konfigurieren, um eingehende VPN-Brute-Force-Angriffe auf die externe Schnittstelle zu blockieren:

Schritt 1: Melden Sie sich über die CLI bei der sicheren Firewall-ASA an, und erhalten Sie wie folgt Zugriff auf das 'configure-Terminal'.

asa# configure terminal

Schritt 2: Verwenden Sie den nächsten Befehl, um eine erweiterte ACL zu konfigurieren, die eine Host-IP-Adresse oder Netzwerkadresse für den Datenverkehr blockiert, der zur ASA blockiert werden muss.

 In diesem Beispiel erstellen Sie eine neue ACL mit dem Namen "ACL-UNWANTED-COUNTRY".
 Der konfigurierte ACE-Eintrag blockiert Brute-Force-VPN-Angriffe aus dem Subnetz 192.168.1.0/24.

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

Schritt 3: Verwenden Sie den nächsten Zugriffsgruppenbefehl, um die ACL "ACL-UNWANTED-COUNTRY" als Kontrollebenen-ACL für die externe ASA-Schnittstelle zu konfigurieren.

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

Schritt 4: Wenn Sie eine neue Kontrollebenen-ACL erstellen oder eine vorhandene bearbeiten, die aktiv genutzt wird, ist es wichtig zu betonen, dass die vorgenommenen Konfigurationsänderungen nicht für bereits bestehende Verbindungen mit der ASA gelten. Sie müssen daher die aktiven Verbindungsversuche mit der ASA manuell löschen. Löschen Sie dazu die aktiven Verbindungen wie folgt.

So löschen Sie die aktive Verbindung für eine bestimmte Host-IP-Adresse:

asa# clear conn address 192.168.1.10 all

So löschen Sie die aktiven Verbindungen für ein ganzes Subnetz:

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

So löschen Sie die aktiven Verbindungen für einen IP-Adressbereich:

asa# clear conn address 192.168.1.1-192.168.1.10 all

Hinweis: Es wird dringend empfohlen, das Schlüsselwort "all" am Ende des Befehls clear conn address zu verwenden, um das Löschen der aktiven VPN-Brute-Force-Verbindungsversuche in die sichere Firewall zu erzwingen, vor allem, wenn die Art des VPN-Brute-Force-Angriffs eine Explosion konstanter Verbindungsversuche auslöst.

Alternative Konfiguration zum Blockieren von Angriffen für eine sichere Firewall mithilfe des Befehls "shun"

Im Falle einer sofortigen Option, Angriffe für die sichere Firewall zu blockieren, können Sie den Befehl "shun" verwenden. Mit dem Befehl huncommand können Sie Verbindungen von einem angreifenden Host blockieren.

- Wenn Sie eine IP-Adresse ignorieren, werden alle zukünftigen Verbindungen von der Quell-IP-Adresse gelöscht und protokolliert, bis die Blockierungsfunktion manuell entfernt wird.

- Die Blockierungsfunktion des Befehls hunwird angewendet, unabhängig davon, ob aktuell eine Verbindung mit der angegebenen Host-Adresse aktiv ist.

- Wenn Sie die Zieladresse, die Quell- und Zielports und das Protokoll angeben, dann lassen Sie die passende Verbindung fallen und schließen alle zukünftigen Verbindungen von der Quell-IP ab.

Adresse; alle zukünftigen Verbindungen werden vermieden, nicht nur solche, die diesen spezifischen Verbindungsparametern entsprechen.

- Sie können nur einen Befehl pro Quell-IP-Adresse haben.

- Da der huncommand verwendet wird, um Angriffe dynamisch zu blockieren, wird er in der Gerätekonfiguration zur Bedrohungsabwehr nicht angezeigt.

- Wenn eine Schnittstellenkonfiguration entfernt wird, werden alle Nebenstellen, die an diese Schnittstelle angeschlossen sind, ebenfalls entfernt.

- Shun-Befehlssyntax:

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

- Um eine Shun-Funktion zu deaktivieren, verwenden Sie die negative Form dieses Befehls:

no shun source_ip [vlan vlan_id]

Um eine Host-IP-Adresse zu vermeiden, gehen Sie für die sichere Firewall wie folgt vor. In diesem Beispiel wird der Befehl "shun" verwendet, um Brute-Force-VPN-Angriffe zu blockieren, die von der Quell-IP-Adresse 192.168.1.10 ausgehen.

Konfigurationsbeispiel für FTD

Schritt 1: Melden Sie sich über die CLI beim FTD an, und wenden Sie den Befehl shun wie folgt an.

<#root>

>

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Schritt 2: Sie können die folgenden Befehle zum Anzeigen verwenden, um die verworfenen IP-Adressen im FTD zu bestätigen und die Anzahl der verworfenen Treffer pro IP-Adresse zu überwachen:

```
<#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)
```

Konfigurationsbeispiel für ASA

Schritt 1: Melden Sie sich über die CLI bei der ASA an, und wenden Sie den Befehl shun wie folgt an.

<#root>

asa#

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Schritt 2: Mit den folgenden Befehlen zum Anzeigen können Sie die Anzahl der gesendeten IP-Adressen in der ASA bestätigen und die Anzahl der gesendeten IP-Adressen pro IP-Adresse überwachen:

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

Hinweis: Weitere Informationen zum Befehl shun für die sichere Firewall finden Sie in der <u>Cisco Secure Firewall Threat Defense Command Reference</u>

Überprüfung

So bestätigen Sie, dass die ACL-Konfiguration der Kontrollebene für die sichere Firewall vorhanden ist:

Schritt 1: Melden Sie sich über die CLI bei der sicheren Firewall an, und führen Sie die nächsten Befehle aus, um zu bestätigen, dass die ACL-Konfiguration der Kontrollebene angewendet wurde.

Ausgabebeispiel für von FMC verwaltete FTD:

<#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

Ausgabebeispiel für von FDM verwaltete FTD:

<#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

Ausgabebeispiel für 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

Schritt 2: Um zu bestätigen, dass die Kontrollebenen-ACL den erforderlichen Datenverkehr blockiert, verwenden Sie den Befehl Packet-Tracer, um eine eingehende TCP 443-Verbindung mit der externen Schnittstelle der sicheren Firewall zu simulieren, und dann den Befehl show accesslist <acl-name>. Die Anzahl der ACL-Treffer sollte jedes Mal erhöht werden, wenn eine VPN-Brute-Force-Verbindung mit der sicheren Firewall durch die Kontrollebenen-ACL blockiert wird:

- In diesem Beispiel simuliert der Befehl "Packet-Tracer" eine eingehende TCP-443-Verbindung, die vom Host 192.168.1.10 stammt und an die externe IP-Adresse unserer sicheren Firewall gerichtet ist. Die Ausgabe von "Packet-Tracer" bestätigt, dass der Datenverkehr verworfen wird, und die Ausgabe von "show access-list" zeigt die inkrementellen Trefferzahlen für unsere ACL auf der Kontrollebene an:

Beispiel für FTD-Ausgabe

<#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

Ausgabebeispiel für 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

Minweis: Wenn eine RAVPN-Lösung wie das Cisco Secure Client VPN in der sicheren Firewall implementiert ist, kann ein echter Verbindungsversuch zur sicheren Firewall durchgeführt werden, um zu bestätigen, dass die ACL auf der Kontrollebene wie erwartet funktioniert, um den erforderlichen Datenverkehr zu blockieren.

Verwandte Fehler

ENH | Standortbasierte AnyConnect Client-Verbindungen: Cisco Bug-ID <u>CSCvs65322</u>

Informationen zu dieser Übersetzung

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