FTD:如何使用FlexConfig策略启用TCP状态绕行 配置

目录

简<u>介</u> <u>先决条件</u> <u>要求</u> 使用的组件 <u>背景信息</u> <u>電置</u> 步骤1.配置扩展访问列表对象 步骤2.配置FlexConfig对象 步骤3.为FTD分配FlexConfig策略 <u>确认</u> <u>故障排除</u> 相关链接

简介

本文档介绍如何在6.3.0之前的版本中使用FlexConfig策略,通过Firepower管理中心(FMC)在 Firepower威胁防御(FTD)设备上实施传输控制协议(TCP)状态绕行功能。

先决条件

要求

Cisco 建议您了解以下主题:

- 了解Firepower管理中心。
- Firepower威胁防御的基本知识。
- •了解TCP状态绕行功能。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Firepower威胁防御(FTD)版本6.2.3。
- Firepower管理中心(FMC)版本6.2.3。

背景信息

TCP状态绕行是从自适应安全设备(ASA)继承的一项功能,在排除可能被TCP规范化功能、非对称 路由条件和某些应用检测丢弃的流量时提供帮助。 从版本6.3.0开始,FMC本地支持此功能。建议在升级后删除Flexconfig对象,并在首次部署之前将 此配置移到FMC。有关如何在版本6.3.0或更高版本中配置TCP状态绕行的详细信息,请转至此配<u>置</u> <u>指南</u>。

Firepower威胁防御使用ASA配置命令来实施某些功能,但并非所有功能。没有唯一的Firepower威 胁防御配置命令集。相反,FlexConfig的要点是允许您配置尚未通过Firepower管理中心策略和设置 直接支持的功能。

注意: TCP状态绕行仅应用于故障排除目的,或者当无法解决非对称路由时。使用此功能会禁 用多个安全功能,如果未正确实施,则可能导致大量连接。

要了解有关TCP状态旁路功能或其在ASA中实施的详细信息,请参阅<u>在ASA 5500系列和Cisco ASA</u> <u>5500系列配置指南上配置TCP状态旁路功能</u>。

配置

本节介绍如何通过FlexConfig策略在FMC上配置TCP状态绕行。

步骤1.配置扩展访问列表对象

要在FMC上创建扩展访问列表,请转至对象>对象**管理,然后在左**侧菜单的访问列表下选择**扩展**访问**列表。点击添加扩展访问列表。**

Object Management Intrusion Rules	Overview Analysis Policie	es Devices <mark>Objects</mark> AMP		Deploy 😔 System	h Help 🔻
Image Security Group Tag No records to display Security Group Tag Security Group Tag Image Security Group Tag No records to display Security Group Tag Security Group Tag Image Security Intelligence Security Intelligence Image Null Lists and Feeds Security Intelligence Image Null Lists and Feeds Security Intelligence Image Null Lists and Feeds Distinguished Name Image Security Intelligence Security Intelligence Image Distinguished Name Security Intelligence	Object Management Intrus	sion Rules			
Name Value Override Application Filters Application Filters No records to display Implicit and Feeds Implicit Set Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit Suble Set Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit Suble Set Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit Suble Set Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit Suble Set Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit Suble Set Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit Suble Set Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit and Feeds Implicit Suble Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set Implicit Set				Add Extended Access List	🔍 Filter
Application Filters VLNN Tag No records to display Security Group Tag UL Geolocation Time Range Variable Set Socity Intelligence Notwork Lists and Feeds UL Lists and Feeds UL Lists and Feeds Ult Lists and Feeds Optimum Lists File List Policy Lists Policy Lists Policy Distriguished Name Distinguished Name	😤 Tunnel Zone	Name		Value	Override
VLNN Tag No records to display Pecurity Group Tag Pecurity Group Tag Pecurity Group Tag Pecurity Group Tag Pecurity Group Tag Pecurity Intelligence Peturity Intelligence Peturity Intelligence Peturity Lists and Feeds Peturity Lists and Feeds Peturity Lists and Feeds Peturity Lists and Feeds Peturity Lists and Feeds Peturity Lists and Feeds Peturity Distinguished Name Peturity Lists	Application Filters				
Security Group Tag Image I	📎 VLAN Tag		No records to display		
WRL Seolocation Imme Range Strable Set Imme Range Variable Set Imme Range	Security Group Tag				
Secolocation Image Time Range Security Intelligence Image Image <t< th=""><th>ORL ORL</th><th></th><th></th><th></th><th></th></t<>	ORL ORL				
Image	Geolocation				
S Variable Set Security Intelligence Vetwork Lists and Feeds Vetwork Lists Vetwor	Time Range				
 Wetwork Lists and Feeds URL Lists and Feeds URL Lists and Feeds URL Lists and Feeds Sinkhole File List Glober Suite List I plistinguished Name I plistinguished Name 	S Variable Set				
Network Lists and Feeds DNS Lists and Feeds Ultimeters Distinguished Name Distinguished Name	Security Intelligence				
W DVS Lats and Feeds Is lists and Feeds Is lists and Feeds Is lists and Feeds Is list and Feeds	Network Lists and Feeds				
Got Lass and Freeds	UPL Lists and Feeds				
initialize initialize initialize initialize initialize initialize initialize initialize initialize	Sinkhole				
Gipher Suite List	File List				
Distinguished Name Individual Objects	Cipher Suite List				
Individual Objects	Distinguished Name				
	Individual Objects				
C Object Groups	Collect Groups				
	Þ 🤌 PKI				
g LA Monitor	SLA Monitor				
▲ B Prefix List	4 🌇 Prefix List				
🛐 IPv4 Prefix List	📑 IPv4 Prefix List				
B IPv6 Prefix List	IPv6 Prefix List				
A Boute Map	Access List				
Standard Bextended	Standard Extended	-			

使用所需值填写"名称"字段。在本例中,名称为TCP_Bypass。单击Add按钮。

New Extended Access List Object

I	Name:	TCP_Bypass	;				
	 Entries (0) 						
	Sequence	Action	Source	Source Port	Destination	Destination Port	
				No reco	rds to display		
				110 1000			
1	Allow Overrides:						
							Save Cancel

此规则的操作必须配置为**允许**。可以使用系统定义的网络,或为每个源和目标创建新的网络对象。 在本示例中,访问列表匹配从主机1到主机2的IP流量,因为这是应用TCP状态绕行的通信。端口选 项卡可以用于匹配特定TCP或UDP端口。单击"Add(添**加)**"按钮继续。

Add Extended A	Access List Entry					? ×
Action:	🖋 Allow	•				
Logging:	Default	\$				
Log Level:	Informational	\$				
Log Interval:	300	Sec.				
Network Por	t					
Available Network	s Ċ	\odot	Source Networks (1)		Destination Networks (1)	
Search by name	e or value		🚍 Host1	i	🚔 Host2	ii
📄 any						
📄 any-ipv4						
📄 any-ipv6		Add to				
FMC		Source				
Host1		Add to				
📄 Host2						
IPv4-Benchmar	k-Tests					
IPv4-Link-Local						
IPv4-Multicast						
IPv4-Private-10	0.0.0.0-8		Enter an IP address	Add	Enter an IP address	Add
					Add	Cancel

选择源网络和目标网络或主机后,单击Save。

Edit Extended Access List Object

Nam	ne:	TCP_Bypass	;				
	chines (1)						O Add
S	equence	Action	Source	Source Port	Destination	Destination Port	
1		🛹 Allow	Host1	Any	Rost2	Any	0
Allow	w Overrides:						
						Save	Cancel

? X

导航至"**对象">"对象管理">"FlexConfig">"FlexConfig对象",**然后单击"添**加FlexConfig对象"**按钮。

Overview Analysis Policie	s Devices Objects AMP	Deploy 📀 System Help 🔻 💌
Object Management Intrus	ion Rules	
		Add FlexConfig Object
Individual Objects	Name	Description
Collect Groups	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaul
SLA Monitor	Default_Inspection_Protocol_Disable	Disable Default Inspection.
4 🛐 Prefix List	Default_Inspection_Protocol_Enable	Enable Default Inspection.
IPv4 Prefix List IPv6 Prefix List	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface
Ø Route Map	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one ir 🛅 🔍 📋
Access List Standard	DNS_Configure	Configure DNS with the help of TextObjects dnsParameter 🖺 🔍 📋
Standard	DNS_UnConfigure	Remove the DNS configurations.
Y AS Path	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures au 🛅 🔍 📋
Bolicy List	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures a
	Eigrp_UnConfigure	Clears eigrp configuration for an AS
IKEV1 Policy	Eigrp_Unconfigure_All	Clears eigrp configuration.
(A) IKEv1 IPsec Proposal	Inspect_IPv6_Configure	Configure inspection for ipv6 traffic.Used text objects in t
IKEv2 IPsec Proposal Group Policy	Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.
AnyConnect File	ISIS_Configure	Configures global parameters for IS-IS.
R. Certificate Map	ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv 🗓 🔍 📋
IPv4 Pools	ISIS_Unconfigure	Unconfigures is-is.
IPV6 Pools	ISIS_Unconfigure_All	Unconfigures is-is.
FiexConfig Text Object	Netflow_Add_Destination	Create and configure a NetFlow export destination.
RADIUS Server Group	Netflow Clear Parameters	Set NetFlow excort alobal settings back to default values. In the Displaying 1 - 20 of 48 rows < < Page 1 of 3 >> C

此示例的对象名称称为TCP_Bypass,与访问列表一样。此名称不需要与访问列表名称匹配。

						Save	Cancel
			No records t	o display			
Name		Dimension	Default Value	Property (Ty	Override	Description	
Variables							
		Extended ACL Object Route Map	-				
- Insert Sect	et ney	Security Zones					
 Insert Syst Insert Sect 	em variable 🕨	Network					
 Insert Polic 	cy Object 🕨	Text Object					
Insert •					Deployment:	Everytime 🗘 Type:	Append \$
							C
Description:	TCP State Bypass						
Name:	TCP_Bypass						
Add FlexConfig	g Object						? 3

选择插入策略对象>扩展ACL对象。

注意:确保选择"Everytime"选项。这允许在其他部署和升级期间保留此配置。

从"可用对象"(Available Objects)部分选择在步骤1中创**建的访**问列表并分配变量名称。然后,单击 "Add(添**加)"**按钮。在本例中,变量名称为**TCP_Bypass**。

单击"Save(保存)"。

Insert Extended Access List Object	Variable		? ×
Variable Name: TCP_Bypass Description:			
Available Objects 😋		Selected Object	
Search		TCP_Bypass	ï
TCP_Bypass	Add		
		Save	Cancel

在空白字段中的"插入"按钮正下**方添**加下一行配置行,并在<u>match access-list</u>配置行中包含以前定义 的变量(**\$TCP_Bypass**)。请注意,**\$**符号在变量名称前面。这有助于定义变量后跟。

class-map tcp_bypass match access-list **\$TCP_Bypass** policy-map tcp_bypass_policy class tcp_bypass set connection advanced-options tcp-state-bypass service-policy tcp_bypass_policy interface outside 在本示例中,会创建策略映射并将其应用到外部接口。如果TCP状态绕行需要配置为全局服务策略 的一部分,则tcp_bypass类映射可应用于global_policy。

完成后单击"保存"。

Add FlexConfig	Object							? ×
Name:	TCP_Bypass							
Description:	TCP State Bypass							G
◯ Insert •	∎¥ ∎X				Deployment:	Everytime \$	Type:	Append \$
class-map match acce policy-map class tcp_ set connec service-po	tcp_bypass ess-list \$TCP_By b tcp_bypass_pol bypass tion advanced-o blicy tcp_bypass	pass icy ptions tcp _policy in	-state-bypass terface outsid	e				
								©
Variables								
Name		Dimension	Default Value	Property (Ty	Override	Description		
			No records to	display				
						52	(Cancel

步骤3.为FTD分配FlexConfig策略

转到**Devices > FlexConfig**并创建新策略(除非已为其他用途创建策略并将其分配给同一FTD)。在 本例中,新的FelxConfig策略称为**TCP_Bypass**。

Overview Analysis	Policies	Devic	es 0)bjects AMP				Deploy	0	System	Help 🔻 👘
Device Management	NAT \	/PN v	QoS	Platform Settings	FlexConfig	Certificates					
										(New Policy
FlexConfig Policy						Status	Last Modified				
					-						

There are no policies created. Add a new policy

将TCP_Bypass FlexConfig策略分配给FTD设备。

New Policy

	TCP_Bypass					
escription: TCP State Bypass						
geted Devices						
Select devices	s to which you want to	apply this policy.				
Available De	vices		Selected Devices			
🔍 Search by	name or value		FTD FTD	ũ		
FTD						
		Add to Polic	y			

选择在步骤2中"**用户定义"**部分下创建的名为**TCP_Bypass的**FlexConfig对象,然后单击箭头将该对 象添加到策略。

Overview Analysis Policies Devices Obje	ects AMP		Deploy 📀 System Help 🗸 👘
Device Management NAT VPN - QoS P	latform Settings Flex	Config Certificates	
TCP_Bypass TCP State Bypass			You have unsaved changes Preview Config 🛛 🔚 Save 🕽 😂 Cancel
			Policy Assignments (1)
Available FlexConfig C SlexConfig Object	Selected Pr	epend FlexConfigs	
×	#	Name	Description
Ger Defined TCP. Bypass Gystem Defined Default_DNS_Configure Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Disable DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure DNS_Configure			
Eiarp Configure	Selected Ap	ppend FlexConfigs	
Eigrp_Interface_Configure	#	Name	Description
Eigrp_UnConfigure Eigrp_Unconfigure_All Inspect_IPv6_Configure Inspect_IPv6_UnConfigure ISIS_Configure ISIS_Interface_Configuration ISIS_Unconfigure ISIS_Unconfigure_All Netflow_Add_Destination Netflow_Clear_Parameters	1	TCP_Bypass	TCP State Bypass 🔍 🖏

Deploy Policies Version: 2017-08-22 12:02 PM



确认

通过SSH或控制台访问FTD,并使用命令system support diagnostic-cli。

> system support diagnostic-cli Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available commands. firepower# show access-list TCP_Bypass access-list TCP_Bypass; 1 elements; name hash: 0xec2b41eb access-list TCP_Bypass line 1 extended permit object-group ProxySG_ExtendedACL_34359739205 object Host1 object Host2 log informational interval 300 (hitcnt=0) 0x42940b0e access-list TCP_Bypass line 1 extended permit ip host 1.1.1.1 host 1.1.1.2 log informational interval 300 (hitcnt=0) 0x769561fc firepower# show running-config class-map 1 class-map inspection_default match default-inspection-traffic class-map tcp_bypass match access-list TCP_Bypass 1 firepower# show running-config policy-map policy-map type inspect dns preset_dns_map

parameters message-length maximum client auto message-length maximum 512 no tcp-inspection policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect ip-options UM_STATIC_IP_OPTIONS_MAP class class-default set connection advanced-options UM_STATIC_TCP_MAP policy-map tcp_bypass_policy class tcp_bypass set connection advanced-options tcp-state-bypass

故障排除

要排除此功能故障,这些命令会有所帮助。

show conn [detail]
 Shows connection information. Detailed information uses flags to indicate special connection characteristics.
 For example, the "b" flag indicates traffic subject to TCP State Bypass

- show service-policy Shows service policy statistics, including Dead Connection Detection (DCD) statistics

相关链接

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/conns_connlimits.html

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118995-configure-asa-00.html

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html