配置网络AMP的Firepower有ASDM的模块或文件 控制。

目录

 箇介

 先决条件

 要求

 使用的组件

 背景信息

 配置文件控制/network AMP的文件策略

 配置文件控制/network AMP的文件策略

 配置文件控制/network AMP的文件策略

 配置文件访问控制

 Configure network恶意软件保护(网络AMP)

 配置文件策略的访问控制策略

 实施访问控制策略

 监控文件策略事件的连接

 验证

 故障排除

 相关信息

简介

本文描述Firepower模块和方法的网络提前的恶意软件保护(AMP) /file访问控制功能用可适应安全设备管理器(ASDM)配置他们。

<u>先决条件</u>

<u>要求</u>

Cisco 建议您了解以下主题:

- •可适应安全工具(ASA)防火墙和ASDM的知识。
- Firepower设备知识。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 运行软件版本5.4.1的ASA Firepower模块(ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)及以后。
- ASA Firepower模块(ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X)该运行软件版 本6.0.0及以后。
- ASDM 7.5.1及以后。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

背景信息

恶意的软件/恶意软件在组织网络能输入通过多种方式。为了识别和减轻此恶意的软件和恶意软件的作用,Firepower的AMP功能可以用于为了检测和或者阻塞恶意的软件和恶意软件发射在网络。

使用文件控制功能,您能选择监控(检测),阻塞或者允许文件加载和下载转移。例如,由用户阻塞 可执行文件下载的文件策略可以实现。

使用网络AMP功能,您能选择您希望在常用的协议监控,并且发送SHA 256切细的文件类型,文件 的元数据从文件,甚至复制到恶意软件分析的Cisco安全智能Cloud。Cloud文件的回归处理切细如 根据文件分析的干净或有恶意。

作为您的整体访问控制配置一部分,文件控制和AMP Firepower的可以配置作为文件策略和使用。 文件策略关联与访问控制规则检查网络流量符合规则情况。

Note:保证Firepower模块有一个保护/控制/恶意软件许可证为了配置此功能。为了验证许可证 ,请选择**Configuration> ASA Firepower Configuration>许可证。**

配置文件控制/network AMP的文件策略

配置文件访问控制

登陆对ASDM并且选择**Configuration> ASA Firepower Configuration>策略>文件。 新的文件策略**对 话框出现。

输入一个名称和可选说明您新的策略的,然后点击**存储ASA Firepower更改**选项。文件策略规则页 出版。

ASA FirePOWER Configur 라 무	Configuration > AS	A FirePOWER Con	figuration > Policies > Files			
Policies Policies Access Control Policy ⊕ Intrusion Policy Files					Compare Policies	New File Policy
SSL Actions Alerts Identity Policy	File Policy	New File Po	licy	? ×	ed Add a new policy	
DNS Policy Device Management Object Management		Description	Network file Access Control		rad a new poney	
Local Gonfiguration Onfiguration		Store A	5A FirePOWER Changes	ancel		

单击**增加文件规则**为了增加规则到文件策略。文件规则给您对您要为恶意软件记录,阻塞或者扫描 的文件类型的粒状控制。

应用程序协议:指定应用协议作为其中**任一**(默认)或特定协议(HTTP、SMTP, IMAP, POP3, FTP, SMB)。

转移的方向:指定文件传输的方向。它能是其中任一或根据应用协议的加载/下载。您能检查协议 (HTTP, IMAP, POP3, FTP, SMB)文件下载的和协议(HTTP, SMTP, FTP, SMB)文件加载 的。请使用**所有**选项为了检测在多个应用程序协议的文件,不管用户是否发送或接收文件。

操作:指定文件访问控制功能的操作。操作是**检测文件**或**块文件。 检测文件**操作生成事件,并且**块** 文件操作生成事件并且阻塞文件发送。使用**块文件**操作,您能或者选择**重置连接**终止连接。

文件类型类别:选择您希望到块文件或生成警报的文件类型类别。

文件类型:选择文件类型。文件类型选项给一更加粒状的选择的选项特定文件类型。

选择存储ASA Firepower更改选项保存配置。

pplication Protocol	Any	Action Kelles		
ile Type Categories		File Types	Selected File Categories and Types	m
Office Documents	20	Search name and description	L Category: Multimedia	9
Multimedia	18	🗋 All types in selected Categories 🔺	L Category: Archive	U
Multimedia Fyseutables	30	TZ (7-Zip compressed file)	4 Category: Office Documents	ü
Executables	11	ACCDB (Microsoft Access 2007 file)		
Encoded	2	AMF (Advanced Module Format for digita	Add	
Lincouleu	2	AMR (Adaptive Multi-Rate Codec File)		
Graphics	12	ARJ (Compressed archive file)		
Graphics	12	ASF (Microsoft Windows Media Audio/Vid		
Graphics				
 Graphics System files 		BZ (bzip2 compressed archive)		

Configure network恶意软件保护(网络AMP)

登陆对ASDM并且导航到**Configuration> ASA Firepower Configuration>策略>文件。** 文件策略页出版。现在请单击新的文件策略对话框出现。

输入一个**名称**和可选说明您新的策略的,然后点击**存储ASA Firepower更改**选项。文件策略规则页 出版。

ASA FirePOWER Configur 🗗 🗜	Configuration > ASA Fire	POWER Configura	ition > Policies > Files				
Policies Access Control Policy Ontrol Policy Ontrol Policy Files SSL	Default SSL SSL Policy	Policy					
Actions Alerts	Els D. Bar	New File Pol	licy Network_Malware_Protection	? ×		Compare Policies	New File Policy
Gobject Management Local Gonfiguration Gonfiguration Time	File_Access_Contro	Description Store AS	Network AMP	ncel	39:53 1in"		0 6

单击**添加文件规则**选项添加规则对文件策略。文件规则给您对您要为恶意软件记录,阻塞或者扫描 的文件类型的粒状控制。

应用程序协议:指定其中任一(默认)或特定协议(HTTP、SMTP, IMAP, POP3, FTP, SMB)

转移的方向:指定文件传输的方向。它能是其中任一或根据应用协议的加载下载。您能检查协议 (HTTP, IMAP, POP3, FTP, SMB)文件下载的和协议(HTTP, SMTP, FTP, SMB)文件加载 的。请使用**所有**选项检测在多个应用程序协议的文件,不管发送或接收文件的用户。

操作:对于网络恶意软件保护功能,操作是恶意软件Cloud查找或阻塞恶意软件。操作恶意软件 Cloud查找生成仅事件,而操作块恶意软件生成事件以及阻塞恶意软件文件发送。

Note:恶意软件Cloud查找andBlock恶意软件规则允许Firepower计算SHA-256哈希和发送它为 了网云查找进程能确定穿程网络的文件是否包含恶意软件。

文件类型类别:选择特定文件类别。

文件类型:选择更加粒状的文件类型的特定**文件类型**。

选择选项存储ASA Firepower更改保存配置。

pplication Protocol	Any	Action Block Malware		
ile Type Categories		File Types	Selected Fi	le Categories and Types
Office Documents	16	Search name and description	Categor	y: PDF files
V Archive	17	All types in selected Categories	Categor	y: Executables
Multimedia	2	TZ (7-Zin compressed file)	Categor	y: Archive
Executables	7	ARI (Compressed archive file)		
PDF files	1	BINARY DATA (Universal Binary/Java By	Add	
Encoded	0	BINHEX (Macintosh BinHex 4 Compresse		
Graphics	0	BZ (bzip2 compressed archive)		
	2	CPIO_CRC (Archive created with the cpio		
System files		CPIO_NEWC (Archive created with the cr		
System files				

Note:文件策略把柄文件按以下规则操作顺序:阻塞优先于恶意软件检查,优先于简单检测和 记录日志。

如果配置基于网络先进的恶意软件保护(AMP),并且Cisco Cloud不正确地检测文件的处理,您能添 加文件到文件列表使用SHA-256 Hash值改善在将来检测文件处理。根据文件列表种类,您能执行 :

•要对待文件,好象网云分配一个干净的处理,请添加文件到干净的列表。

• 要对待文件,好象网云分配恶意软件处理,请添加文件到定制列表。

配置此,导航到Configuration> ASA Firepower Configuration>对象Management>文件列表和编辑 列表添加SHA-256。

ASA FirePOWER Configur 리 무	Configuration > ASA FirePOWER Configuration	n > Object Management > FileList		
Device Management			🔍 Filter	
 Object Management Network 	Name	Number of Entries		
Port Security Zones	Clean-List	0	Ø	6
Application Filters	Custom-Detection-List	2	Ø	
Individual Objects A Object Groups				
GeoLocation				
SecurityIntelligence				
DNS Lists and Feeds				
Sinkhole				

配置文件策略的访问控制策略

如此镜像所显示,导航对Configuration> ASA Firepower Configuration>策略>访问控制策略,并且 创建新建的**访问规则**或编辑现有**访问规则**。

要配置文件策略,操作应该是准许。导航对检查选项卡,并且选择从下拉菜单的**文件策略**。

对启用日志,请导航**日志选项**,并且选择适当的日志选项&**日志文件**选项。点击"Save"/Add<mark>按钮</mark>保 存配置。

选择选项存储ASA Firepower更改保存AC策略变更。

ASA	ASA FirePOWER	raffic								
d Duk		Ianic								
Name	Network-AMP		▼ IPS:	no polic	✓ Enabled ies Variables: n/a	Insert Files: Network_1	below rule Ialware_Pro I	✓ 1 Logging: files: Event	: Viewer	
Zones	s Networks 🔺 Us	ers Applications	Ports	URLs	🔺 ISE Attributes			Inspection	Logging	Com
	Policy	No.			1	ariable Set				
ntrusion										

实施访问控制策略

导航对ASDM**部署**选项,并且选择**部署**从下拉菜单的**Firepower崔凡吉莱**选项。点击**Deploy**选项部署 更改。

Jeploy FirePOWER Changes	
Deploy Policies Version:2016-01-07 11:57 AM	
D Access Control Policy: Default Allow All Traffic	
Intrusion Policy: Balanced Security and Connectivity	
🔊 Intrusion Policy: No Rules Active	
Communication Policy: IPS_Policy	
DNS Policy: Default DNS Policy	
System Policy: Default	
ට Sensor Policy: firepower	
	Deploy Cancel

导航对Monitoring> ASA Firepower Monitoring>任务状态。保证任务必须完成应用配置更改。

Note:在版本5.4.x,适用于访问策略传感器,您需要clickApply ASA Firepower更改。

文件策略事件的箴言报连接

为了看到Firepower模块生成的事件与文件策略涉及,导航对**Monitoring> ASA Firepower** Monitoring>实时Eventing。

ing > ASA FirePOWER Mon	itoring > Real Time Ev	<u>venting</u>					ć
e Eventing							
All ASA FirePOWER Even	nts Connection Intru	usion File Malware File	Security Intelligence				
ter							
eason=File Monitor 🕷							
Pause Refresh F	ate 5 seconds	• 1/7/16 12:06:30	D PM (IST)	•			±Ш
Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP	Sou
/6/16 1:29:48 PM	Allow	1/6/16 11:38:29 AM	1/6/16 1:26:46 PM	File Monitor	192.168.20.3	10.76.76.160	6073
/6/16 2:21:23 AM	Allow	1/6/16 2:16:47 AM	1/6/16 2:18:21 AM	File Monitor	192.168.20.3	13.107.4.50	5832
l/5/16 9:22:57 PM	Allow	1/5/16 9:16:21 PM	1/5/16 9:22:56 PM	File Monitor	192.168.20.3	46.43.34.31	5512
/5/16 9:21:27 PM	Allow	1/5/16 9:15:15 PM	1/5/16 9:21:26 PM	File Monitor	192.168.20.3	46.43.34.31	5511
1/5/16 9:12:44 PM	Allow	1/5/16 9:10:44 PM	1/5/16 9:12:43 PM	File Monitor	192.168.20.3	23.3.70.24	5503

<u>验证</u>

当前没有可用于此配置的验证过程。

<u>故障排除</u>

保证文件策略正确地conifigured与协议方向动作文件类型。 保证那在访问规则包括的正确文件策略 。

保证访问控制策略部署成功地完成。

监控连接事件&文件事件(Monitoring> ASA Firepower Monitoring>实时Eventing)验证,如果通信流 点击正确规则。

相关信息

• <u>技术支持和文档 - Cisco Systems</u>