



Cisco FireSIGHT 和 ISE 快速威胁控制解决





目录

关于本文档	4
技术概述	5
FireSIGHT 领域配置	8
配置 LDAP 连接	8
用户 LDAP 信息样本	10
在使用 pxGrid 的独立环境中配置自签名证书的 ISE	11
将 ISE 身份自签名证书导入到 ISE 受信任证书库中	11
配置自签名证书的 FireSIGHT 管理中心	13
使用自签名证书配置 pxGrid 代理	18
CA 签名操作的自定义 pxGrid 模板	21
在使用 pxGrid 的独立环境中配置 CA 签名证书的 ISE	24
配置 CA 签名证书的 FireSIGHT 管理中心	27
使用 CA 签名证书配置 pxGrid 代理	
FireSIGHT pxGrid 补救模块	31
上传 FireSIGHT pxGrid 补救模块	31
创建新实例	31
创建 FireSIGHT pxGrid 缓解类型	
隔离	32
portBounce	
重新身份验证	33
关闭	
终止	
FireSIGHT pxGrid 入侵策略	
FireSIGHT 连接规则	40
配置 ISE EPS 服务和隔离授权策略	43
FireSIGHT 管理中心关联策略	45
隔离	
测试	47
端口跳转	

cisco.

	测试	51
	端口关闭	54
	测试	56
	重新身份验证	58
	测试	60
	终止	63
	测试	65
取消隔离关	联策略	67
	测试	69
故障排除		72
	ISE pxGrid 服务未显示	72
	pxGrid 代理证书错误消息	72
	, FireSiGHT 管理中心未与 ISE 进行通信	72
	在 FireSIGHT 管理中心内未出现关联事件	72
	FireSIGHT 尝试缓解失败	72
	缓解"查询失败"尝试	72
	从 FireSIGHT 管理控制台发出表明 pxGrid 尝试连接失败的系统日志错误消息	73
	通过将自签名证书导入到 ISE 系统库中进行验证	74
解决方案警	告	76
	pxGrid 和身份映射服务重新启动	76
		76
参考		77

关于本文档

本文档面向对于使用(平台交换网格)pxGrid 的自适应网络控制 (ANC) 缓解操作对终端采取操作,从而通过 思科身份服务引擎(ISE 1.3 或更高版本)来部署 FireSIGHT 管理中心 (5.4) 感兴趣的思科工程师和客户。请注 意,这仅适用于 FireSIGHT 管理中心 5.4,对于 FireSIGHT 管理中心 6.0 不适用。

本文档提供有关在使用自签名证书以及使用已启用 pxGrid 的证书颁发机构 (CA) 签名证书的独立环境中通过 ISE 配置 FireSIGHT 管理中心的详细信息。涵盖 pxGrid 补救模块、pxGrid 代理安装和配置详细信息。pxGrid 补救模块提供 pxGrid ANC 缓解功能:隔离、端口退回、端口关闭、重新身份验证、终止和取消隔离。pxGrid 代理提供证书信息以及 FireSIGHT 管理中心与 ISE pxGrid 节点之间的 ISE pxGrid 节点连接信息。对于每个 ANC 缓解操作类型,将会定义关联策略、规则、补救类型。

读者应该对 FireSIGHT 管理中心和身份服务引擎 (ISE) 访问控制系统有一定的熟悉。假设已安装 FireSIGHT 管理中心 5.4 和独立 ISE 1.3 或 ISE 1.4 环境。FireSIGHT 管理中心 5.4 还在 ISE 2.0 上进行了测试。

以下软件版本用于本文档的测试:

- FireSIGHT 管理中心 5.4
- FireSIGHT 设备虚拟传感器 5.4
- 思科身份服务引擎 ISE 1.3 和 ISE 1.4
- FireSIGHT pxGrid 补救模块 1.0
- FireSIGHT pxGrid 代理 1.0
- Microsoft CA 2008 R2 Enterprise

有关在分布式 ISE 环境中配置 ISE pxGrid 的信息,请参阅"参考"部分中的链接。另外包括使用以 MAC 为 pxGrid 客户端的 CA 签名证书和自签名证书的操作部署指南链接作为参考。



技术概述

思科的平台交换网格 (pxGrid) 在 IT 基础设施中启用多供应商、跨平台网络系统协作。它允许例如安全监控和 检测系统、网络策略平台、资产和配置管理、身份和访问管理平台以及几乎任何其他 IT 操作平台。pxGrid 使 用身份服务引擎 (ISE) 策略服务器提供身份验证、授权和访问控制 (AAA)。

pxGrid 框架包括以下内容:

pxGrid 发布程序 - 发布相关主题或功能

pxGrid 控制器 - 管理所有 pxGrid 客户端身份验证、授权、功能和订阅列表

pxGrid 用户(也称为 pxGrid 客户端)-订阅所发布的 pxGrid 主题。



FireSIGHT ISE 补救模块是 pxGrid 客户端,并通过 ISE 发布/订阅方法提供缓解操作。

ISE 发布会话目录和终端保护服务。会话目录显示 ISE 会话目录中 pxGrid 会话对象的现有属性。其中包括:

会话状态

IP 地址

用户名

用户 AD 域

MAC

NAS IP 地址

TrustSec 安全组名称

终端配置文件名称

分析策略名称

终端安全评估状态

审计会话 ID

帐户会话 IP(RADIUS AV 对中的最后更新时间)

端点保护服务显示以下 pxGrid ANC 缓解对象:

隔离

取消隔离

终止

端口退回

关闭

FireSIGHT 代理作为 pxGrid 客户端注册到 ISE pxGrid 节点,并且订阅终端保护服务主题和 EPS 会话组,从而 执行 pxGrid ANC 缓解操作。

ahaha				License Warning 🔥 ise1	14 admin Logout Feedback	۹.
cisco Identity Services E	ingine	☆ Home Operations ▼ Policy	Guest Access	Administration 🔍		Setup Assistant 🔻
🐝 System 🛛 🖓 Identity Ma	anagement 🛛 🔛 Network Resourc	es 🛃 Device Portal Management	pxGrid Services	Feed Service	lentity Mapping	
Clients Live Log			k			o-Registration Disable Auto-Registratio View By Capabilitie
✓ Enable Ø Disable Ø Appro	we 📵 Group 👎 Decline 🛞 Dele	ete 👻 🍕 Refresh 🛛 Total Pending Appr	oval(0) 👻		1 - 3 of 3 Show 25 -	per page Page 1 🗘 of 1
Client Name	Client Description	Capabilities	Status	Client Group	Log	
□ ▶ ise-admin-ise14		Capabilities(3 Pub, 1 Sub)	Online	Administrator	View	
□ ▶ ise-mnt-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View	
☐ ▼ fsmc-agent-sd	Cisco FireSIGHT Manageme	nt Ce Capabilities(0 Pub, 1 Sub)	Online	EPS	View	
•	Capability Detail			1-1 of 1 Show 25 * pt	er page Page 1 🗍 of 1	
	Capability Name	Capability Version	Messaging Role	Message Filter		
	O EndpointProtectionService	1.0	Sub			

通过将 pxGrid 代理和 pxGrid 补救模块上传到 FireSIGHT 管理中心,执行实际 FireSIGHT pxGrid 集成。

pxGrid 代理安装有三个作用:

安装 pxGrid 服务和支持库

- 配置 pxGrid 连接参数,例如 pxGrid 节点 IP 地址、主机/身份证书、主机私钥证书和受信任 CA 根
- 启动 pxGrid 服务,处理来自 pxGrid 补救模块的缓解操作请求,并将信息发送到 ISE pxGrid 节点。
- pxGrid 补救模块将所有 pxGrid 交互都移交到 pxGrid 服务,并从 ISE pxGrid 节点获取通知结果。

FireSIGHT pxGrid 补救模块将 pxGrid ANC 缓解操作请求发送到 FireSIGHT pxGrid 服务,由其根据 pxGrid GCL 库处理这些请求,然后将此信息发送到 ISE pxGrid 节点。将在对主机和用户开启网络发现的情况下配置 Microsoft AD 领域,以使 FireSIGHT 管理中心获取终端的用户登录/注销信息和操作系统详细信息。

Cisco Sourcefire 和 pxGrid 集成



FireSIGHT 领域配置

系统将会定义提供 LDAP 用户信息的身份验证服务器。此外,还会启用用户感知并开启网络发现,以提供用户登录/注销详细信息和主机信息及操作系统详细信息。

配置 LDAP 连接

第1步: 策略 (Policies)->用户 (Users)->添加 LDAP 连接 (Add LDAP Connection),进入以下选项:

Overview Analysis	Policies Devices Objects	АМР							
Access Control Intr	usion • Files Network Discover	ry SSL Application Detectors	Users Correlation	Actions 🔻					
	External Authentication Obj	ect							
	Name *	Lab							
	Description								
	Server Type	MS Active Directory \$	MS Active Directory ÷						
	Primary Server								
	Host Name/IP Address *	192.168.1.14		ex. IP or hostname					
	Port *	389	389						
	Backup Server (Optional)								
	Host Name/IP Address			ex. IP or hostname					
	Port	389							
	LDAP-Specific Parameters								
	Base DN *	dc=lab6,dc=com	Fetch DNs	ex. dc=sourcefire,dc=com					
	User Name *	Administrator		ex. cn=jsmith,dc=sourcefire,dc=com					
	Password *	•••••							
	Confirm Password *	•••••							
	Encryption	○ SSL ○ TLS ● None							
	SSL Certificate Upload Path	Browse No file selected.		ex. PEM Format (base64 encoded version of DER)					
	Timeout (Seconds)	30							

第2步: 启用 (Enable)->用户/组访问控制参数 (User/Group Access Control Parameters)->获取组 (Fetch Groups)

User/Group Access	Control Parameters		
Enable			
Group Filter	Available Groups <none></none>	Groups to Include Account Operators Administrators Allowed RODC Password Replica Backup Operators Groups to Exclude > Groups to Exclude	Users in Groups to Include will be used for User Awareness.
	Fetch Groups		Users in Groups to Exclude will be excluded from User Awareness.

第3步: 测试和保存

注意: 请为"用户感知" (User Awareness) 包含所有组

第4步: 激活 LDAP 连接,点击->以下按钮



第5步: 您应该看到以下内容:

Overview Analysis Policies Devices Objects AMP			🛕 Health System Help 🔻 admin 🔻
Access Control Intrusion • Files Network Discovery SSL Applica	ion Detectors Users Correlation	Actions 🔻	
			External Authentication
	Task Notification <u>Task Status</u> Your task Installation Setup succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Ch task status to monitor progress.	X (Register) eck	N
	Success Successfully enabled LDAP connection	×	
LDAP Connections			
LDAP server connections that contain user accounts and information			O Add LDAP Connection
Name			
Lab			🔽 🖉 🖗 🗊

第6步: 对主机、用户和应用启用网络发现

策略 (Policies)->网络发现 (Network Discovery)->并点击->铅笔->选择主机、用户和应用 (Hosts, Users and Applications)->保存 (Save)

Overview Analysis Policies Devi	ces Objects AMP			🔺 Health System Help 🔻	admin 🔻
Access Control Intrusion • Files	Network Discovery SSL Application	on Detectors Users Correlation A	Actions 🔻		
				Custom Operating Systems Custom	Topology
Networks User Advanced				Up to date on all targeted devices.	🖌 Apply
				•	Add Rule
Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action	
≈ 0.0.0.0/0 ≈:/0	any	none	none	✓ Discover: Hosts, Users, Applications	a 🛛

2015-09-08 20:10:03

<u>192.168.1.51</u>

用户 LDAP 信息样本

"用户活动"(User Activity)屏幕显示最终用户信息

Overview Analysi	s Policies D	evices Obje	cts AMP	•							🔺 Health	System	Help 🔻	admin 🔻
Context Explorer C	onnections •	Intrusions •	Files 🔻	Hosts • Use	ers ► User Activity	Vulnerabilities •	Correlation •	Custom •	Search					
									Bookm	ark This Page Report	Designer Dash	board Viev	Bookmark	s Search
User Activity														
					Task Notif Task Status Y succeeded at Sensors are b monitor prog	fication 'our task Installation Se Mon Sep 7 12:30:51 20 being registered. Check ress.	tup (Register) 015 task status to	×						
Table View of Events	Users										2015-09-08 17	:02:00 - 20)15-09-09	18:45:00 Static
No Search Constraints (Edit Search)														
□ ▼ <u>Time</u> ×			Event ×	Use	ar × j	User Type ×	IP Add	ress ×		Description ×		Device	×	
J <u>2015-09-08</u>	20:16:06		User Login	 _i	jeppich	LDAP	192	.168.1.7				192.168	.1.51	

此外,如果点击下面的 PC 图标,则将收到以下 IP 地址的"主机配置文件"

User Login 📑 jeppich 🗖 LDAP 📑 192.168.1.7

●	rtual Defense Center 64bit 5.	4.0 Build 763 (se	d.lab6.com) – admin	La construction de la constructi	N						10 ⁷⁰
A https://192.168.1.	50/network_map/view_host.cgi	?ip=192.168.1.7									
Host Profile			Scan Host Genera	te White List Profile	▼ C Q Search ☆ 自 🛡 🖡 🏫					↓ ♠ 9	9 =
IP Addresses	dresses 192.168.1.7								🔺 Health Syste	m Help v a	ıdmin v
NetBIOS Name	JEPPICH-PC 102 168 1 51 (0)				erabilities 🔻	Correlation •	Custom v	Search			
MAC Addresses (TTL)	00:0C:29:C8:EB:4F (VMware	, Inc.) (255)						Realizade This Dage Depen	Decisional Dashboard	liou Rookmarke	Conroh
Host Type	Host							bookinark mis rage Repon	C Designer Dashboard		Search
Last Seen	2015-09-08 20:16:07										
Current User	John Eppich (jeppich, LDAP)						~				
View	Context Explorer Connection	Events Intrusion E	vents File Events Ma	lware Events	n		^				
Indications of Cor	npromise (0)		(CEdit Rule States	p 7 12:30:51 20 pistered. Check	tup (Register) 015 task status to					
Operating System	1 🔻		🥔 Edi	t Operating System					2015-09-08 17:02:00	- 2015-09-09 18	:45:00 🕑
Vendor	Product	Version	Source								Static
Microsoft	Windows	7	FireSIGHT								
Com. (1)					pe ×	IP Address ×		Description ×	Dev	ice ×	
Servers (1) +						I 92	2.168.1.7		<u>192.</u>	168.1.51	
Protocol Port	Application Protocol	Vendor a	nd Version			192	2.168.1.7		<u>192.</u>	168.1.51	
tcp 445	NetBIOS-ssn (SMB)			2 🔍 📑 🕤		I 192	2.168.1.7		192.	168.1.51	
Applications (7) -						i 192	2.168.1.7		<u>192.</u>	168.1.51	
Application Protocol	Client	Marrian	Web Application			I9 2	2.168.1.7		<u>192.</u>	168.1.51	
Application Protocol	Client	version	web Application			I92	2.168.1.7		<u>192.</u>	168.1.51	
WSDD	WSDD		-			I 192	2.168.1.7		192.	168.1.51	
HTTP	Firefox	40.0	Google			I9 2	2.168.1.7		<u>192.</u>	168.1.51	
<pre>I< < Page 1 of 1 ></pre>	> Displaying rows 1-8 of 8 row	vs									

此主机配置文件包含用户历史记录信息、主机协议和漏洞信息。

Users	2015-09-07 20:33:54		2015-09-08 20:33:54
John Eppich (jeppich, LDAP	1		
Attributes			Contract Edit Attributes
Protocol		Layer	
icmp		Transport	ü
tcp		Transport	5
udp		Transport	5
ipv6-icmp		Transport	5
IP		Network	5
ARP		Network	5
RARP		Network	5
IP Version 6		Network	5
II Version o			

在使用 pxGrid 的独立环境中配置自签名证书的 ISE

本节分步说明在使用 pxGrid 的独立环境中使用自签名证书配置 ISE 的过程。

将 ISE 身份自签名证书导入到 ISE 受信任证书库中

这对于 ISE 信任自签名证书是必需的。

<u>注意</u>:请注意,这在 ISE 2.0 中不是必需的。默认情况下,在 ISE 中启用 pxGrid 后,将会显示所发布的节点,并将建立与 ISE pxGrid 节点的连接。 此 ISE 身份自签名证书受信任。

第1步: 选择->管理 (Administration)->系统 (System)->证书 (Certificates)->系统证书 (System Certificates)-> 选择 ISE 自签名身份证书

								License Warning 🛕 ise14	admin Logout Feedback	Q		
CIS	o Identit	y Services Engine	e		🟠 Home	Operations V	Policy V Guest Acce	ess 🔹 Administratio	n 🔻		Set.	up Assistant •
•	System	🚰 Identity Manager	nent	Network Res	sources 🛃	Device Portal Manag	jement 🛛 🔂 pxGrid Se	ervices 🔂 Feed S	Service 💶 📲 pxGrid Identi	ty Mapping		
Dep	loyment	Licensing Cer	rtificates	Logging	Maintenance	Backup & Rest	ore Admin Access	Settings				
Cer	Certificate Management System Certificates 🛆 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.											
Ove	rview			🖊 Edit	Generate Self Si	gned Certificate	F Import Export	X Delete Vi	ew			
Sys	tem Certificate	5		Friendly N	lame	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	3
End	point Certifica	ites		Default se ertificate	elf-signed server c	Admin, Portal, EAP	Default Portal Certificate Group ()	ise14.lab7.com	ise14.lab7.com	Sat, 22 Aug 2015	Sun, 21 Aug 20	16 🗹

第2步: 仅导出证书, 点击->导出 (Export)

	ahaha							License	Warning 🔥 ise14
	cisco Identi	ty Services Engine		💧 Home	Operations •	Policy 🔻	Guest Access	Administration •	
(💀 System	Analytic Management	Network Res	ources 🛃	Device Portal Mana	igement	a pxGrid Services	Feed Service	2 pxGrid Identity
	Deployment	Licensing Certificate:	Logging	Maintenance	Backup & Res	store Ad	dmin Access Set	ttings	
	Certificate Man	agement	System Certi	ficates 🔺 For	disaster recovery it	is recommend	ded to export certificat	e and private key pairs	of all system certificates.
	Overview		💋 Edit	Generate Self Si	gned Certificate	Import	Export X C	Delete View	
ľ	Durkens Centificati		Friendly N	ame	Used By	Portal grou	up tag Is	sued To	Issued By
L	System Certificati	es V	▼ ise14	Export Cert	ificate 'Default s	self-signed	server certificate'		×
	Endpoint Certifica	ates	Default se ertificate	-11		(Export Certificate Or	nlv	
	Trusted Certificat	es	G sd.lab7.co 00001	n		C	Export Certificate ar	nd Private Key	
	OCSP Client Profi	le			*Private Key	Password			
	Certificate Signing	g Requests		Manajara 6	*Confirm	Password		d 1	af the activity law.
	Certificate Auth	nority		warning: E	xporting a private k	ey is not a se	cure operation. It could	a lead to possible expos	Export Cancel

第3步:将 ISE 身份自签名证书导入到 ISE 受信任库中
 选择->管理 (Administration)->系统 (System)->证书 (Certificates)->受信任证书 (Trusted Certificates)->导入 (Import) ->ISE 身份自签名证书 (PEM)->对 ISE 内的身份验证启用信任->提交 (Submit)

cisco Identity Services Engine	License Warning (), j tech j admin j
System System	Hourie Operations - Policy - Gless Access - Administration -
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Import a new Certificate into the Certificate Store
Overview	* Certificate File Browse Defaultselfsignedservercerti(5).pem
System Certificates	Trusted For: ①
Endpoint Certificates	Trust for authentication within ISE
Trusted Certificates	Trust for client authentication and Syslog Trust for authentication of Clicco Services
OCSP Client Profile	Validate Certificate Extensions
Certificate Signing Requests	Description
Certificate Authority	Submit Cancel

第4步: 在 ISE 节点上启用 pxGrid

管理 (Administration)->系统 (System)->部署 (Deployment)->选择节点->启用 pxGrid, 然后保存 (Save)

alah	License Warning 🔥 ise14	admin
cisco Identity Services Engine	Home Operations Policy Guest Access Administration	
💀 System 🥂 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🕞 Feed Service 💵 🔩 pxGrid Iden	tity Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings	
Deployment → F = * ↔ * Boployment * PAN Failower	Deployment Rodes List > iss14 Edit Node Comma Issting: Profiling Configuration Hostname iss14 FQDN Res14.lab7.com IP Address 10.0.0.15 Node Type Identity Services Engine (ISE) Personas Monitoring Role PRIMARY Make Standalone Monitoring Role PRIMARY Other Monitoring Node Policy Service Plable Session Services (1) Include Node In Node Group Mone Plable Profiling Service Plable Setting Service Plable Profiling Service Plable Profiling Service Plable Profiling Service Plable Setting Setting Service Plable Setting Setti	

第5步:验证 pxGrid 服务是否正在运行。 **管理 (Administration)->pxGrid 服务->启用"启用自动注册"(Enable Auto Registration)**

<u>注意</u>:这可能需要几秒钟时间才能连接

System	A Identity Manage	ement 🎟	Network R	esources	4. Device	Portal Management	R pxGrid Services	Feed Service	Identity Mapping		
ients Li	ve Log	_						Enal	ble	OEnable Auto-Registra	Disable Auto-Re View By C
able 🥝 Die	sable 😋 Approve	😝 Group 🛛 🌪	Decline	Delete 👻	🛞 Refresh	Total Pending Approval(0) -		1 - 2 of 2	Show 25 + per page	Page 1 0
Client Nar	ne	Client Des	cription		Capabilitie	s	Status	Client Group	Log		
ise-admin	-ise14				Capabilitie	s(3 Pub, 1 Sub)	Online	Administrator	View	v	
ise-mnt-is	e14				Capabilitie	s(2 Pub, 0 Sub)	Online	Administrator	View	N .	

配置自签名证书的 FireSIGHT 管理中心

在本节中,FireSIGHT 管理中心 (FMC) 配置为使用自签名证书执行 ISE pxGrid 节点操作。在 FireSIGHT 管理中心上会创建内部 FMC 证书颁发机构,并会导出公钥/私钥对,然后将其导入到 ISE 证书系统库中。内部 FMC 公共证书将导出到 ISE 证书受信任系统库中。ISE 身份自签名公共证书将导入到 FireSIGHT 管理中心受信任 CA 库中。

第1步: 选择->对象 (Objects) > 对象管理 (Object Management) > PKI -> 内部 CA (Internal CAs) ->生成 CA (Generate CA)-> 提供以下认证信息:

在本例中,FMC2是指定给内部 CA 的名称

Overview	Analysis	Policies	Devices	Objects	AMP				🕕 He
Object Mar	nagement								
								Genera	ite CA
Security	y Intelligence	_	Name				Value		
4 🥜 Port			EMC CA				C01 - 6	1-1-7 O	
🛄 Indi	vidual Objects		Gener	ate Intern	al Certificate	e Authorit	у		? ×
🔄 🔁 Obje	ect Groups								
VLAN T	ag		Nam	e:		FMC2			
Indi	vidual Objects								
Cbje	ect Groups		Cour	itry Name (tw	ro-letter code):	US			
June 1	uidual Obiecte		State	e or Province:		Maryland			
- Obje	ect Groups		Loca	lity or City:		Germanto	wn		
Applicat	tion Filters		Orga	nization:		Lab			
\$ Variable	e Set		Orga	nizational Uni	it (Department):	Lab			
File List						Lab			
Security	/ Zones		Com	mon Name:		sd.lab7.co	m		
🎲 Cipher :	Suite List								
4 🗐 Disting	uished Name								
Indi	vidual Objects								
🔁 Obje	ect Groups								
A DKI			Gene	rate CSR			Generate self-sig	aned CA	Cancel
Inte Inte	rnal CAs		Conte				and a set of a sig		

第 2 步: 点击->**生成自签名 CA** (Generate self-signed CA) **第 3 步:** 下载 CA 证书文件,在下方点击->**铅笔**:

Overview Analysis Polic	es Devices Objects AMP	🔺 Health	System Help 🔻 admin 🔻
Object Management			
		Generate CA Generate CA	A Filter
4 🚃 Network	Name	Value	
Individual Objects	fmc2	CN=sd.lab6.com, ORG=Lab, OU=Lab, C=US	/

第4步: 选择下载 (Download)

Overview Analysis Policie	es Devices Objects	AMP	
Object Management			
4 Network	Name	Edit Internal Certificate Authority	? ×
Individual Objects	Name		
Chiest Groups	fmc2	Name: fmc2	
Security Intelligence		▲ Subject:	
Best		Common Name: sd.lab6.com	
a gr Port		Organization: Lab	
		Organization Unit: Lab	
Object Groups		4 Issuer:	
▲ SVLAN Tag		Common Name: sd.lab6.com	
Individual Objects		Organization: Lab	
Collect Groups		Organization Unit: Lab	
		A Not Valid Refore:	
Individual Objects		E 100 Vala Delote:	
Collect Groups		360 / 23.03.35 2013 GMT	
Application Filters		a Not Valid Arter:	
\$ Variable Set		Oct 7 23:03:59 2015 GMT	
🗋 File List		▲ Serial number:	
Security Zones		E6D624E48734213E	
🌼 Cipher Suite List		Certificate Fingerprint:	
4 💐 Distinguished Name		60:5F:77:50:85:B5:58:58:DF:9E:EE:8C:AB:FC:61:76:EB:9E:89:79	
Individual Objects		Public Key Fingerprint:	
Collect Groups		cbaefa2423f429a3702e3260742bbaa065e2afea	
a 🖉 PKI			
Internal CAs			_
Trusted CAs		L Download Save Ca	ancel

第5步: 输入加密密码,然后点击确定(OK)。在本例中,使用 cisco123

Overview Analysis Po	licies Devices Objects	s AMP
Object Management		
Individual Objects	Name	Edit Internal Certificate Authority
 Object Groups Security Intelligence Port Individual Objects Object Groups Win Tan 		Subject: Common Name: sd.lab6.com Organization: Lab Organization: Lab Subject: Lab Lasuer: Lab
 Veck ray Individual Objects Object Groups URL Individual Objects Object Groups Application Filters Variable Set File List 		Common Ni Encrypt Download File ? X Organizatio Organizatio 4 Not Valid Befor Sep 7 23:01 A Not Valid After Oct 7 23:01 A Serial Number: OK Cancel

第6步: 在本地保存.p12文件

Overview Analysis Pol	icies Devices Objects	АМР
Object Management		
		Edit Internal Certificate Authority
Network	Name	● ○ ○ Opening 81e5ada4-55b4-11e5-a8bb-8d638a691462.p12
Individual Objects	fmc2	Name: fmc2 You have chosen to open:
Security Intelligence		Subject: B1e5ada4-55b4-11e5-a8bb-8d638a691462.p12
4 JP Port		Common Nam which is: Binary File (2.4 KB)
Individual Objects		Organization: from: https://192.168.1.50
Content Groups		Organization Would you like to save this file?
A SVLAN Tag		Issuer:
Individual Objects		Common Nam Cancel Save File

第7步: 重命名该.p12文件名以使其更易于处理。在本示例中,文件重命名为fmc2.p12。

第8步: 使用 WinSCP 或其他方法将该文件上传到 FireSIGHT 管理控制台

安全访问操作指南

_									
🎦 54_1 - admin@192.168.1.50 - WinSCP									
Local Mark Files Commands Session Options Remote Help									
🛛 🖶 🚉 😂 Synchronize 🗾 🧬 👔	3 🛛 🖓 🖓	Queue 👻 Transfer Se	ttings Defau	lt - 🧬 -					
admin@192.168.1.50									
				🛯 🕦 a duatio 🖉 🗖 🗐 🖉		🕞 Circle 🖸			
		🖸 🔟 😰 🗠							
🗐 🕼 Upload 🎲 🛛 🖉 Edit 🗶 🚮 🕞 Prope	erties 🚰 [7 + - A		📲 🔂 Download 🙀 📝 Edit 🗙 🛛	🚮 🕞 Properties 📑 🚹 📗	+ - 🗸			
C:\54_1				/Volume/home/admin					
Name Ext	Size	Туре	Change 📤	Name Ext	Size	Changed			
👪		Parent directory	9/7/201	👪		10/2/2014 11:48:14 AM			
Sourcefire_3D_Device_Virtual64_VMware	543 MiB	GZ File	8/12/20	mc2.p12	2,501 B	9/7/2015 6:24:40 PM			
Sourcefire_Defense_Center_Virtual64_V	677 MiB	GZ File	8/12/20						
SFIRETERMFEAT201509071316572380.lic	1,046 B	LIC File	9/7/201						
SFIRETERMFEAT201509071318082390.lic	1,039 B	LIC File	9/7/201						
SFIRETERMFEAT201509071318222590.lic	1,056 B	LIC File	9/7/201						
SFIRETERMFEAT201509071318343330.lic	1,070 B	LIC File	9/7/201						
Sourcefire_3D_Device_Virtual64_VMware	212 B	MF File	10/2/20 =						
Sourcefire_3D_Device_Virtual64_VMware	210 B	MF File	10/2/20						
Sourcefire_Defense_Center_Virtual64_V	222 B	MF File	10/2/20						
Sourcefire_Defense_Center_Virtual64_V	220 B	MF File	10/2/20						
Sourcefire_3D_Device_Virtual64_VMware	5,912 B	OVF File	10/2/20						
Sourcefire_3D_Device_Virtual64_VMware	36,957 B	OVF File	10/2/20						
Sourcefire_Defense_Center_Virtual64_V	4,711 B	OVF File	10/2/20						
Sourcefire_Defense_Center_Virtual64_V	34,856 B	OVF File	10/2/20						
j fmc2.p12	2,501 B	Personal Informati	9/7/201						

第9步: 通过 SSH 传输到 FireSIGHT 管理控制台

第10步:通过键入以下命令将.p12文件转换为 CER 和 KEY 文件:

注意: CER 和 KEY 文件名是随机的。original.p12 文件已重命名为 fmc2.p12

```
sudo openssl pkcs12 -nokeys -clcerts -in fmc2.p12 -out fmc2.cer
Enter Import Password:
MAC verified OK
admin@sd:~$
sudo openssl pkcs12 -nocerts -in fmc2.p12 -out fmc2.key
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
admin@sd:~$
```

第11步: WinSCP 用于将 fmc2.cer 和 fmc2、key 文件从 FireSIGHT 管理中心复制到本地 PC。

💑 admin - admin@10.0.21 - WinSCP 💿 🕞 💽								
Local Mark Files Commands Session Options Remote Help								
💾 🔁 😂 Synchronize 🔳 🥵 👔 🛞 🕼 Queue 🔹 Transfer Settings Default 🔹 💋 🔹								
admin@10.0.0.21 🚅 New Session								
🕌 C: Local Disk 🔹 🤗 😨 🛛 🖛 🕶	-> - 🔁	🖻 🏦 🎜 💁		📗 admin	• 🚰 🔽 (🔶 • 🔿 • 🔂 🕻	🔁 🚡 🔁	🎇 Find Files 🗧 🔒	
📳 Upload 👔 📝 Edit 🗙 🏑 🕞 Prope	erties 📑 📑	+ - V		Download 🙀	📝 Edit 🗙 🛃 🕞 Properties	🖆 🖪 🛙	+ - V	
C:\smc_certs				/Volume/home/adm	nin			
Name Ext	Size	Туре	Changed	Name Ext		Size	Changed	
월		Parent directory	9/5/2015 1	🕹			10/2/2014 11:48:14 AM	
fmc2.cer	1,498 B	CER File	8/31/2015	.bash_history		2,419 B	9/3/2015 2:20:29 PM	
fmc2.key	1,958 B	KEY File	8/31/2015	fmc2.cer		1,498 B	8/31/2015 8:39:40 PM	

第 12 步: FireSIGHT 管理内部 CA 公共证书已导出到 ISE 证书信任库中
 管理 (Administration)->系统 (System)->证书 (Certificates)->受信任证书 (Trusted Certificates)->浏 览 (Browse) 并上传 fmc2.cer

cisco Identity Services Er	igine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼	
👾 System 🦳 💆 Identity M	anagement	📰 Network Resources 🛛 🛃 Device Portal Management 🖓 pxGrid Services 🕞 Feed 🖏 v	ice
💵 pxGrid Identity Mapping			
Deployment Licensing	Certificates	Logging Maintenance Backup & Restore Admin Access Settings	
Certificate Management		Import a new Certificate into the Certificate Store	
Overview		* Certificate File Browse fmc2.cer	
System Certificates		Friendly Name	
Endpoint Certificates	E	Trusted For: (i)	
Trusted Castification		 Trust for authentication within ISE 	
Trusted Certificates		Trust for client authentication and Syslog	
OCSP Client Profile		Trust for authentication of Cisco Services	
Certificate Signing Requests		Validate Certificate Extensions	
		Description	

- 第13步: 启用"信任 ISE 内的身份验证"(Trust for authentication within ISE)->提交(Submit)
- 第 14 步:从 ISE 受信任证书库同时导出 ISE 身份自签名公共证书和私钥。您只需将 ISE 身份自签名公共证书 导出到 FireSIGHT 管理受信任 CA 库中即可。FireSIGHT 管理控制台将此识别为受信任证书。
 管理 (Administration)->系统证书 (System-Certificates)->证书管理 (Certificate Management)->受信
 - 任证书 (Trusted Certificates)->选择 ISE 证书 ->导出公钥和私钥,提供密码

注意:此程序对于 ISE 2.0 仍然相同

aludu .			License Warning	ise14 admin	Logout Feedback
cisco Identity Services En	gine 🏠 H	ome Operations	Policy •	Guest Access	Administration
System 🐉 Identity Ma	inagement 🛛 🔛 Network Re	esources 🛃 Dev	rice Portal Managen	nent 🛛 🗔 pxGr	id Services 🛛 🗔 Feed
2. pxGrid Identity Mapping					
Deployment Licensing	Certificates Logging	Maintenance	Backup & Restore	Admin Acces	is Settings
Certificate Management	Export Certificate 'Default	self-signed server	certificate'		×
Overview		○ Expo	ort Certificate Only		
System Certificates	*Private K	Expo Expo Cey Password ••••••	ort Certificate and F	Private Key	
Endpoint Certificates	*Conf	irm Password			
Trusted Certificates	Warning: Exporting a private	key is not a secure op	eration. It could le	ad to possible expo	sure of the private key.
occo chas parti-					Export Cancel

第 15 步:将 ISE 自签名身份证书导入到 FireSIGHT 管理受信任 CA 库中
 对象 (bjects)->对象管理 (Object Management)->PKI->受信任 CA (Trusted CAs)->添加受信任 CA (Add Trusted CA)->输入名称->保存 (Save)。

• Overview Analysis Po	licies Devices Objects	MP
Object Management		
4 🚃 Network	Name	Value
Distance of the second	A-Trust-nQual-01	Import Trusted Certificate Authority ? × .
Security Intelligence	A-Trust-nQual-03	Name: ISE
Port Individual Objects	A-Trust-Qual-01	Certificate Data or, choose a file: Browse
Cobject Groups	A-Trust-Qual-02	BEGIN CERTIFICATE
VLAN Tag Individual Objects	AAA Certificate Services	PILIDNJCLARNQAWIBAGIQV0JWAAAADUWKL3JCSWIJWABGQTIRUGSWOBAQUHADA2 MRCwFQYDVQDDEwSpc2UxXCSsYWI3LmNvb7AeFw0x/TAAMJuANJISMDdaFw0xNjA4 MIEANITSMBIGSTURAU MAMTHAVITSTEIL avAUVUK V10MMINIANIAAANUVC
Cobject Groups	AC Raz Certicmara S.A.	9w08AQEFAAOCAQ8AMIIBG2KCAQEAvQkmIINF3YYSUG2QrXxRpdY9WWZEC5s/tx
URL Individual Objects	Actalis Authentication Root CA	acvE3jRhKz4omLYfroDE5XWE10AYYXK44bM8HD1Im6hVumHbsg3REEDHiKT3 bi2didthattroffUnDE5XWE10AYYXK44bM8HD1Im6hVumHbsg3REEDHiKT3
Cobject Groups	AddTrust Class 1 CA Root	zkytwHsQa7NRpkcp/ZMpscJBHYHOX5tZvNSWhWekdJrEeGRPvt0BTGvZXB9uOh/
Application Filters	AddTrust External CA Root	cCDryY67cw2utrR4n+V4Sc8+r+i4/SofL3YPrHiA1hnjGK4N/QIDAQABo24wbDAM BoNVHRMEBTADAQH/MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUmSHYs4JtPWWfbxRH
Rie List	AddTrust Public CA Root	ENvo60CnGt4wHQYDVR0BBYwFAYIKwYBBQUHAwEGCCsGAQUF9wMCMBEGCWCGSAGG + EIBAQQEAwIGQDANBgkqhkiG9w0BAQUFAAOCAQEAiFhT/spRWhcnsd1hmr3eP60e
Security Zones	AddTrust Qualified CA Root	Xxn8FMKuSj2t85GMXg+1DK/VRPWf5/WZIdbbNR7Ng5br0lZvkpEOx8w8q8bJd+ <u>Sx</u> VrZrWC3VX79mnqsIoKZ0MXBRpU5PXQQZKMrFv6/IMOM55/wJax7rzPvenJXCgaX4
A 🗐 Distinguished Name	Admin-Root-CA	vffL8aVcwqDMGF80SSqHkmjb0D7kIR2C5zlQ6/s0FLuud7v0ToIWQ0Ek8EaGHYg sizF6t80SYQg8Ry8sACICNMnnrQbM6I+AqcDkIac8HFz1FquDvbafEfz4kUrt8Ip
Individual Objects	AdminCA-CD-T01	logWzzq6Y7b6o9d+BQXBI8dm030PE1z73weuo18rg+Waa67ALnxNPzSFHniH+Q==
▲ 🤌 PKI	AffirmTrust Commercial	Encrypted, and the password is:
Internal CAs	AffirmTrust Networking	Save Cancel "

第16步:将 FireSIGHT 管理内部 CA 公钥/私钥对导入到 FireSIGHT 管理中心的内部证书库中

选择->对象 (Objects)->对象管理 (Object Management)->PKI->内部证书 (Internal Certs)->添加内部 证书 (Add Internal Cert)

针对私钥按照同一程序执行操作

```
注意:删除袋属性,直至到达 ----Begin Certificates
```

Overview Analysis Policies Devices Objects AMP Object Management	
Object Management	
Add Known Internal Certificate	×
Individual Objects Object Groups Security Intelligence Certificate Data or, choose a file: Browse	
Port Individual Digets Conject Groups VUAN Tay VUAN Tay VUAN Tay VUAN Tay Objets Groups VUAN Tay Objets Groups VUAN Tay Objets Groups NUAN Tay Objets Groups NUAN Tay Objets Groups NUAN Tay NUAN Tay Objets Groups NUAN Tay NUAN TAY	
Individual Objects Key or, choose a file: Browse Asplication Fitters Variale Set Tite Lat Generny Zones Coher Suite Lat Distinguished Name	
Individual Objects Depted Groups Prof Save Cancel	

第17步: 请删除密钥文件的袋属性, 直至您正好位于"---Begin…"之前。



第18步: 另请删除 </no> 并输入加密密码



第19步: 您应看到以下内容,点击"确定"(OK)以完成

Add Kno	own Internal Certificate	? ×
Name:	FMC2_InternalCA	
Certifical	te Data or, choose a file: Browse	
MIIDgDC BAYTAIV MAOGA10 MB4XDTI ETAPBgN DANMYW CSqGSIb	IN CERTIFICATE CAmigwill Bagli Alcohuroshince + MAGGCsGoSlb3DQEBBQUAMGcxC2AJBgHV Timeshow YD cyclicahur Y33bGruzze TIMESGALUEBwwRc2V(hVhFudG33)EH E HDCwhc2babDhUI (VXXDTEH TAwktabDHDN) (VXXZELHAAGALUEBHNCVNe VBabCELholmsVisMHMKeQTV0VDDHAPLC2V(VXSDBJMQMVcQFV)VQK VLDDARBgHVBLMAADAH) EUMBIGALUEAwuk 22QUGFRNI3Jb20wgBHA0G SDEBAQUAHBDWWgBKABBACSCR/WVhAm+HGWVQFTR/TDVQcp1	<
Key or, o	choose a file: Browse	
FtlgQtlFn Zrc5Fa6u tjLnpJ8X/ L1xGF/8r pPt3JLkW /D9KeU// SiK6jzXY/ Glw=	nT DostUbe446:5159C201-3 MAR9kr Um9-4H4ffWNL3ENG-JamX5BHEn JouzzBHRK95169H5FHSVSC50520_C20155 031450JH4mBAIACMHvoTD0 ADEI/L52gow0/IKSs66igini2/WH274+Whitt/KB13T5+yvfTRbarxCVD aDEi/L52gow0/IKSs66igini2/WH274F57gLmini/y+amBikDPK9- 1021W57AV2750Q4FH2afFD25H4fB08/V(FRmackJ4CD1ED2F6JouFE 2021W57AV2750Q4FH2afFD25H4fB08/V(FRmackJ4CD1ED2F6JouFE 2021W57AV2750Q4FH2afFD25H4fB08/V(FRmackJ4CD1ED2F6JouFE 2021W57AV2750Q4FH2afFD25H4fB08/V(FRmackJ4CD1ED2F6JouFE 2021W57AV2750Q4FH2afFD25H4fB08/V(FRmackJ4CD1ED2F6JouFE 2021W57AV2750Q4FH2afFD25C02G2aID00Q22eIDAn2Ydq3W6H3EID100W nzWegM0+uu9rOJWV(EH47JFf/COCgCaID00Q22eIDAn2Ydq3W6H3EID100W	^
END	ENCRYPTED PRIVATE KEY	•
Encry	/pted, and the password is:	
	ок	Cancel

使用自签名证书配置 pxGrid 代理

pxGrid 代理负责 FireSIGHT 管理中心和 ISE pxGrid 节点之间的证书配置和通信。需要 ISE pxGrid 节点的 IP 地址。FireSIGHT 管理中心的公共证书和密钥文件对于后续步骤是必需的。

FireSIGHT 管理中心的公共证书将用作主机证书。ISE 身份自签名证书将用作 CA 证书。

FireSIGHT 管理中心的私钥文件将是主机密钥。此外,还将需要密钥的密码。

第1步: 使用 WinSCP 或所选的其他 SCP/SFTP 客户端将 pxGrid 代理上传到 FireSIGHT 管理控制台。



第2步: 使用 WinSCP 或其他方法将 FireSIGHT 内部 CA 公共证书和内部 CA 密钥上传到 FireSIGHT MC /Volume/home/admin

<u>注意</u>:大写/小写语法予以保留

第3步: 通过 SSH 传输到 FireSIGHT 管理中心并键入以下内容:



安全访问操作指南

请参阅样本脚本的以下内容:



Verifying archive integrity...All good. Uncompressing Cisco pxGrid Agent Installer..... Installing the agent... Installing the pxGrid libraries and Perl module... Setting up the agent to be managed by PM... Installation done! Configuring pxGrid... Below you will be asked a series of questions relating to your pxGrid install and the files supporting it. Health alerts WILL be generated by PM until the configuration is completed, however. The answers to these questions will populate the /etc/sf/pxqrid/pxqrid.conf configuration file, which can be manually modified later at any time.A configuration example is provided in the same directory with the filename pxgrid.conf.example. To get this all to work, the agent will need to connect to a pxGrid server. This is typically your Cisco Identity Services Engine instance, which must also have the pxGrid service enabled. What is the IP address of your pxGrid server > 192.168.1.71 Every agent connecting to pxGrid must have a unique host certificate which will be used to identify the agent host.Associated key and CA certs must also be provided. What is the full path and filename to the host certificate? > /Volume/home/admin/fmc2.cer What is the full path and filename to the host key? > /Volume/home/admin/fmc2.key What is the host key password? > cisco123 What is the full path and filename to the CA certificate? > /Volume/home/admin/ise14lab.pem Configuration witten to /etc/sf/pxgrid/pxgrid.conf

第 4 步: 选择->系统 (System)->监控 (Monitoring)->系统日志 (Syslog) 以了解 FireSIGHT 管理中心是否已作 为客户端成功注册到 ISE pxGrid 节点并已订阅 EPS 主题

Overview Analysis Policies Devices	Objects AMP			🔺 He	alth System Help v	admin 🔻
		Local 🔻	Updates	Licenses	Monitoring > Syslog	Tools 🔻
L≱	Task Notification Task Status Your task Installi succeeded at Sun Oct 11 12: Sensors are being reg task status to monitor	ation Setup (Regist 47:00 2015 istered. Check r progress.	× ær)			
Case-sensitive Exclusion	Messages					
pxgrid	Oct 12 2015 13:24:25 sourcefiredc EndpointProtectionServiceCapability	SF-IMS[12566]: p: to connection	xgrid_agent.pl	normal [INFO]	Assigned	
Go	Oct 12 2015 13:24:25 sourcefiredc SF-IMS[12566]: pxgrid_agent.pl:normal [INFO] Connected to pxGrid server					
	Oct 12 2015 13:24:24 sourcefiredc server (192.168.1.71)	SF-IMS[12566]: p	xgrid_agent.pl	normal [INFO]	Attempting to connect to pa	xGrid
	Oct 12 2015 13:24:24 sourcefiredc SF-IMS[3947]: [3947] pm:process [INFO] Started pxgrid_agent (12566)					
	Oct 12 2015 13:23:25 sourcefiredc cleanly	SF-IMS[3947]: [39	947] pm:proce	ess [INFO] Proce	ess pxgrid_agent (12469) ex	rited
	Oct 12 2015 13:23:25 sourcefiredc SF-IMS[3947]: [3957] pm:log [INFO] Process 'pxgrid_agent' closed output.					
	Oct 12 2015 13:23:25 sourcefiredc SF-IMS[3947]: [3957] pm:log [INFO] Process 'pxgrid_agent' closed output.					
	Oct 12 2015 13:23:25 sourcefiredc configuration file	SF-IMS[12469]: p	xgrid_agent.pl	ifatal [WARN] I	No CA certificate defined in t	he
	Oct 12 2015 13:23:24 sourcefiredc	SF-IMS[3947]: [39	947] pm:proce	ess [INFO] Start	ed pxgrid_agent (12469)	

.

第5步: 要在 ISE 中查看,请选择->管理 (Administration)->pxGrid 服务 (pxGrid Services)。请注意, FireSIGHT 管理控制台已注册到 ISE pxGrid 节点 EndpointProtectionService Capability

←	o_xmp_web_page_administration_mes	sagesei 🔻 🤁 🔍 Search	☆ 🖻 🛡 造 🏫 😑
iste ISE diste Defense Center			
cisco Identity Services Engine	▲ Home Operations ▼	License Warning ▲ ise14 admin Policy ▼ Guest Access ▼ A	Logout Feedback 🔎 Administration 🔻 Setup Assis
🐝 System 🛛 🖓 Identity Management 🛛 📱	Network Resources 🛛 🛃 Devi	ce Portal Management 🛛 🕞 pxGrid	Services 😡 Feed Service
Clients Live Log	Darline Obalata - Refath	Total Panding Approval(0) = 1 - 3 of 2	OEnable Auto-Registration Disable Auto-Reg View By Cap
Clients Live Log ✓ Enable ⊘ Disable ⊘ Approve @ Group ♥ ☐ client Name Client Date	Decine 😥 Delete 🔻 🍕 Refresh	Total Pending Approval(0) + 1 - 3 of 3	OEnable Auto-Registration Disable Auto-
Clients Live Log ✓ Enable ⊘ Disable ⊘ Approve ⊕ Group ✓ Client Name Client Des ► ise-mnt-lse14	Decine 😵 Delete 🔻 🍪 Refresh cription Capabilitie Capabilitie	Total Pending Approval(0) + 1 - 3 of 2 s s(2 Pub, 0 Sub) Online	
Clients Live Log	Decine ODelete V Brefresh Capabilitie Capabilitie Capabilitie	Total Pending Approval(0) + 1 - 3 of 3 s Status s(2 Pub, 0 Sub) Online s(3 Pub, 1 Sub) Online	OEnable Auto-Registration Disable Auto-Registration 3 Show 25 • per page Page 1 0 3 Show 25 • per page Page 1 0 Client Group Administrator Administrator Administrator
Clients Live Log	Decine ODelete V Brefresh cription Capabilitie Capabilitie Capabilitie Capabilitie	Total Pending Approval(0) * 1 - 3 of 3 s Status s(2 Pub, 0 Sub) Online s(3 Pub, 1 Sub) Online c(0 Pub, 1 Sub) Online	●Enable Auto-Registration Disable Auto-Reg View By Cal 3 Show 25 ▼ per page Page 1 ♥ or Clent Group Administrator EPS
Clients Live Log Client Name Glient Des Client Name Client Des ise-mrt-ise14 ise-admin-ise14 ise-admin-ise14 Capability Detail	Dedine Opelete V Brefresh cription Capabilitie Capabilitie Capabilitie SIGHT Management Ce Capabilitie	Total Pending Approval(0) * 1 - 3 of 3 s Status s(2 Pub, 0 Sub) Online s(3 Pub, 1 Sub) Online s(0 Pub, 1 Sub) Online	●Enable Auto-Registration Disable Auto-Reg View By Cal 3 Show 25 ▼ per page Page 1 ♥ or Clent Group Administrator EPS 1 - 1 of 1 Show 25 ▼ per page Page
Clients Live Log Client Name Client Name Client Name Client Des ise-mt-ise14 ise-admin-se14 ise-admin-se14 Capability Detail Capability Name	Decine Decine	Total Pending Approval(0) 1 - 3 of 2 s Status s(2 Pub, 0 Sub) Online s(3 Pub, 1 Sub) Online s(0 Pub, 1 Sub) Online Messaging Role	

CA 签名操作的自定义 pxGrid 模板

同时具有客户端身份验证和服务器身份验证的增强型密钥用法 (EKU) 的自定义 pxGrid 模板对于 pxGrid 客户端、FireSIGHT 管理中心和 ISE pxGrid 节点之间的 pxGrid 操作是必需的。这对于 FireSIGHT 管理中心和 ISE pxGrid 节点均由同一 CA 进行签名的证书颁发机构 (CA) 签名环境是必需的。

第1步: 选择->管理工具 (Administrative Tools)->证书颁发机构 (Certificate Authority)->CA 证书旁边的 "+"下拉菜单->右键->点击证书模板 (Certificate Templates)->管理 (Manage)

certsrv - [Certification Aut	ority (Local)\lab7-WIN-LTE11SBAKT	M-CA\Certificate Templates]	
File Action View Help			
(= =) 🖄 🧟 📑 👔	Certificate Templates Console		
Certification Authority (Local)	File Action View Help		
🖻 👼 lab7-WIN-LTE11SBAKTM-C	(≈ ⇒) 🔽 🔍 🚍		
Revoked Certificates	Certificate Templates (WINH TE119	Templata Dicolay Name	Minimum Supported CAr
Pending Requests	Certificate relipiones (with Electro	Administrator	Windows 2000
Failed Requests		Authenticated Session	Windows 2000
Certificate Templates		Basic EFS	Windows 2000
		CA Exchange	Windows Server 2003 Ent

第2步: 右键点击并复制用户模板->选择->Windows 2003 Enterprise->确定 (OK)



第3步: 输入证书模板的名称,取消选中"在 Active Directory 中发布证书"(Publish certificate in Active Directory),并提供有效期和续订期。



第4步: 点击扩展 (Extensions)->添加 (Add)->服务器身份验证 (Server Authentication)->确定 (OK)->应用 (Apply)

Recentificate Templates Console		al	
File Action View Help	Properties of New Template		
Certificate Templates (WIN-BG7GPC	Issuance Requirements Superseded Templates Extensions Security	Ver +	Actions
	To modify an extension, select it, and then click Edit.	110	Certificate Templa 🔺
	Extensions included in this template:	6.1 4.1	More Actions
	Application Policies	5.1	User 🔺
	Basic Constraints Contrictor Emplote Information Issuance Policies Key Usage	4.1 6.1 7.1 8.1 7.1 110 105 101	More Actions
	Description of Application Policies	10C 101	
	Chert Athentication A	5.1 4.1 6.1 11. 5.1 3.1	
×1	OK Cancel Apply Help	3.1 4.1 4.1 101	

第5步: 点击主题名称 (Subject name), 启用在请求中提供 (Supply in request)



第6步: 点击扩展 (Extensions)->颁发策略 (Issuance Policies)->编辑 (Edit)->所有颁发策略 (All Issuance Policies)

🖳 Certificate Templates Console		
File Action View Help	Properties of New Template	
Certificate Templates Console File Action View Help Certificate Templates (WIN-LTE11S Certificate Templates (WIN-LTE11S	Properties of Itew Template X General Request Handling Subject Name Server Issuance Requements Superseded Templates Extensions Security To morifician extension select it and than click Ent Effit Tssuance Policies Extension X Extensi Anissuance policy describes the conditions under which a contribute is issued. X Bring Ke Alissuance policies: Alissuance policies: Alissuance policies Descrit Add Edt	Actions 4.1 100 6.1 4.1 101 5.1 4.1 102 103 104 105 105 101 101 6.1
× ×	Make this extension critical OK Cancel	0.1 11. 5.1 3.1 4.1 4.1 100

第7步: 保留请求处理的默认设置



- **第8步:** 右键->点击证书模板 (Certificate templates)
- **第9步:**选择->新建模板 (New Template) 以发出并选择 pxGrid



第10步: 您应该看到 pxGrid 模板



在使用 pxGrid 的独立环境中配置 CA 签名证书的 ISE

在本节中,将为证书颁发机构 (CA) 签名环境配置 ISE pxGrid 节点。最初,使用 pxGrid 自定义模板从 ISE 节 点生成 "pxGrid" CSR 请求并由 CA 服务器签名。证书将绑定到初始 ISE CSR 请求。

CA 根证书将导入到 ISE 证书受信任库中。ISE 身份证书将在 ISE 证书系统库中导出。将为 pxGrid 操作启用 ISE 节点。

第1步: 请为将成为 ISE pxGrid 节点的 ISE 节点生成 CSR 请求

管理 (Administration)->系统 (System)->证书 (Certificates)->证书签名请求 (Certificate Signing Requests)->生成 (Generate)

<u>注意</u>:只要模板是 pxGrid 自定义模板,证书用途即可是管理、多用途或 pxGrid。

ahah	License Warning
cisco Identity Services Engine	Home Operations Policy Guest Access Administration Administration
System 🛛 👰 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🔂 pxGrid Services 🕞 Feed Service 💵
Deployment Licensing Certifica	tes Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Contificate Similar Request
Overview	Certificate signing Request Certificate types will require different extended key usages. The list below outlines which extended key usages are
System Certificates	ISE Identity Certificates:
Endpoint Certificates	Multi-Use - Client and Server Authentication Admin - Server Authentication EAP Authentication - Server Authentication
Trusted Certificates	Portal - Server Authentication pxGrid - Client and Server Authentication
OCSP Client Profile	ISE Certificate Authority Certificates:
Certificate Signing Requests	ISE Root CA: This is not a signing request, but an ability to generate a brand new Root CA certificate for ti ISE Intermediate CA: This is an International CA Signing Request. Renew ISE COSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP re ISE Root CA/ISE Intermediate CA
Certificate Authority	Usage
Internal CA Settings	Certificate(s) will be used for Admin
Certificate Templates	Allow Wildcard Certificates 📋 🕧
External CA Settings	Generate CSR's for these Nodes:
	Node CSR Friendly Name
	✓ ise14 ise14#Admin

第2步: 将 CSR 信息复制/粘贴到**请求证书 (Request a certificate)->高级证书请求 (Advanced Certificate request)** 中,选择自定义 pxGrid 模板,然后**提交 (Submit)**

To submit a sav Request box.	red request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request
Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	G1A/OKOPkmzOV7mr4HFW2KjQPPS5Z8ognzobOJ/1 ScIKU6R6BIy+mojVxfjH0B+r6QUEALfQ0ZY0kJId rWG1BGLHWUBRyPT8n9uOeNJKNngD2LJyFBPvRIub 67v5h57UApcSZLhh6/Hj+/Dzj1J/o4Od34zAovJp 8xr503L4yPLKMLUQ61/QChp8VQ== END CERTIFICATE REQUEST
Certificate Templa	te:
	pxGrid ÷
Additional Attribu	tes:
Attributes:	

第3步: 下载 base-64 编码格式的 CA 根证书

Microsoft Active Directory Certificate Services - lab6-WIN-49T17723UO8-CA	
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA ce	Prificate.
To download a CA certificate, certificate chain, or CRL, select the certificate	You have chosen to open:
CA certificate: Current [lab6-WIN-49T17723U08-CA] Encoding method: OER OBase 64 Install CA certificate Download CA certificate Download CA certificate	 certnew.cer which is: Document (1.3 KB) from: http://192.168.1.14 What should Firefox do with this file? Open with Keychain Access (default) + Save File Do this automatically for files like this from now on.
Download latest base CRL Download latest delta CRL	Cancel OK

第4步: 将 CA 根证书上传到 ISE 证书受信任系统库中

选择->管理 (Administration)->系统 (System)->证书 (Certificates)->受信任证书 (Trusted Certificates)->上传 CA 根证书

aludu	License Warning 🔬 ise14 admin	Logout
CISCO Identity Services Engine	Home Operations ▼ Policy ▼ Guest Access ▼ Administration ▼	
🔆 System 🦉 Identity Management	📲 Network Resources 🚯 Device Portal Management 🔯 pxGrid Services 🗔 Feed Service 🕰 pxGrid Identity Mapping	
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings	
Certificate Management	Import a new Certificate into the Certificate Store	ķ
Overview	* Certificate File Browse root.cer	
System Certificates	Trusted For: ①	
Endpoint Certificates	✓ Trust for authentication within ISE	
Trusted Certificates	Trust for client authentication and Syslog Trust for authentication of Cisco Services	
OCSP Client Profile	Validate Certificate Extensions	
Certificate Signing Requests	Description	
Certificate Authority	Submit Cancel	

- 第5步: 启用"信任 ISE 内的身份验证"(Trust for authentication within ISE), 然后提交(Submit)
- **第6步:** 将 ISE pxGrid 节点证书上传到 ISE 证书系统库中 选择->管理 (Administration)->系统证书签名请求 (System-Certificate Signing Requests) 并将证书绑 定到 CSR 请求

ahah			License War	ning 🚹 ise14 admin Logout	I Feedback D	
Lonex Wurning in lead in logout i Peadaac. Certificate Engine Identity Services Engine Identity Services Engine Identity Services Engine Identity Management Network Resources Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings Certificate Signing Requests Certificate Signing Requests (CSRs) A Certificate Signing Requests (CSRs) A Certificates System Certificates Certificates System Certificates Show All Yoe Stopent Yoeke Engine Requests Certificate Signing Requests Cortificate Show All Yoeke Engine Certificate Subject Yoekee Yoekee Show A	Setup Assistant +					
🙀 System 🛛 🦉 Identity Management	🔛 Network Resources 🛛 🛃 Device Portal Manag	gement 🛛 🙀 pxGrid Services	S Feed Service	2. pxGrid Identity Mapping		
Deployment Licensing Certificates	Logging Maintenance Backup & Rest	tore Admin Access Setting	js			
Certificate Management	Certificate Signing Requests					
Overview	Generate Certificate Signing Requests (CSR)					
	A Certificate Signing Requests (CSRs) must be sent to	and signed by an external authority. C	lick "export" to download	one or more CSRs so that they may	be signed by an external author	ity. After a request
System Certificates	has been signed, click "bind" to bind the request to the	e signed certificate issued by that auth	ority. Once a CSR is bour	d, it will be removed from this list.		
Endpoint Certificates		te			Show All	• 😽
	Friendly Name	Certificate Subject	Key Length	Portal group tag Timestamp	▲ Host	
Trusted Certificates	ise14#Admin	CN=ise14.lab7.com	2048	Sat, 5 Sep 2015	ise14	
OCSP Client Profile						
Certificate Signing Requests						
Certificate Authority						

第7步: 浏览并上传 ISE pxGrid 节点证书, 然后提交 (Submit)

ahaha								License V	Varning 🔥 ise14	
cisco Identity	y Services E	ngine		💧 Home	Operations 🔻	Policy	Guest Acces	_{is} •	Administration 🛛	
ystem	😤 Identity Ma	inagement	Network Res	sources 🛃	Device Portal Manag	gement	👵 pxGrid Sei	vices	S Feed Service	1 pxGrid Identit
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Rest	ore	Admin Access	Setti	ings	
Certificate Mana	gement		Bind CA Ci	and Castification						
Overview			BING CA SI	gned Certifica	te					
System Certificates	s			 Certification 	e File Browse	certnew-8	.cer			
-,				Friendly N	lame				٢	
Endpoint Certificat	ies		Validat	e Certificate Exten	sions 🗌 🛈					
Trusted Certificates	s			Us	age					
OCSP Client Profile	•				🗹 Admin: U	se certifica	te to authenticate	the ISE	Admin Portal	
Certificate Signing	Requests				Submit	Cancel				

第8步: 在 ISE 节点上启用 pxGrid
 选择-管理(Administration)->系统 (System)-部署 (Deployment)->突出显示 ISE 节点并启用 pxGrid
 角色

cisco Identity services Engine	Home Operations Policy Guest Access Administration Administration
💀 System 🦉 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🔂 pxGrid Services 🔂 Feed Service 11 pxGrid Identity Mappir
Deployment Licensing Certific	Logging Maintenance Backup & Restore Admin Access Settings
Deployment	Deployment Nodes List > ise14 Edit Node
	General Settings Profiling Configuration
💑 PAN Failover	Hostname ise14 FCDN ise14.lab7.com IP Address 10.0.15 Node Type Identity Services Engine (ISE)
	Personas
	Administration Role PRIMARY Make Standalone
	Monitoring Role PRIMARY * Other Monitoring Node
	Policy Service
	Enable Session Services Include Node in Node Group None T
	C Enable Profiling Service
	Ø pxGrid 0

第9步:验证 pxGrid 服务是否正在运行并**启用"启用自动注册"(Enable Auto Registration) 管理 (Administration)->pxGrid 服务 (pxGrid Services)**

		 Guest Access (* Administ 	ration 1 *			Setup Assistant +
Network Resources	🛃 Device Portal Management	pxGrid Services 🛛 🔂 🕅	ed Service	ty Mapping		
			Enable	ΘEn	able Auto-Registratio	on Disable Auto-Registratio
						View By Capabilitie
oup 🎈 Decline 🛛 😵 Delete 👻	Refresh Total Pending Approve	al(0) +		1 - 2 of 2 Show	25 👻 per page	Page 1 🗘 of 1
Client Description	Capabilities	Status	Client Group	Log		
	Capabilities(3 Pub, 1 Sub)	Online	Administrator	View		
	Capabilities(2 Pub, 0 Sub)	Online	Administrator	View		
	Network Resources	Methods: Resources Model Model	Network Resources Speake Aphresh Total Rending Approval(0) Capabilities Status Capabilities Capabilities(2 Pub, 0 Sub) Online	Methods Resources Methods Resources	Methods Resources Methods Resource	Methods Resources Methods Resources

配置 CA 签名证书的 FireSIGHT 管理中心

在本节中,将为证书颁发机构 (CA) 签名操作配置 FireSIGHT 管理中心 (FMC)。FireSIGHT 管理中心私钥和 CSR 请求从 FireSIGHT 管理中心控制台 (FMC) 进行创建。CA 服务器使用自定义 pxGrid 模板对 CSR 请求进行签名并提供 FMC 身份证书。

FMC 证书和 FMC 密钥均上传到 FMC 内部证书库中。CA 根证书上传到 FMC 受信任 CA 库中。

第1步: 生成 FireSIGHT 私钥

注意:此处的密码将在 pxGrid 代理配置中进行定义

openssl genrsa -des3 -out sourcefire.key 4096

第2步: 生成 CSR 请求

openssl req -new -key sourcefire.key -out sourcefire.csr

第3步: 使用 WinSCP 将文件从 FireSIGHT 管理中心 (FMC) 以本地方式复制到 PC

🌆 admin - admin@10.0.0.21 - WinSCP								- 0 💌
Local Mark Files Commands Session (Options Rem	ote Help						
🕀 🚟 📮 Synchronize 📓 🧬 💽 🔮) 🕄 🕄 🖗	ueue 🔹 Transfer S	Settings Defaul		-	<i>8</i> ·		
📮 admin@10.0.0.21 📫 New Session								
🚢 C: Local Disk 🔹 🖻 😨 🖛 •	÷ - 💽	🗈 🏠 🎜 🐁		🔋 📔 admii	n	• 🚰 😨 💠 • 🔶 度	🗖 🏠 🎜	😭 Find Files 🛛 🔒
🗐 Upload 🎯 📝 Edit 🗶 🛃 🕞 Prop	erties 🛗 🔓	• • •		Dowr	nload 🙀	📝 Edit 🗙 🛃 🕞 Properti	s 💕 🛐 !	+ - V
C:\smc_certs				/Volume/I	home/adr	min		
Name Ext	Size	Туре	Changed	Name	Ext		Size	Changed
🕹		Parent directory	9/5/2015 1	a				10/2/2014 11:48:14 AM
fmc2.cer	1,498 B	CER File	8/31/2015	source	fire.csr		1,744 B	9/5/2015 4:24:25 PM
inc2.key	1,958 B	KEY File	8/31/2015	📄 source	fire.key		3,247 B	9/5/2015 4:23:24 PM

第4步: 使用自定义 pxGrid 模板将 FMC CSR 请求复制/粘贴到"请求证书"(Request a certificate)->"高级用 户请求"(Advanced User request)中,然后提交。下载 base-64 编码格式的证书

<i>Microsoft</i> Active I Submit a Certif	Directory Certificate Services – lab7-WIN-LTE11SB/ ficate Request or Renewal Request	ктм-са
To submit a sav by an external s	red request to the CA, paste a base-64-enco source (such as a Web server) in the Saved I	ded CMC or PKCS #10 certificate request or PKCS #7 Request box.
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	Important Important <t< th=""><th></th></t<>	
Certificate Templa	ite:	
	pxGrid ÷	
Additional Attribu	tes:	
Attributes:		
	Submit >	

第5步: 下载 base-64 编码格式的 CA 根证书

第6步: 将 CA 根证书上传到 FireSIGHT 管理受信任 CA 库中

选择->对象 (Objects)->对象管理 (Object Management)->PKI->受信任 CA (Trusted CAs)->添加受 信任 CA (Add Trusted CA)-> 提供名称并上传 CA 证书,然后保存 (Save)

Overview Analysis Pol	icies Devices Objects A	AMP	
4 🚃 Network	Name	Value	
Individual Objects	A-Trust-nQual-01	Import Trusted Certificate Authority	? ×
Security Intelligence	A-Trust-nQual-03	Name: CA_root	
Port Individual Objects	A-Trust-Qual-01	Certificate Data or, choose a file: Browse	
- Object Groups	A-Trust-Qual-02	BEGIN CERTIFICATE MUD/JTCCAU2ndw/IBA/IO/Sc6vEerbnBKb00/X12HE2ANBo/cnbk/G9w0BA/OsEADBN	
VLAN Tag Individual Objects	AAA Certificate Services	MRMwEQYKCZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPyLGQBGRYEbGFiNjEgMB4G	
Cobject Groups	AC Raz Certicmara S.A.	MjawnTe4MDIzOD14WjBNMRMwEQYKCZImiZPyLGQBGRYDY29MRQwEgYKCZImiZPy COBOFFICEINEEMECA11E2AMECA11E2AMECA11E2AMENTE4COEmecA11E	
URL Individual Objects	Actalis Authentication Root CA	MAGCSqGSIb3DQEBAQUAA4IBDwAwgEKAoIBAQDbeZfPrLBNue/fZpmIDL8b/nFU	
Collect Groups	AddTrust Class 1 CA Root	IZxy/th6mGhZJ/K36f5idG0UzniIHji5V8G8VH2YuVJ3j1f0EhD01a8XXFG200x PP7yGSs51+FsWIPOB52EPCrx66O7D+FpYGu7LOMM01ieW98B49QgOruINPyBZDdU	
Application Filters	AddTrust External CA Root	YXSthhqQaTYHD/e17VnmuMP4p3KvqistXJxQy26RgP21a/dF3zMmQr9gHM2vkSU GLpN8BVTMhZzHzL4sqnehDfMWTuRLD8Uz+CoaqSRT8zZeJKEpISaMoFyHCaO+ecc+	
File List	AddTrust Public CA Root	n8+ov9tm3FxqmU9gbqkCjIOcmwSDYUuv9vt4b0HJ2RWKuHF0HEtQ4EYxE08jAgMB AAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRF	
Security Zones	AddTrust Qualified CA Root	viZGoanfdzS0QVHQTpZZoIsTCTAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B AQsFAAOCAQEAEfKRdin5JOOsKJm0O6WVAdkdDtzbZxl83M82zjC8pFDDQN8Lr06g	
Oistinguished Name	Admin-Root-CA	NtyW0uLeKzIEPlavel0dPIOzFs9zD2y5a/Tqcqk2Z/wk0pkPBiLnVyHjS28B4uUV xKzrxvcM4aCX+x8rhUIVt0YVY72T0fY2DgRStVZxrvt04tCswHnuzqvlyCIKEH1H	
Individual Objects	AdminCA-CD-T01	BfeFKkc5VrcKYE6kq9ugo/DXZonmumhW//Hd4unV5Mjo9LMnL+Ga9E85Jglw1ZGd rDGzz5Gmurd/J3iTwfJYPEtRM6TTJ3Own+JDvEkRMKE2ththTHisOKbb8WJ5o6oE0	
Object Groups PKI	AffirmTrust Commercial	Encrypted, and the password is:	
Internal CAs	AffirmTrust Networking	Save	Cancel
Trusted CAs			

第7步: 将 FireSIGHT 管理中心公共证书和私钥上传到 FMC 内部证书库中 选择->对象 (Objects)->对象管理 (Object Management)->PKI->内部证书 (Internal Certs)->添加 Sourcefire CER 文件和 Sourcefire KEY 文件, 然后保存 (Save)

Overview Analysis Poli	cies Devices Objects	АМР	
Object Management			
a 🚃 Network	Name	Value	
Individual Objects Object Groups Application Filters Object Set	FMC2_InternalCA	Add Known Internal Certificate Name: PAC_CAcert Certificate Data or, choose a file: Browse	? X
File List Security Zones Cipher Suite List Sittinguished Name Individual Objects Object Groups KI Security Zones		Smit FFA22Pay/Mbught/XDw(Staj)HELF411/ScanOblugh/SMXMPGFBdScHFFB4 LagO11LW/PMLR2/MDUBACE/SacDMIRLLGOS/ZZNLRFmacilgefBdg QPFGTW1Qcouhz/G/AbbL575467FBCTDoHEDbyxC2554MQW65LJSqBMF SRSchLeft/2012/T2MMSU22DcoHabbackSi71XKEHE44BacfUrblaht+ MMMADDALAGE/MARKALSACLARGE MMMADDALAGE/MARKALSACLARGE MMMADDALAGE/MARKALSACLARGE Encrypted, and the password is:	
Internal CAs		Save	Cancel

使用 CA 签名证书配置 pxGrid 代理

pxGrid 代理负责 FireSIGHT 管理中心和 ISE pxGrid 节点之间的证书配置和通信。需要 ISE pxGrid 节点的 IP 地址。需要 FireSIGHT 管理中心的公共证书和密钥文件。

FireSIGHT 管理中心的公共证书将用作主机证书。CA 根证书将用作 CA 证书。

FireSIGHT 密钥文件将是主机密钥。此外,还将需要密钥的密码。

- 第1步: 使用 winSCP 将 pxGrid 代理上传到 FireSIGHT 管理控制台
- **第2步:** 使用 WinSCP 或其他方法将 FireSIGHT 公共证书、FireSIGHT CA 密钥和 CA 根证书上传到 FireSIGHT MC /Volume/home/admin

<u>注意</u>:大写/小写语法予以保留

第3步: 通过 SSH 传输到 FireSIGHT 管理中心并键入以下内容:

sudo bash sfdc-pxgrid_agent_v1.0.35.sh

请参阅样本脚本的以下内容:

Verifying archive integrity...All good. Uncompressing Cisco pxGrid Agent Installer..... Installing the agent... Installing the pxGrid libraries and Perl module... Setting up the agent to be managed by PM... Installation done! Configuring pxGrid... Below you will be asked a series of questions relating to your pxGrid install and the files supporting it. Health alerts WILL be generated by PM until the configuration is completed, however. The answers to these questions will populate the /etc/sf/pxgrid/pxgrid.conf configuration file, which can be manually modified later at any time. A configuration example is provided in the same directory with the filename pxgrid.conf.example. To get this all to work, the agent will need to connect to a pxGrid server. This is typically your Cisco Identity Services Engine instance, which must also have the pxGrid service enabled. What is the IP address of your pxGrid server > 10.0.0.0.15 Every agent connecting to pxGrid must have a unique host certificate which will be used to identify the agent host.Associated key and CA certs must also be provided. What is the full path and filename to the host certificate? > /Volume/home/admin/sourcefire.cer What is the full path and filename to the host key? > /Volume/home/admin/sourcefire.key What is the host key password? > cisco123 What is the full path and filename to the CA certificate? > /Volume/home/admin/root.cer Configuration witten to /etc/sf/pxgrid

第4步: FireSIGHT 管理中心应已成功注册为 pxGrid 客户端并订阅 EPS 发布主题 选择**管理 (Administration)->pxGrid 服务 (pxGrid Services)**

	udu.											1	Joense Warn	ing 🔥 (ise	e14 admin	n i La	ogout i l	Feedback	P				
ci	sco I	dentity Se	rvices Engin	e		â	Home	Opera	tions V Policy	Guest Access	al 🔻 Ad	Iministration	*								Setu	p Assis	tant 🕶
	System	n 🤻 I	dentity Manage	ment 📕	Network	Resources	🛃 De	vice Po	ortal Management	🛛 🗑 pxGrid Serv	rices	S Feed Ser	vice	💵 pxGrid Io	dentity Map;	ping							
																	OEnal	ble Auto	Registra	tion (visable Au	to-Reg	istratio
С	lients	Live Log								k.											View	By Cap	Jabilitie
V	inable	Ø Disable	Approve	😝 Group 🛛 🖷	Decline	😧 Delete 🦄	Refr	sh	Total Pending Appr	oval(0) v					1-3	of 3	Show :	25 - 1	er page	Page	1	of	1
	Clier	nt Name		Client De	scription		Capal	oilities		Status			Client Grou	1p		Log							
	ise-a	admin-ise14					Capat	vilities(3 Pub, 1 Sub)	Online			Administra	tor		View	1						
	ise-r	mnt-ise14					Capat	oilities(2 Pub, 0 Sub)	Online			Administra	tor		View	(
	▼ fsmo	c-agent-sd		Cisco Fire	eSIGHT Ma	anagement C	e Capal	oilities(0 Pub, 1 Sub)	Online			EPS			Viev	(
			Capat	oility Detail								1-1	of 1 Sh	ow 25 💌 p	per page I	Page [1 ‡	of 1					
			(Capability Name	е		Capability '	Version	ı	Messaging Role		Me	ssage Filte	r									
			0	EndpointProtect	tionService	2	1.0			Sub													



FireSIGHT pxGrid 补救模块

在本节中, pxGrid 缓解补救模块上传到 FireSIGHT 管理中心。系统将创建 pxGrid 实例并定义补救类型。这些补救类型在作为响应分配到其各自的关联策略时提供 pxGrid ANC 功能。

这些补救类型包括:

- 隔离 (Quarantine) 根据源 IP 地址隔离终端
- 端口跳转 (portBounce) 暂时退回终端或主机端口
- 终止 (Terminate) 终止最终用户会话
- 关闭 (Shutdown) 启动主机端口关闭,这将在交换机端口配置上插入"shutdown"命令
- 重新身份验证 (reAuthenticate) 重新对最终用户进行身份验证
- 取消隔离 (UnQuarantine) 取消隔离终端

上传 FireSIGHT pxGrid 补救模块

第1步:将 pxGrid 补救模块上传到 FireSIGHT 管理中心
 选择策略 (Policies)->操作 (Actions)->补救 (Remediations)->模块 (Modules)-安装新模块 (Install a new module),浏览并上传模块 pxGrid_Mitigation_Remediation_v1.0.tgz 文件。

Overview Analysis Policies Devices Objects Fin	EAMP	
Access Control Intrusion Files Network Discovery	Application Detectors	Users Correlation Actions Modules
Installed Remediation Modules		
Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Cisco PIX Shun	1.1	Shun an IP address in the PIX firewall
Nmap Remediation	2.0	Perform an Nmap Scan
Set Attribute Value	1.0	Set an Attribute Value
Talos Labs - pxGrid Mitigation	0.2	Perform a pxGrid mitigation against an involved IP addresses
		Install a new module
		Browse No file selected.
		Install

创建新实例

第1步: 创建新的 pxGrid 实例

选择策略 (Policies)->操作 (Actions)->补救 (Remediations)->实例 (Instances)->添加新实例 (Add a new Instance)->模块类型 (Module type)->Talos 实验室 - pxGrid 缓解 (Talos Labs - pxGrid Mitigation)->添加 (Add)->实例名称 (Instance Name)->pxGrid->创建 (Create)

Overview Analysis Policies Devices Objects FireAMP		
Access Control Intrusion • Files Network Discovery Appl	ation Detectors Users Correlation	ctions > Instances
Access Control Intrusion • Files Network Discovery Appl	Auton Datectors Users Correlation A Edit Instance Instance Name [pxGrid] Module Talos Labs - pxt Description [number logging] On Off	Grid Mitigation (v0.2)
	Create	ancel

创建 FireSIGHT pxGrid 缓解类型

这些补救类型定义作为响应分配到用于在终端上触发补救操作的关联规则的 pxGrid ANC 缓解操作

注意:点击放大镜进行选择

隔离

根据缓解源创建隔离缓解操作

- 第1步: 策略 (Policies)->操作 (Actions)->补救 (Remediations)->模块 (Modules)->Talos 实验室 pxGrid 缓解 (Talos Labs - pxGrid Mitigation)->已配置的实例 (Configured Instances) 下的 pxGrid
- 第2步: 点击"放大镜"->根据缓解源添加新的补救类型
- 第3步: 输入补救名称: Quarantine_SourceIP
- 第4步: 对于缓解操作,请从下拉菜单中选择隔离 (quarantine)
- **第5步:** 点击保存(Save)

Overview Analysis Policies Devi	ices Objects AMF	,					
Access Control Intrusion • Files	Network Discovery	SSL Applicatio	n Detectors	Users	Correlation	Actions	Instances
			Task N	otificatio	n		×
			Task Sta succeede	tus Your tas ed at Mon Se	k Installation Set p 7 12:30:51 20	up (Register) 15	
			s	iensors are b	eing registered.	Check	
			t	ask status to	monitor progres	is.	
			Edit Remed	iation			
			Remediation Na	ime	Quarantine_Sou	rceIP	
			Remediation Ty	pe	Mitigate Source		
			Description				
			Mitigation Actio	n	quarantine	•	
			Whitelist				
			(an optional list of	networks)			
					Save	ancel Do	ne

portBounce

根据缓解源创建 portBounce 缓解操作

- **第1步:** 策略 (Policies)->操作 (Actions)->实例 (Instances),点击已配置的实例 (Configured Instances)下的 "pxGrid"旁边的放大镜
- 第2步: 从下拉菜单中选择缓解源 (Mitigate Source),然后点击添加 (Add)
- **第3步:** 输入补救名称: portBounce
- 第4步: 对于缓解操作,请从下拉菜单中选择端口跳转 (portBounce)
- **第5步:** 点击保存 (Save)



重新身份验证

根据缓解源创建重新身份验证缓解操作

- **第1步:** 策略 (Policies)->操作 (Actions)->实例 (Instances),点击已配置的实例 (Configured Instances)下的 "pxGrid"旁边的放大镜
- 第2步: 从下拉菜单中选择缓解源 (Mitigate Source),然后点击添加 (Add)
- **第3步:** 输入补救名称: reAuthenticate
- 第4步: 对于缓解操作,请从下拉菜单中选择重新身份验证 (reAuthenticate)
- **第5步:** 点击保存(Save)

cess Control	Intrusion •	Files	Network Disc	overy !	SSL	Application	n Detectors	Users	Correlation	Actions	Instance
							Task I	Notificatio	on		×
							Task Sta succeed	atus Your ta ed at Sat Au	sk Installation Sel 1g 22 09:19:25 20	tup (Register) 015	
							-	Sensors are æsk status t	being registered. o monitor progres	Check is.	
							Edit Remed	liation			
							Remediation N	ame	reAuthenticate		
							Remediation Ty	rpe	Mitigate Source		
							Description				
							Mitigation Actio	in	reAuthenticate	1	
							Whitelist (an optional list o	f networks)			
									Save	ancel	100

关闭

根据缓解源创建关闭缓解操作

- **第1步:** 策略 (Policies)->操作 (Actions)->实例 (Instances), 点击已配置的实例 (Configured Instances)下的 "pxGrid"旁边的放大镜
- 第2步: 从下拉菜单中选择缓解源 (Mitigate Source),然后点击添加 (Add)
- 第3步: 输入补救名称: Shutdown
- 第4步: 对于缓解操作,请从下拉菜单中选择关闭 (shutdown)
- **第5步:** 点击保存 (Save)

Overview A	nalysis Polici	ies Dev	vices Objects A	MP							
ccess Control	Intrusion •	Files	Network Discovery	SSL	Applicatio	n Detectors	Users	Correlatio	in Ac	tions 🕨	Instance
						Task	Notificati	on			×
						Task St	atus Your ta	sk Installation	1 Setup (R	egister)	
						Juccece	Sensors are	being registe	red. Check	<i>,</i>	
							task status I	to monitor pro	gress.		
						Edit Reme	diation				
						Remediation N	ame	Shutdown			
						Remediation T	ype	Mitigate So	urce		
						Description					
						Mitigation Activ		chutdown	•		
						And gutton Acta		- Shataonni			
						Whiteliet					
						(an optional list of	of networks)				
								Save	Cancel	Don	

终止

根据缓解源创建终止缓解操作

- **第1步:** 策略 (Policies)->操作 (Actions)->实例 (Instances),点击已配置的实例 (Configured Instances)下的 "pxGrid"旁边的放大镜
- 第2步: 从下拉菜单中选择缓解源 (Mitigate Source),然后点击添加 (Add)
- 第3步: 输入补救名称: Terminate
- 第4步: 对于缓解操作,请从下拉菜单中选择终止(terminate)
- **第5步:** 点击保存 (Save)

Access Control Intrusion • Files Network Discovery	SSL	Applicatio	n Detectors	Users	Correlation	Actions + Instan
			Task	Notificat	ion	×
			Task St succeed	<u>atus</u> Your t led at Sat A	ug 22 09:19:25 2	tup (Register) 015
				Sensors are	being registered.	Check
				task status	to monitor progre	ss.
			Edit Reme	diation		
			Remediation N	ame	Terminate	
			Remediation T	ype	Mitigate Source	3
			Description			
			Mitigation Acti	on	terminate	\$
			Whitelist (an optional list of	of networks)		

取消隔离

根据缓解源创建取消隔离缓解操作

- **第1步:** 策略 (Policies)->操作 (Actions)->实例 (Instances),点击已配置的实例 (Configured Instances)下的 "pxGrid"旁边的放大镜
- 第2步: 从下拉菜单中选择缓解源 (Mitigate Source),然后点击添加 (Add)
- **第3步:** 输入补救名称: UnQuarantine_SourceIP

第4步: 对于缓解操作,请从下拉菜单中选择**取消隔离 (unquarantine)** 第5步: 点击保存 (Save)

Overview Analy	ysis Polici	ies Dev	rices Objects	AMP						
Access Control	Intrusion •	Files	Network Discovery	SSL	Applicatio	n Detectors	Users	Correlation	Actions	Instance
						Task I	Notificati	on		×
						Task St	atus Your ta	sk Installation Se	tup (Register)	
						succeed	ed at mon s	sep / 12:30:51 20	115	
							Sensors are task status t	being registered. to monitor progre	Check ss.	
						Edit Remed	liation			
						Remediation N	ame	UnQuarantine_I	by_SourceIP	
						Remediation T	ype	Mitigate Source		
						Description				
						Description				
						Mitigation Actio	on	unquarantine	\$	
						Whitelist				
						(an optional list o	f networks)			
								Save	ancel Do	one



FireSIGHT pxGrid 入侵策略

在本节中,将会创建 pxGrid 入侵策略并将其部署到 FireSIGHT 传感器。此策略包含 "SERVER IIS CMD.EXE 访问"规则,当最终用户在其浏览器中键入 <u>www.yahoo.com/cmd.exe</u> 时,这将根据关联策略(取消隔离关联策略除外)生成入侵事件。

- 第1步: 导航到策略 (Policies)->入侵 (Intrusion)->入侵策略 (Intrusion Policy)
- 第2步: 点击创建策略 (Create Policy)
- 第3步: 将新策略命名为 pxGrid_Intrusion_Policy
- 第4步: 点击创建策略 (Create Policy)

Overview Analysis Policies Devices Ob								
Access Control Intrusion > Intrusion Policy	Files	Network Discovery	SSL	Application Detectors	Users	Correlation	Actions •	
								Impor
			-					
		Create Intrusi	on Poli	сy			7 ×	
		Policy Informa	tion				1	
		Name *		pxGrid Intrusion	Policy			
		Description						
Intrusion Policy		Drop when In	line				4	
Default policy		Base Policy		No Rules Active		\$		
Initial Passive Policy - sd.lab7.com								
below poincy		* Required		Create Policy	Create	and Edit Policy	Cancel	

第5步: 点击->pxGrid_Intrusion_Policy以进行编辑

Overview Analysis Policies Devices Obj	ects AMP						🛕 Health System	Help 🔻 admin 🔻
Access Control Intrusion + Intrusion Policy	Files Network Discove	ary SSL	Application Detectors	Users	Correlation	Actions •		
		Task Notification Task Status Your task Installat succeeded at Mon Sep 7 12:30 Bensors are being registered. I monitor progress.	ion Setup (I 1:51 2015 Check task :	× Register) itatus to		Import/Export Rule Editor Access Control Policy N	etwork Analysis Policy es Oreate Policy	
Intrusion Policy	Drop when I	inline	Status				Last Modified	
Initial Inline Policy - sd.lab6.com Default policy	Yes	Yes		No access control policies use this policy Policy not applied on any devices			2015-09-07 12:30:49 Modified by "admin"	2 🖪 🕞 🥒 🖯
Initial Passive Policy - sd.lab6.com Default policy	No		No access control Policy not applied	policies use on any dev	this policy ices		2015-09-07 12:30:45 Modified by "admin"	2000
pxGrid_Intrusion_Policy*	No		You are currently No access control Policy not applied	editing this policies use on any dev	policy this policy ices		2015-09-07 20:37:47 Modified by "admin"	w 🖻 🖬 🥒 6

第6步: 点击->规则 (Rules) 并对 cmd.exe 进行过滤, 然后选择以下规则

Overview Analysis Policie	Devices Objects	AMP										
Access Control Intrusion > I	ntrusion Policy Files	Network Discov	ery SSL	Application Detectors	Users	Correlation	Actions v					
Edit Policy: pxGrid_Intrusion_Policy												
			Ta Tas suc Ser mo	Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.								
Policy Information 🛕	Rules											
Rules	Rule Configuration	Filter: cmd	exe									
FireSIGHT Recommendations	Rule Content					Filter retu	rned 21 result	s				
Advanced Settings	Category	⇒ • • •	• 🕞 •	🕕 🔹 고 🗸								
Reliev Lavers	app-detect	Rule State Ever	nt Filtering Dyna	mic State Alerting Comm	ents							
Policy Layers	blacklist	GID SID	Message									
	browser-chrome	1 17442	FILE-OTHE	FILE-OTHER Microsoft Windows download of .Ink file that executes cmd.exe detected								
	browser-firefox	I 18756 INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows 7/Server 2008F										
	browser-ie	1 18757	INDICATO	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows Vista								
	browser-other	1 2123	INDICATO	R-COMPROMISE Microsoft c	md.exe banı	her						
	browser-plugins	1 30390	INDICATO	R-SHELLCODE Metasploit pa	yload cmd_	windows_downloa	ad_exec_vbs					
	browser-webkit	1 3193	SERVER-II	S .cmd executable file parsi	ng attack							
	content-replace	1 1002	SERVER-I	IS cmd.exe access								
	Classifications	✓ 1 23626	SERVER-I	IS cmd.exe access								
	Microsoft Vulnerabilities	✓ 1 1661	SERVER-I	IS cmd32.exe access								
第7步: 点击规则状态 (Rule State) > 生成事件 (Generate Events), 然后确定 (OK)

Overview Analysis Policie	es Devices Objects	AMP						
Access Control Intrusion > I	ntrusion Policy Files	Network Discovery	SSL	Application Detectors	Users	Correlation	Actions •	
Edit Policy: pxGrid_I	Intrusion_Policy							
] s r	Task Notification Task Status Your task Installat succeeded at Mon Sep 7 12:30 Sensors are being registered. nonitor progress.	tion Setup (0:51 2015 Check task	× Register) status to		
Policy Information 📐	Rules							
Rules	Rule Configuration	Filter: cmd exe						
FireSIGHT Recommendations	Rule Content					Filter retu	rned 21 results	5
Advanced Settings	Category app-detect		ring Du		onto			
Policy Layers	blacklist	Generate Events	ing of		enes			
	browser-chrome	Drep and Concepto Fu	то	HER Microsoft Windows downl	load of .Ink	file that executes	cmd.exe detecte	d
	browser-firefox	Drop and Generate Ev	CAT	OR-COMPROMISE Microsoft c	md.exe bar	ner Windows 7/Se	erver 2008R2	
	browser-ie	Disable	CAT	OR-COMPROMISE Microsoft c	md.exe bar	ner Windows Vist	а	
	browser-other	1 2123	INDICAT	OR-COMPROMISE Microsoft c	md.exe bar	iner		
	browser-plugins	1 30390	INDICAT	OR-SHELLCODE Metasploit pa	ayload cmd	_windows_downloa	ad_exec_vbs	
	browser-webkit	1 3193	SERVER	IIS .cmd executable file parsi	ing attack			
	content-replace	✓ 1 1002	SERVER	-IIS cmd.exe access				
	Classifications	1 23626	SERVER	-IIS cmd.exe access				
	Microsoft Vulnerabilities	✓ 1 1661	SERVER	-IIS cmd32.exe access				

- **第8步:** 您应该看到一条成功消息,表明"已成功设置3个规则的规则状态"(successfully set the rule state for 3 rules)
- 第9步: 点击策略信息 (Policy Information)

Overview Analysis Polici	es Devices Objects	АМР	
Access Control Intrusion > 3	Intrusion Policy Files	Network Discovery	SSL Application Detectors Users Correlation Actions •
Edit Policy: pxGrid_	Intrusion_Policy		
			Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Set p 12:30:51 2015 Sensors are being registered. Check task status to monitor progress. *
Policy Information 🛆	Rules		
Rules	Rule Configuration	Filter: cmd exe	
FireSIGHT Recommendations	Rule Content		Filter returned 21 results
Advanced Settings	Category		
	app-detect	Rule State Event Filte	ering Dynamic State Alerting Comments
Policy Layers	blacklist	GID SID	Message 🔺
	browser-chrome	1 17442	FILE-OTHER Microsoft Windows download of .Ink file that executes cmd.exe detected
	browser-firefox	1 18756	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows 7/Server 2008R2
	browser-ie	1 18757	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows Vista
	browser-other	1 2123	INDICATOR-COMPROMISE Microsoft cmd.exe banner
	browser-plugins	1 30390	INDICATOR-SHELLCODE Metasploit payload cmd_windows_download_exec_vbs
	browser-webkit	1 3193	SERVER-IIS .cmd executable file parsing attack
	content-replace	✓ 1 1002	SERVER-IIS cmd.exe access
	Classifications	✓ 1 23626	SERVER-IIS cmd.exe access
		✓ 1 1661	SERVER-IIS cmd32.exe access

第10步:然后,点击"确认更改"(Commit Changes)

Overview Analysis Policie	s Devices Objects	AMP					
Access Control Intrusion > I	ntrusion Policy File	s Network Discovery	SSL	Application Detectors	Users	Correlation	Actions 🔻
Edit Policy: pxGrid_I	intrusion_Policy	/					
			T s s n	Task Notification (ask Status) Your task Installat ucceeded at Mon Sep 7 12:30 iensors are being registered, nonitor progress.	tion Setup (f 0:51 2015 Check task s	× Register) status to	
Policy Information 📐	Policy Information						
Rules FireSIGHT Recommendations Advanced Settings	Name Description Drop when Inline	pxGrid_Intrusion_Policy					
Policy Layers	Base Policy No Re	ules Active up to date (Rule Update 2014-	¢ 09-02-00	1-vrt)			
	This policy has 3 er ⇒ 3 rules generate ev X 0 rules drop and generate ev	abled rules vents enerate events					
	No recommendations have	e been generated. Click here t	o set up F	FireSIGHT recommendations.			
				Cor	mmit Change	Discard C	hanges

第11步:点击确定(OK)

第12步:选择并编辑策略 (Policies)->访问控制策略 (Access Control Policies)->默认入侵防御 (Default Intrusion Prevention)

verview Analysis	Policies Devic	es Objects	AMP							🔺 Healt	n System	Help v adm i
cess Control Intr	usion • Files	Network Discov	ery SSL	Application Detec	tors Users	Correlatio	n Actions 🔻					
									Object Management	Intrusion Policy Net	vork Analysis P	olicy Import/Ex
										, 	,,	
										Jr c	ompare Policies	New Po
ccess Control Policy									Status			
fault Intrusion Preven	tion								Applied to 1 out of 1 Up-to-date on 1 dev	targeted devices		~ % E 🖉 E
												_
13 步: 7	在"默认	人操作"	(Defa	ult actio	ons) 下	,从	下拉列表	長中选	择 pxGrie	d_Intru	sion_	Policy
			1 1000100								a atomati	- 16 (16 (16 (16 (16 (16 (16 (16 (16 (16
rview Analysis	Policies Dev	ices Objects	AMP								🔺 Health	System He
ss Control Intr	usion • Files	Network Discr	overy SSL	Application D	etectors U	sers Cor	relation Actions	•				
ault Intrusio	n Preventi	on							You have uns	aved changes	Save	Cancel
a description Targets (1)	Security Intelliger	nce HTTP Res	ponses Adva	nced						•		
Filter by Device									Add Catego	ry 😳 Add Rule	Search Rul	es
	Source	Dest	Source	Dest								
Name	Zones	Zones	Networks	Networks	VLAN Tags	Users	Application	s Src Ports	Dest Ports	URLs	Action	
nistrator Rules												
ategory is empty												
dard Rules												
category is empty												
Bules												
Kulta												
category is empty			_	_	_	_		_				
ult Action						_			Intrusion Prevention	on: pxGrid_Intrusio	1_Policy	
												
14 步:)	点击 保 石	∓ (Save	e)									
		· (- · · · ·	í 🖬 💷 🖓			्राम्ना	<u> </u>					
15 步:)	点击表る	ヨト万臣	9日志1	记录 (L	ogging	<u>z</u>) 图체	不					
					00 0	,	•					
00 10 00 AMPT			Valuestatio								1 2000 M	10.10 02.00
rview Analysis	Policies Devic	es Objects	AMP							🔺 Healti	n System	Help 🔻 adm
ass Control Intro	usion • Files	Network Discove	ery SSL	Application Detec	tors Users	Correlatio	n Actions •					
fault Intrucio	n Proventio									Save	Cancel	Save and Ac
Tault Inclusio	in Freventio								•			
a description												
es Targets (1)	Security Intelligent	e HTTP Respon	nses Advance	d								
Filter by Device									Add Category O /	Add Rule Search R	ules	
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications Src	Ports D	est Ports URLs	Action	U	
inistrator Rules												
category is empty												
category is empty												
category is empty ndard Rules category is empty												
category is empty ndard Rules category is empty t Rules												
a category is empty ndard Rules a category is empty t Rules a category is empty a category is empty												

第 16 步: 在连接开始和结束时启用日志记录。选择"防御中心"(Defense Center)作为目标 **第 17 步:** 点击确定(OK)

Overview Analysis	Policies Device	es Objects 🛛 A	MP						
Access Control Intr	rusion • Files	Network Discovery	SSL	Application De	tectors User	s Correlation	Actions •		
Default Intrusio	on Prevention	ı							
Rules Targets (1)	Security Intelligence	HTTP Response	es Advance	ed					
Filter by Device									🔘 Ad
# Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Po
Administrator Rules			Logging						? ×
This category is empty			🗹 Log at	Beginning of C	onnection				
Standard Rules			Log at	End of Connect	ion				
This category is empty									
Root Rules			Send Cor	nection Events	:0:				
This category is empty			🗹 Defen	se Center					
Default Action			C Syslo	Select a Sysl	og Alert Configural			▼ ○	
			SNMP	Trap Select a	SNMP Alert Confi	guration		v O	
							0	K Ca	ncel

第18步: 点击保存并应用 (Save and Apply)

第19步: 您应该看到以下内容:



第20步: 点击全部应用 (Apply All)

第21步: 您应该看到任务已加入队列

Overview Analysis	Overview Analysis Policies Devices Objects AMP													
Access Control Intru	sion v Files	Network Discove	ry SSL	Application De	tectors Users	Correlatio	n Actions 🔻							
Default Intrusion	n Preventior	ı												
Rules Targets (1) Security Intelligence HTTP Responses Advanced														
Biller by Device Device														
# Name	ara Hiter by Device # Name Source Dest Source Dest Networks VLAN Tags Users Applications 5													
Administrator Rules														
This category is empty														
Standard Rules				Apply Acce	ess Control Po	licy								
This category is empty				Access Cor	Apply Access	Control Poli	су							
Root Rules				Accession	Policy apply ta	isk queued.								
This category is empty Apply this A Task Status														
Default Action				and policy c		ſ	OK							

第22步: 点击确定(OK)

第23步:选择系统 (System)->监控 (Monitoring)->任务状态 (Task Status) 以获取结果,请注意任务已成功完成

Overview	Analysis	Policies	Devices	Objects	АМР				
							Local 🔻	Updates	Licens
Job Summ	ary								
Running		0							
Waiting		0							
Completed		12							
Retrying		0							
Failed		0							
Jobs									
Task Descri	iption				Message	Creation Time	Las	t Change	
Active D 0 Runnin	irectory Dow g 0 Waiting	nload Task 1 Complete	ts d 0 Retryin	g 0 Failed					
Download u LDAP Downlo	users/groups	from Lab			LDAP download successful: 37 groups, 8 users downloaded	2015-09-07 18:46:11	201	5-09-07 18:46	i:12
Policy and 0 Runnin	pply tasks g 0 Waiting	4 Complete	d 0 Retryin	g 0 Failed					
Apply Defai Access Contr	ult Intrusion rol Policy	Prevention	to 192.168	.1.51	Access Control Policy applied successfully	2015-09-07 17:51:37	201	5-09-07 17:52	1:37
Network Di Network Dise	scovery policy	cy apply to	192.168.1.!	51	Network Discovery policy successfully applied	2015-09-07 17:52:37	201	5-09-07 17:53	1:38
Apply Defai Access Contr	ult Intrusion rol Policy	Prevention	to 192.168	8.1.51	Access Control Policy applied successfully	2015-09-07 21:10:39	201	5-09-07 21:11	:27
Apply Defai Access Contr	ult Intrusion rol Policy	Prevention	to 192.168	3.1.51	Access Control Policy applied successfully	2015-09-07 21:12:33	201	5-09-07 21:13	1:19

FireSIGHT 连接规则

在本节中,我们定义要添加到默认访问策略中的连接规则。此默认访问策略还包括 pxGrid 入侵策略。此连接规则通过 HTTP/HTTPS 监控连接事件,并将这些连接详细信息记录到 FireSIGHT 管理中心。此连接规则将由 UnQuarantine 策略用于监控触发 unquarantine 补救类型的连接事件。

第1步: 导航到策略 (Policies)->访问控制 (Access Control)

第2步: 通过点击铅笔图标编辑默认入侵防御 (Default Intrusion Prevention)

	Overview Analysis Policies Devices Object	cts AMP		🔺 н	ealth System Help v admin v
	Access Control Intrusion • Files Network I	Discovery SSL Application Detectors	Users Correlation Actions •		
				Object Management Intrusion Policy	Network Analysis Policy Import/Export
					Compare Policies ONew Policy
	Access Control Policy			Status	
	Default Intrusion Prevention			Applied to 1 out of 1 targeted device Up-to-date on 1 devices	s 🖌 🖓 🕞 🚺
第3岁	▶: 点击 添加规则 (Add	l Rule)			
第43	▶: 将规则命名为"H1	TP Checks"			
447 6 1		TE F.			
おうろ	ア: 远洋垢口 (Ports) 辺	现下			
笛 6 屴	き : 洗择 HTTP 和 HT	FPS 作为目标端口			
1					
	Add Rule			? ×	
		d			
	Name HTTP checks	Enabled In	isert below rule 1		
	Action V Allow	TP3: no poincies Variables: n/a Piles: no n	ispection Logging: no logging		
	Zones Networks VLAN Tags Users	Applications Ports URLs	Inspection Loggin	ng Comments	
	Available Ports C	Selected Source Ports (0)	Selected Destination Ports (2)		
		any			
	Bittorrent			_	
	DNS over TCP	Add to Source			
	DNS over UDP	Add to			
	W FTP				
	HTTP				
	🛫 IMAP				
	👷 LDAP				
	NFSD-TCP	Protocol TCP (6) Y Port Enter	a port Add Protocol Y Port En	ter a port Add	
			Add	Cancel	

第7步: 点击 IPS 并选择 pxGrid_Intrusion_Policy

ame HTTP checks			🗹 En	abled	Insert	below rule		✓ 1	
ction 🖌 Allow		✓ IPS: pxt	Grid_Intrus	ion_Po V	ariables: default	Files: no ins	pection Logging:	no logging	
Zones Networks VLA	AN Tags Users	Applications	Ports	URLs			Inspe	ction Logg	ing Comments
ailable Ports 🖸	C		Select	ed Source Po	orts (0)		Selected Destir	nation Ports (3	2)
Search by name or value ADL Bittorrent DNS over TCP DNS over UDP FTP HTTPS HTTP MAR AAP AAP AAP AAP AAP AAP AA		Add to Source Add to Destination	any				₩ HTTPS ¥ HTTP		
NFSD-TCP			Protoc	DI TCP (6)	Port Enter a p	ort Add	Protocol	Y Port E	inter a port Add

第8步: 选择日志记录 (Logging)

				C. Carolin				121 12		
Action	Allow	V IPS: p	Grid_Intrusion_	Po Variable	s: default File	s: no inspection	spection Logging: connections: dc			
Zone	s Networks VLAN	Taos Users	Applications	Ports UR	4			Inspection	Logging	Comme
🕑 Log a File Even	t End of Connection									
Uog a File Even Log F Send Cor	t End of Connection ts: iles inection Events to: se Center									

第9步: 您应该看到以下内容

Overview Analy	sis Policies	Devio	es Objects	AMP								🔺 Health S	ystem H	elp v a e	dmin v
Access Control	Intrusion •	Files	Network Discove	ry SSL	Application Detec	ctors Users	Correlation	Actions •							
Default Intro	usion Prev	entio	n							You have unsa	ved changes [Save 🛛 🔀 Ca	ancel	🕈 Save and	d Apply
Rules Targets (1) Security In	ntelligenc	e HTTP Respon	ses Advance	ed										
曲 Filter by Device										Add Category	/ 🔾 Add Rule	Search Rules			×
# Name	Sourc	e i	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action			
Administrator Rule	s														
his category is emp	ty														
tandard Rules															
HTTP checks	any		any	any	any	any	any	any	any	HTTP HTTPS	any	🖋 Allow	0	0	0
Root Rules															
This category is emp	ty														
Default Action										Intrusion Prevention	: pxGrid_Intrusion_	Policy		- × 🧷	\$ 🔳

第10步:选择保存 (Save)

0.0	anviour Analysis	Policies Devic	os Objects	AMD									Suctor	Holp -	ade	nin -
0ve	erview Analysis	rion T Filos	Notwork Discov	APIP CCI	Application Date	octors Usors	Corrolati	an Actions				A nealur	system	neip v	aui	
ACC	less control Intro	sion • Files	Network Discov	ery SSL	Application Deb	ectors Osers	Correlatio	Actions •								
De	efault Intrusio	n Preventio	n							You have unsav	ved changes	Save 🛛 🔀 🤇	Cancel	Sav	e and /	Apply
Enter	r a description															
Ru	Rules Targets (1) Security Intelligence HTTP Responses Advanced															
đb	Filter by Device								Add Category	Add Rule	Search Rules				×	
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	U		Ģ	
Adr	ministrator Rules															
Thi	is category is empty															
Sta	indard Rules															
1	HTTP checks	any	any	any	any	any	any	any	any	HTTP HTTPS	any	Allow	1	08	0	0
Roc	ot Rules															
This	is category is empty															
De	fault Action									Intrusion Prevention	pxGrid_Intrusion	Policy		~	0	5 🔳

第11步:选择保存并应用 (Save and Apply)

Overview Analysis	Policies	Devices	objects	MP								🔺 Health S	ystem Help	• ad	min •
Access Control I	ntrusion •	Files N	Network Discovery	y SSL	Application Dete	ctors Users	Correlatio	n Actions •							
Default Intrus	Internation Prevention Cancel Serve and Apply														
Rules Targets (1) Security Intelligence HTTP Responses Advanced															
齢 Filter by Device										Add Category	/ 🔾 Add Rule	Search Rules			×
# Name	Source Zones		Dest : Zones :	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	v 🕞 🛛	-	
Administrator Rules															
This category is empty															
Standard Rules															
1 HTTP checks	any		any	any	any	any	any	any	any	HTTP HTTPS	any	🖋 Allow	🤍 🗅 🚺	0	J
Root Rules															
This category is empty															
Default Action										Intrusion Prevention	n: pxGrid_Intrusion_	Policy		× 🧭 :	\$ 🔳

第12步: 点击全部应用 (Apply All)

Overview Analysis	Policies Device	es Objects 🛛 A	AMP							
Access Control Int	rusion • Files	Network Discovery	y SSL	Application Det	ectors U	Isers Correlation	on Actions •			
Default Intrusion Prevention										
Rules Targets (1)	Security Intelligence	HTTP Response	es Advan	ced						
器 Filter by Device										
# Name	Source Zones	Dest 2 Zones	Source Networks	Dest Networks	VLAN Tag	s Users	Applications	Src Ports		
Administrator Rules										
This category is empty										
Standard Rules										
1 HTTP checks	any	any	any	Apply Acces	ss Control	Policy		? X		
Root Rules				Access Cont	rol Policy: D	efault Intrusion Pr	evention			
This category is empty				Apply this Acc and policy cha	cess Control p anges to affect	olicy and all associat ted devices.	ed rule configurat	ions, objects,		
Default Action				poncy cit	ingen to unce					
						Apply All	Details	Cancel		

第13步: 您应该看到"策略应用任务已加入队列"(Policy apply task queued),点击确认 (OK)

Overview Analysis	olicies Device	es Objects	AMP							
Access Control Intrusio	on 🔻 Files	Network Discove	ery SSL	Application Det	ectors Users	Correlation	Actions •			
Default Intrusion Prevention										
Rules Targets (1) Se	curity Intelligence	HTTP Respon	nses Advanc	ed						
# Filter by Device										
# Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports		
Administrator Rules	Administrator Rules									
This category is empty										
Standard Rules										
1 HTTP checks	any	any	any	Apply Acce	ss Control Poli	су		? X		
				Access Cor	Apply Access	Control Polic	cy .			
Root Rules				Apply this A	Policy apply tas	sk queued.		e objecte		
This category is empty				and policy c	Task Status	Task Status				
Default Action							OK			
					A	pply All	Details	Cancel		

配置 ISE EPS 服务和隔离授权策略

本节说明在 ISE 中启用 EPS 以及在 ISE 中创建隔离授权策略的步骤。在 ISE 1.4 中, "终端保护服务"重命名为"自适应网络控制"。在 ISE 2.0 中,默认情况下会启用此重命名,在"管理"(Administration)下没有自适应网络控制服务设置。

- 注意: ISE 2.0 中的自适应网络控制策略取决于注册到 AdaptiveNetworkControl Capability 的 pxGrid 客户端。对于 FireSIGHT 管理中心情况并非如此。FireSIGHT 管理中心注册到 EndpointProtectionService Capability 并依赖于 ISE 授权策略。请注意,在 ISE 2.0 中,必须使用 pxGrid GCL EPS_unquarantine 脚本来取消隔离终端。这在 FireSIGHT 管理中心内通过创建 unquarantine 关联策略,取消关联规则并将取消隔离的缓解响应分配到 unquarantine 关联策略来执行。
- 第1步: 启用 ISE 终端保护服务
 管理 (Administration)->系统 (System)->设置 (Settings)->终端保护服务 (Endpoint Protection Service)
 并启用终端保护服务->保存 (Save)

<u>注意</u>:终端保护服务在 ISE 2.0 中不适用;默认情况下会打开此服务



第2步: 创建隔离授权配置文件

策略 (Policy)->策略元素 (Policy Elements)->结果 (Results)->授权 (Authorization)->授权配置文件 (Authorization Profiles)->添加 (Add)->名称 (Name): Quarantine->保存 (Save)

cisco Identity Services Engine		🟠 Home	Operations 🔹	Policy V	Guest Acces	ss •	Administration	*	
Authentication Authorization Dictionaries Conditions Results	Profiling	Posture	Client Provisi	oning	🔄 TrustSec		Policy Elements		
Results	Authoriz Des * Acce Service Te	ation Profile * Name Quarant cription ess Type ACCESS emplate	ACCEPT	Ţ					
Non_Cisco_IP_Phones PermitAccess	▼ Comm	non Tasks							

注意: 在本例中, "访问类型"(Access Type)设置为 ACCESS_ACCEPT, 以演示授权条件配置文件

第3步: 创建隔离授权策略

策略 (Policy)->授权 (Authorization)->例外 (Exceptions)-> 输入以下内容: 规则名称: EPS Quarantine 创建新的条件规则: Session:EPSStatus:EQUALS:Quarantine 标准配置文件: Quarantine 点击->完成 (Done)									
cisco Identity Services Engine	🟠 Home	Operations V Policy V	Guest Access V Administration	1 🔻		Setup Assistant +			
Authentication	Refiling Posture	Client Provisioning	📄 TrustSec 🦂 Policy Elements	5					
Authorization Policy									

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page First Matched Rule Applies

▼ E	xception	s (1)				
	Status	Rule Name		Conditions (identity groups and other conditions)	Permissions	
1		EPS Quarantine	ŀ	f Session: EPSStatus EQUALS Quarantine	then Quarantine	Edit 👻

第4步: 点击->保存 (Save)

FireSIGHT 管理中心关联策略

在本节中,将为隔离、端口跳转、重新身份验证、端口关闭、终止和取消隔离创建 FireSIGHT 关联策略和规则。这些策略分配有其各自的补救响应,在终端上提供 pxGrid ANC 缓解补救操作。

系统将创建关联策略,然后创建规则模块。关联策略将添加其各自的规则模块。规则模块将分配有其各自的响应。

例如,将会创建隔离关联策略。系统将创建隔离规则模块,以便在发生入侵事件时,将隔离终端的源 IP 地址。隔离规则模块将分配有隔离补救类型响应。当最终用户违反 pxGrid 入侵策略时,这将触发入侵事件,并且还触发会根据隔离补救类型响应启动隔离缓解操作的关联事件。

端口跳转、重新身份验证、端口关闭、终止策略将遵循同一流程。

取消隔离策略将具有会触发连接事件的取消隔离规则模块,当终端访问特定 URL 站点时,将根据终端的源 IP 地址对其取消隔离。

隔离

创建隔离关联策略。

第1步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->创建策略 (Create Policy)-> pxGrid_ANC_Quarantine->保存 (Save)

Overview Analysis Policies Devices Objects AMP			🔺 Health	System Help	▼ admin
Access Control Intrusion • Files Network Discovery SSL Application	Detectors Users Correlation Act	ions 🔻			
				Alerts Remedia	ions Group
Policy Management Rule Management White List Traffic Profile:					
	Task Notification Task Status Your task Installation Setup (Reg succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.	×			
Correlation Policy Information				Save	Cancel
Policy Name pxGrid_ANC_Quarantine					
Policy Description					
Default Priority None +					
Policy Rules				٢	Add Rules

第2步: 策略 (Policies)->关联 (Correlation)->规则管理 (Rule Management)->创建规则 (Create Rule)->添加 规则名称->Quarantine_by_SourceIP,并输入以下内容,然后保存 (Save)

注意:此规则提供源 IP 地址受到隔离的概念证明

Overview Analysis Policies Devices Objects AMP	
Access Control Intrusion - Files Network Discovery SSL Applica	ation Detectors Users Correlation Actions •
Policy Management Rule Management White List Traffic Pro	files
	× Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7.17:30:51 2015 Sensors are being registered. Check task status to monitor progress.
Rule Information	Add Connection Tracker
Rule Description	
kule Group	
Select the type of event for this rule	
If an intrusion event occurs and it meets the following conditions:	
Add condition Add complex condition	
X Source IP is	192.168.1.7

第3步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->pxGrid ANC Quarantine>添 加规则 (Add rules)->pxGrid ANC Quarantine->添加 (Add)



第4步: 接下来,我们将添加响应,点击响应(Responses)选项卡

Overview Analysis Policies Devices Objects AMP		🛕 Health System Help 🔻 admin
Access Control Intrusion • Files Network Discovery SSL Application	Detectors Users Correlation Actions •	
		Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles	5	h
	Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Set 71 2:3025 2015 Second are being registered. Check task status to monitor progress.	
Correlation Policy Information		You have unsaved changes Save Cancel
Policy Name pxGrid_ANC_Quarantine		
Default Priority None +		
Policy Rules		Add Rules
Rule	Responses	Priority
Quarantine by SourceIP	This rule does not have any responses.	Default 💠 🚺

第5步: 将 Quarantine_SourceIP 移至已分配的响应 (Assigned Responses)->更新 (Update)->保存 (Save)

Overview Analysis Policies Devices Objects AMP	
Access Control Intrusion Files Network Discovery SSL	Application Detectors Users Correlation Actions v
Policy Management Rule Management White List Traff	ic Profiles
	Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015
	Responses for Quarantine_by_SourceIP
	Assigned Responses
Correlation Policy Information	Quarantine_SourceIP
Policy Name pxGrid_ANC_Quarantine	
Policy Description	
Default Priority None 🗧	Unassigned Responses
Policy Rules	Shutdown
Rule	Terminate UnQuarantine_by_SourceIP
Quarantine_by_SourceIP	portBounce reAuthenticate
	Update Cancel

第6步: 通过点击按钮激活隔离关联策略

Overview Analysis Policies Devices Objects AMP	🔺 Health System Help 🔻 admin
Access Control Intrusion - Files Network Discovery SSL Application Detectors Users Correlation Actions -	
	Alerts Remediations Group
Policy Management Rule Management White List Traffic Profiles	
	O Create Policy
Task Notification × Task Status Your task Installation Setup (Register) successful at Non Sep 7 12:0:03:2013 Sensor are being registered. Check task status to monitor progress.	
Success × Activited Policy: pxGrid_ANC_Quarantine	
	Sort by State +
pxGrid ANC Quarantine	ette 🗸 🕄
pxGrid_ANC_portBounce	CTR / 6
pxGrld_ANC_reAuthenticate	STR / 5
pxGrid_ANC_shutdown	() 🔊 🧳 🗓
pxGrid_ANC_Terminate	IN 🥖 5
pxGrid_ANC_Unguarantine	J 🖉 🥖 🗄

测试

最终用户将在其浏览器窗口中键入 <u>www.yahoo.com/cmd.exe</u>,这将会由于 FireSIGHT 的 pxGrid 入侵策略中发 生 "SERVER-IIS.cmd.exe 访问"规则违规而触发入侵事件。终端将根据分配到关联策略中所定义的隔离规则 的隔离缓解响应进行隔离。

- **第1步:** 最终用户在其浏览器中输入 www.yahoo.com/cmd.exe
- **第2步:** 这将触发"Web 应用攻击"(Web Application Attack)入侵事件

Overview Anal	view Analysis Policies Devices Objects AMP										
Context Explorer	Connections •	Intrusions + Events	Files Hosts	Users •	Vulnerabilities •	Correlation •	Custom •	Search			
Events By P	riority and	Classification (swi	ch workflow)					Bookmark This Page	e Report Designer Dashboa	rd View Bookn	narks Serich V
				×							
Drilldown of Event,	Priority, and Class	fication > Table View of Eve	nts > Packets						2015-09-08 17	:02:58 - 2015-	Expanding
No Search Constraints	(Edit Search)										
Jump to 🔻											
Messag	<u>e</u>				▼ <u>Priori</u>	ty	Cla	ssification		Count	
SERVER-	IIS cmd.exe access (1:1002)			high		Web	Application Attack		1	

第3步: 这还会触发"关联事件"

请注意将要隔离的源 IP 地址和基于 FireSIGHT LDAP/用户感知配置的用户信息。

Overview	Analysis Po	licies Devic	es Object	5 AMP							🔺 Health	System	Help 🔻
Context Ex	plorer Connect	ons • Intru	usions • F	iles 🔻 Hosts 🔻	Users •	Vulnerabilities •	Correlation >	Correlation Events	Custom •	Search			
									В	ookmark This Pa	age Report Designer Dash	board View	Bookmark
Correla	ation Events	5											
						Task Notificat Task Status Your t succeeded at Mon Sensors are being	ion ask Installation Setu Sep 7 12:30:51 201 registered, Check ta	× up (Register) L5 ask status to			ħ		
						monitor progress.					2015-00-08-1	7-02-59 - 20	15.00.09.1
Correlation	1 Events										2015-09-08 1.	/:02:58 - 20	E:
No Search C	Constraints (<u>Edit Sear</u>	<u>h</u>)											
Jump to													
	<u>▼ Time</u> ×	Impact ×	Inline × Result	Source IP ×	Source × Country	Destination × IP	Destination × Country	Security Intelligence	Source L	Jser ×	Destination × User	Source P ICMP Ty	<u>ort /</u> × pe
1 🗆	2015-09-08 19:15:	5 3		192.168.1.7		98.139.183.24	usa usa		John E	ppich (jeppich,	LDAP)	53245 / to	2

第4步: 随着我们继续处理同一事件 请注意目标端口和 pxGrid_Intrusion_Policy 规则中包含的规则违规。

erview Analy	sis Policies	Devices Obj	ects AN	1P						
text Explorer	Connections •	Intrusions •	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation > Correlation Events	Custom 🔻	Search	
ks Search										
										Į
-										
<u>19:27:21</u> Expanding										
Destination Po ICMP Code	ort / × Descrip	otion ×								

第5步: 随着我们继续深入处理同一事件 请注意已触发所分配的隔离缓解响应的关联策略和关联规则

AMP									🔺 Health	System	Help 🔻	admin
▼ Host	:s ▼ Users	 Vulnerabilities 	Correlation	• • Correlation	Events	Custom	 Search 	1				
Policy ×		Rule ×	Priority ×	Source ×	Destinati	on × 1	Ingress ×	Egress ×	Device ×	Ingress	× Egr	ess >
				Criticality	Criticality	. 7	Zone	Zone		Interface	Int	errace
pxGrid_AN	C_Quarantine	Quarantine by SourceIP	None	None		Р	assive		192.168.1.51	eth2		

第6步: 要在 ISE 中查看响应,请选择"操作"(Operations)->"身份验证"(Authentications)

ျပျပ cisco Identity Services Engine		Home Operations	Policy 🔍 Guest Access 🔍	License Warning A ise14sd Administration	admin Logout Feedback 🔎	Setup Assistan
Authentications	Adaptive Network Control	💊 Troubleshoot				
Misconfigured Supplicants (i)	Misconfigured Netw	ork Devices	RADIUS Drops (1)	Client Stopped Responer	nding (1) Re	epeat Counter (i)
🔝 Show Live Sessions 🛛 🏠 Add or Remove	Columns 🔻 👙 Refresh 💿 Reset R	epeat Counts	k	Refresh Every 1 minute	Show Latest 20 records	within Last 24 hours
Time Status Detai	s Repeat Count	Endpoint ID	Endpoint Profile (Authentication	Policy () Authorization Policy () Authorization	ation Profiles () Network Device ()	Device Port
Time Status Detai	's Repeat Count Identity () 0 jeppich	Endpoint ID (1) 00:0C:29:C8:EB:4F	Endpoint Profile () Authentication	Policy Authorization Policy Authorization Policy Authorization Policy	ation Profiles Network Device	Device Port
Time Status Detail 2015-09-08 23:15:18.995 0 2015-09-08 23:15:18.377 ☑	Identity i O jeppich	Endpoint ID () 00:0C:29:C8:EB:4F 00:0C:29:C8:EB:4F	Endpoint Profile (i) Authentication Microsoft-Workstatior Microsoft-Workstatior Default >> Dol	Policy i Authorization Policy i Policy i Authorization Policy i	tion Profiles () Network Device ()	Device Port
Time Status Detail 2015-09-08 23:15:18.395 0 0 2015-09-08 23:15:18.377 2 0 2015-09-08 23:15:18.327 2 0	Is Repeat Count Identity () 0 jeppich jeppich	Endpoint ID 00:0C:29:C8:EB:4F 00:0C:29:C8:EB:4F 00:0C:29:C8:EB:4F	Endpoint Profile () Authentication Microsoft-Workstatior Microsoft-Workstatior Default >> Dof	Policy () Authorization Policy	tition Profiles I Network Device I Netwo	Device Port (1) GigabitEthernet1/0/3

端口跳转

创建端口跳转关联策略

第1步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->创建策略 (Create Policy)-> pxGrid ANC portBounce->保存 (Save)

Overview Analysis Policies Devices Objects AMP		🔺 Health System Help 🔻 admin
Access Control Intrusion • Files Network Discovery SSL Applicatio	n Detectors Users Correlation Actions •	
		Alerts Remediations Group
Policy Management Rule Management White List Traffic Profile	25	
	Task Notification × Task Statue Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.	
Correlation Policy Information		Save Cancel
Policy Name pxGrid_ANC_portBounce		
Policy Description		
Default Priority None \$		
Policy Rules		O Add Rules

第2步: 策略 (Policies)->关联 (Correlation)->规则管理 (Rule Management)->创建规则 (Create Rule)->添加 规则名称->portBounce_by_SourceIP,并输入以下内容,然后保存 (Save)



第3步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->pxGrid ANC portBounce>添 加规则->选择 "portBounce_by_SourceIP",添加规则

第4步: 接下来,我们将添加响应,**点击响应**(Responses)选项卡

Overview Analysis Policies Devices Objects AMP		🔺 Health System Help 🔻 admin 🔻
Access Control Intrusion • Files Network Discovery SSL Application	Detectors Users Correlation Actions •	
		Alerts Remediations Group
Policy Management Rule Management White List Traffic Profile		
	Task Notification × Task Saking Your task Invalidion Sotug (Rejister) succeeded at Sat Aug 22 09:19:25 2015 succeeded at Sat Aug 22 09:19:25 2015 Sensions are being registered. Check task status to monitor progress.	
Correlation Policy Information		You have unsaved changes Save Cancel
Policy Name pxGrid_ANC_portBounce		
Policy Description		
Default Priority None =		
Policy Rules		O Add Rules
Rule	Responses	Priority
portBounce_bySourceIP	This rule does not have any responses.	Default 🗧 🎒 🗐

第5步: 选择策略 (Policies)->关联 (Correlation)->portBounce_by_SourceIP,将 portBounce 移至已分配的 响应(Assigned Responses)->更新 (Update)->保存 (Save)



第6步: 激活终止政策,点击将会打开该策略的以下按钮

Overview Analysis Policies Devices Objects AMP		🔺 Health System Help 🔻 admin 🔻
Access Control Intrusion • Files Network Discovery SSL Application	Detectors Users Correlation Actions •	
		Alerts Remediations Group
Policy Management Rule Management White List Traffic Profile	5	
		Create Policy
	Task Notification Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.	×
	Success Activated Policy: pxGrid_ANC_portBounce	×
		Sort by State :
pxGrid ANC portBounce		
pxGrid_ANC_Quarantine		
pxGrid_ANC_reAuthenticate		
pxGrid_ANC_shutdown		
pxGrid_ANC_Terminate		
pxGrid_ANC_Unquarantine		JE / 5

测试

最终用户将在其浏览器窗口中键入 <u>www.yahoo.com/cmd.exe</u>,这将会由于 FireSIGHT 的 pxGrid 入侵策略中发 生 "SERVER-IIS.cmd.exe 访问"规则违规而触发入侵事件。包含终端的端口将根据分配到关联策略中所定义 的规则的端口跳转缓解响应进行跳转。

第1步: 最终用户在其浏览器中输入 <u>www.yahoo.com/cmd.exe</u>

第2步: 这将触发"Web 应用攻击"(Web Application Attack)入侵事件

Overview Analysis Policies Devices Objects AMP						🔺 Health S	System Help	admin [·]
Context Explorer Connections ▼ Intrusions ≻ Events Files ▼ Hosts	▼ Users ▼	Vulnerabilities •	Correlation •	Custom •	Search			
Events By Drivity and Classification					Bookmark This Page Report Desig	ner Dashboard	View Bookmark	s Senech v
Events by Priority and Classification (switch workflow)								
	Task	Notification		×				
	Task S	tatus Your task Installat	ion Setup (Register)					
	Sensor	s are being registered.	Check task status to					
	monito	r progress.			2	015-09-08 17:0	2:58 - 2015-09-0	8 19:31:18 🤅
Drilldown of Event, Priority, and Classification > Table View of Events > Packets						010 00 00 1010		Expanding
No Search Constraints (<u>Edit Search</u>)								
Jump to 🔻								
Message		→ Priorit	¥	Clas	sification		Count	
SERVER-IIS cmd.exe access (1:1002)		high		Web	Application Attack		1	

第3步: 这还会触发"关联事件" 端口将针对属于源 IP 地址的主机进行跳转。

Overview Anal	lysis Policies	s Devices	Objects	AMP							🔺 Health S	iystem Help v adr
Context Explorer	Connections	 Intrusio 	ns 🔻 🛛 Fil	es 🔻 Hosts 🔻	Users •	Vulnerabilities •	Correlation +	Correlation Events	Custom •	Search		
									Bool	mark This Page Re	port Designer Dashboa	rd View Bookmarks Se
Correlation	Events											
						Task Notificat Task Status Your t succeeded at Mon Sensors are being monitor progress.	ion ask Installation Setu Sep 7 12:30:51 201 registered. Check ta:	⊮ p (Register) 5 sk status to			2015-09-07 22:3	5:00 - 2015-09-08 23:42
Correlation Events											2013 03 07 22.3	Store 2015 05 00 25.42
No Search Constraint	s (Edit Search)											
Jump to 🔻												
□ ▼ <u>Time</u>	× 1	Impact ×	Inline × Result	Source IP ×	Source × Country	Destination × IP	Destination × Country	Security Intelligence Category	× <u>Source</u> × <u>User</u>	Destination × User	Source Port / X ICMP Type	Destination Port / > ICMP Code
J <u>2015-09</u>	9-08 01:02:16	0		i <u>92.168.1.8</u>		98.139.180.149	🔤 USA				<u>49552 / tcp</u>	80 (http) / tcp

第4步: 随着我们继续处理同一事件

请注意 pxGrid_Intrusion_Policy 规则中包含的规则违规。

Overview Analysis Policies	Devices Obj	jects AM	IP							🔺 Health	System	Help 🔻
Context Explorer Connections •	Intrusions •	Files v	Hosts 🔻	Users •	Vulnerabilities •	Correlation + Correlation Events	Custom •	Search				
											•	
9												
Description ×												
[1:1002:18] "SERVER-IIS cmd.exe acce	ss" [Impact: Unkno	wn] From "192	2.168.1.51" a	at Tue Sep 8 0	5:02:20 2015 UTC [Cl	assification: Web Application Attack] [Priority:	1] {tcp} 192.1	68.1.8:49552	(unknown)->98	.139.180.149	1:80 (united	states)

第5步: 随着我们继续深入处理同一事件 请注意已触发所分配的端口跳转缓解响应的关联策略和关联规则

ects AMP								🔺 Health	System	Help 🔻	admin v
Files • Hosts •	Users • Vulnerabilities •	Correlation	n Correlation E	vents C	ustom 🔻	Search					
					k						
Policy ×	<u>Rule</u> ×	Priority ×	Source X Host Criticality	<u>Destination</u> <u>Host</u> <u>Criticality</u>	× Ingr Secu Zone	ress × urity	Egress × Security Zone	<u>Device</u> ×	<u>Ingress</u> <u>Interface</u>	× Egr Int	ress × erface
pxGrid_ANC_portBounce	portBounce_bySourceIP	None			Passi	ve		192.168.1.51	eth2		

第6步: 要在 ISE 中查看响应,请选择操作 (Operations)-身份验证 (Authentications)

ahah						License Warning 🔒 👔	ise14sd admin Logout	I Feedback	
cisco Identity Services	Engine	<u></u>	Home Operations	Policy Gue	st Access 🛛 🔻 🛛 Admini	istration 🛛 🔻			Setup Assista
Authentications	leports	Adaptive Network Control	💊 Troubleshoot						
Misconfigured Supplicat	nts (i)	Misconfigured Net	work Devices (i)	RADI	US Drops (i)	Client Stop	oed Responding (i)	Re	apeat Counter (i)
0		0		(D		0		0
🔝 Show Live Sessions 🛛 🎡 Add o	or Remove Colu	ımns 🔻 🛞 Refresh 🛭 💿 Reset	Repeat Counts			Refresh Every	1 minute 🔻 Show La	atest 20 records *	within Last 24 hour:
Time V Status	▼ Details	Repeat Count	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port
2015-09-08 05:06:44.968	0	0 00:0C:29:5F:04	E 00:0C:29:5F:04:E0	VMWare-Device					
2015-09-08 05:06:44.051	0	00:0C:29:5F:04	:E 00:0C:29:5F:04:E0	VMWare-Device	Default >> MAB >> De	f Default >> Basic_Auth	PermitAccess	sw	GigabitEthernet1/0/3
2015-09-08 05:04:10.726	ò	00:0C:29:5F:04	:E 00:0C:29:5F:04:E0		Default >> MAB >> De	f Default >> Default	DenyAccess	SW	GigabitEthernet1/0/3
2015-09-08 05:02:37.896	à	0 jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior					
2015-09-08 05:02:37.353	Ô.	jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior	Default >> Dot1X >> D	D Default >> Basic_Auth	PermitAccess	sw	GigabitEthernet1/0/3
2015-09-08 05:02:22.866	-		00:0C:29:C8:EB:4F					sw	
2015-09-08 04:32:21.130		jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior	Default >> Dot1X >> D	D Default >> Basic_Auth	PermitAccess	sw	GigabitEthernet1/0/3

第7步: 通过选择详细信息按钮,我们看到端口根据 CiscoAVpair 属性进行跳转

ConfigVersionId	41	
DestinationPort	1700	
Protocol	Radius	
Acct-Terminate-Cause	Admin Reset	
Event-Timestamp	1441688542	
AcsSessionID	ise14sd/231029914/147	
CPMSessionID	0A0000010000004001ED7026	
EndPointMACAddress	00-0C-29-C8-EB-4F	
Location	Location#All Locations	
Device Type	Device Type#All Device Types	
Device IP Address	192.168.1.3	
CiscoAVPair	audit-session-id=0A0000010000004001ED7026, subscriber:command=bounce-host-port	
ession Events		
2015-09-08 05:02:22.866	Dynamic Authorization succeeded	
2015-09-08 05:02:22.861	RADIUS Accounting stop request	
2015-09-08 04:32:21.953	RADIUS Accounting start request	

第8步: 此外,还可以查看 FireSIGHT 管理中心系统日志事件来验证端口跳转缓解操作是否成功

Overview Analysis Policies	Devices	Objects	АМР						🔺 He	alth System	Help 🔻	admin •	
							Local •	Updates	Licenses	Monitoring	Syslog	Tools •	
				Task Notifical <u>Task Status</u> Your i succeeded at Mon Sensors ar task status	tion task Installation Setup (Register) Sep 7 12:30:51 2015 re being registered. Check to monitor progress.	×	ħ						
Case-sensitive Exclusion		Message	s										
		Sep 08 2	015 01:16:00 Sourcefire3	D SF-IMS[15096]: [15106] pr	m:log [INFO] Process 'store_whitelist	history' closed o	utput.						
Go		Sep 08 2	Sep 08 2015 01:16:00 Sourcefire3D SF-IMS[15096]; [15096] pm:process [INF0] Started store_whitelist_history (21412)										
		Sep 08 2	015 01:11:00 Sourcefire3	D SF-IMS[15096]: [15106] pr	m:log [INFO] Process 'store_whitelist	_history' closed or	utput.						
		Sep 08 2	015 01:11:00 Sourcefire3	D SF-IMS[15096]: [15106] pr	m:log [INFO] Process 'store_whitelist	_history' closed or	utput.						
		Sep 08 2	015 01:11:00 Sourcefire3	D SF-IMS[15096]: [15096] pr	m:process [INFO] Started store_whit	elist_history (208	31)						
		Sep 08 2	015 01:06:00 Sourcefire3	D SF-IMS[15096]: [15106] pr	m:log [INFO] Process 'store_whitelist	_history' closed or	utput.						
		Sep 08 2	015 01:06:00 Sourcefire3	D SF-IMS[15096]: [15106] pr	m:log [INFO] Process 'store_whitelist	_history' closed or	utput.						
		Sep 08 2	015 01:06:00 Sourcefire3	D SF-IMS[15096]: [15096] pr	m:process [INFO] Started store_whit	elist_history (202	50)						
		Sep 08 2	015 01:02:17 Sourcefire3	D SF-IMS[11218]: pxgrid_age	ent.pl:normal [INFO] Mitigation Suco	essful							
		Sep 08 2	015 01:02:17 Sourcefire3	D SF-IMS[19876]: pxgrid_mit	igation.pl:normal [INFO] Notification	pushed to the so	cket						
		Sep 08 2	015 01:02:17 Sourcefire3	D SF-IMS[11218]: pxgrid_age	ent.pl:normal [INFO] Attempting Miti	gation: action=po	rtBounce, ip_ac	idress=192.16	8.1.8				
		Sep 08 2	015 01:02:01 Sourcefire3	D SF-IMS[15096]: [15106] pr	m:log [INFO] Process 'RUAScheduled	Download' closed	output.						

端口关闭

创建端口关闭关联策略。

第1步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->创建策略 (Create Policy)-> pxGrid_ANC_shutdown->保存 (Save)

Overview Analysis Pe	olicies De	vices Ob	jects Al	٩P							🛕 Health System Help 🕶 admin
Access Control Intrusion	n ▼ Files	Network	Discovery	SSL	Application De	etectors	Users	Correlation	Actions •		
											Alerts Remediations Groups
Policy Management	Rule Mana	gement	White Lis	t Tr	affic Profiles						
						Task Task St succeed	Notificati atus Your ta led at Mon S Sensors are task status	ON Isk Installation Setu Gep 7 12:30:51 201 being registered. C to monitor progress	p (Register) 5 heck	×	
Correlation Policy Int	formation										Save Cancel
Policy Name	pxGrid_ANC	_shutdown									
Policy Description											
Default Priority	None ‡										
Policy Rules											O Add Rules

第2步: 策略 (Policies)->关联 (Correlation)->规则管理 (Rule Management)->创建规则 (Create Rule)->添加 规则名称->shutdown_by_SourceIP,并输入以下内容,然后保存 (Save)

verview Ana	alysis Po	licies De	vices Ol	bjects A	MP				
cess Control	Intrusion	 Files 	Network	Discovery	SSL	Application D	etectors	Users	Correlatio
Policy Manag	ement	Rule Mana	gement	White Lis	t Tr	affic Profiles			
							Task	Notificati	on
							Task St	atus Your ta led at Mon S	sk Installation
								Sensors are	being registere
								task status I	to monitor prog
Rule Name	shu	tdown_bySour	ceIP						
Rule Description									
Rule Group	Un	grouped \$							
Select the ty	/pe of eve	ent for this	rule						
If an intrusio	on event occu	urs : and	it meets t	he following	conditio	ns:			
	Add conditi	ion 🚺 🔕 Ad	d complex c	ondition					

第3步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->pxGrid_ANC_shutdown>添加 规则 (Add rules)->选择 "shutdown_bySourceIP",添加规则

Overview Analysis	olicies Devices Ot	ojects AMP					
Access Control Intrusio	n 🔻 Files Network	Discovery SSL	Application Detectors	Users	Correlation	Actions •	
Policy Management Correlation Policy Ir Policy Name Policy Oscription Defailt Prority Policy Rules No Rules Currently Active	Rule Management	White List Th	Araffic Profiles Task Select the rules you wish t Gongrouped Rule Gongroupe	Notification Av to add to this ip ip rceIP rceIP	on aliable Rules policy, then click "/	Add".	× 1
						(Add Cancel

第4步: 接下来,我们将添加响应,点击响应(Responses)选项卡

Overview Analysis Policies Devices Objects AMP			🔺 Health System Help 🔻 admin v
Access Control Intrusion • Files Network Discovery SSL Applica	tion Detectors Users Correlation	Actions •	
			Alerts Remediations Groups
Policy Management Rule Management White List Traffic Pro	ïles		\
	Task Notification Task Statug Your task Installation Setup succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Ch task status to monitor progress.	X (Register) eck	
Correlation Policy Information			You have unsaved changes Save Cancel
Policy Name pxGrid_ANC_shutdown			
Policy Description			
Default Priority None :			
Policy Rules			Add Rules
Rule	Responses		Priority
shutdown_bySourceIP	This rule does not have any responses.		Default 🗢 🍘 j

第5步: 选择策略 (Policies)->关联 (Correlation)->pxGrid_ANC_shutdown,将 Shutdown 移至已分配的响应 (Assigned Responses)->更新 (Update)->保存 (Save)



第6步: 激活终止政策,点击将会打开该策略的以下按钮

Overview Analysis Policies Devices Objects AMP		🛕 Health System Help 🔻 admin 🔻
Access Control Intrusion Files Network Discovery SSL Application	on Detectors Users Correlation Actions •	
		Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profile	es	Country Balling
		Ureate Policy
	Task Notification Task Statu; Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:512 2015 Sensors are being registered. Check task status to monitor progress.	x
	Success Activated Policy: pxGrid_ANC_shutdown	×
		Sort by State +
pxGrid_ANC_shutdown		
pxGrid_ANC_portBounce		
pxGrid_ANC_Quarantine		
pxGrid_ANC_reAuthenticate		III / II
pxGrid_ANC_Terminate		
pxGrid_ANC_Unguarantine		

测试

最终用户将在其浏览器窗口中键入 <u>www.yahoo.com/cmd.exe</u>,这将会由于 FireSIGHT 的 pxGrid 入侵策略中发 生 "SERVER-IIS.cmd.exe 访问"规则违规而触发入侵事件。终端的端口将根据分配到关联策略中所定义的规则的端口关闭缓解响应进行关闭。

- **第1步:** 最终用户在其浏览器中输入 <u>www.yahoo.com/cmd.exe</u>
- **第2步:** 这将触发"Web 应用攻击"(Web Application Attack)入侵事件

Overview Anal	ysis Policies	Devices Objects A	AMP							+ 🛦	Health System Help v admin '
Context Explorer	Connections •	Intrusions > Events	Files v	Hosts 🔻	Users •	Vulnerabilities •	Correlation •	Custom	 Search 		
Events By P	Priority and	Classification (swi	itch workflow)		Task Task St succeed Sensors monitor	Notification atus Your task Installa led at Mon Sep 7 12:3 s are being registered. r progress.	tion Setup (Register) 0:51 2015 Check task status to	×	Boo	kmark This Page Report Designer E	Dashboard View Bookmarks Septch 🔻
vrilldown of Event,	Priority, and Class s (Edit Search)	sification > Table View of Eve	ents > <u>Packets</u>							2015-0	19-08 17:02:58 - 2015-09-08 19:31:18 (Expanding
Messag	<u>le</u>					✓ Priori	ty	<u>CI</u>	lassification		Count
SERVER	-IIS cmd.exe access	(1:1002)				high		We	eb Application At	ttack	1

第3步: 这还会触发"关联事件" 请注意,属于源 IP 地址的主机的端口将关闭

注意:由于未开启网络发现主机和用户,因此没有任何用户信息。

Overview Analysis Polic	ies Device	s Objects	AMP							🔺 Health S	iystem Help v admin
Context Explorer Connection	s 🔻 Intrus	ions 🔻 🛛 Fi	iles 🔻 Hosts 🔻	Users •	Vulnerabilities •	Correlation +	Correlation Events	Custom •	Search		
								Book	mark This Page Rep	oort Designer Dashboa	rd View Bookmarks Search
Correlation Events											
					Task Notificati Task Status Your ta succeeded at Mon S Sensors are being i monitor progress.	ion ask Installation Setu Sep 7 12:30:51 201 registered. Check ta:	× p (Register) 5 sk status to		k		
Correlation Events										2015-09-07 22:3	5:00 - 2015-09-08 23:42:00 Stati
No Search Constraints (<u>Edit Search</u>) Jump to •											
□ <u>Time</u> ×	Impact ×	Inline × Result	Source IP ×	Source × Country	Destination × IP	Destination × Country	Security Intelligence Category	× <u>Source</u> × <u>User</u>	Destination × User	Source Port / × ICMP Type	Destination Port / × ICMP Code
2015-09-08 02:13:38	0		192.168.1.8		98.139.183.24	usa				49885 / tcp	80 (http) / tcp

第4步: 随着我们继续处理同一事件 请注意 pxGrid_Intrusion_Policy 规则中包含的规则违规。

Context Explorer Connections V Intrusions V Files V Hosts V Users V Vulnerabilities V Correlation Correlation Events Custom V Search	
io.	
2	
Description ×	
[1:1002:18] "SERVER-IIS cmd.exe access" [Impact: Unknown] From "192.168.1.51" at Tue Sep 8 06:13:43 2015 UTC [Classification: Web Application Attack] [Priority: 1] {tcp} 192.168.1.8:49885 [unknown]->98.139.183.24:80	(united states)

第5步: 随着我们继续深入处理同一事件

请注意已触发所分配的端口关闭缓解响应的关联策略和关联规则

Dbi	ects AN	1P											🔺 Health	System	Help 🔻	admin v
•	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation	► Correla	ation	Events	Custor	m 🔻 Sea	rch					
													k			
						-				_	_			_		
ļ	Policy X		<u>Rule</u> ×		Priority ×	Source Host Criticality	×	Destinati Host Criticality	on ×	Ingress × Security Zone	Secu Zone	<u>iss</u> × irity	Device ×	Ingress Interface	× Egr Int	ess × erface
ŗ	xGrid ANC s	shutdown	shutdown	bySourceIP	None					Passive			192.168.1.51	eth2		

第6步: 要在 ISE 中查看响应,请选择操作 (Operations)->身份验证 (Authentications)

ahah			License Warning 🔥 ise14sd admin Logout	Feedback O
CISCO Identity Services Engine	Home Operations	Policy Guest Access Adminis	stration	Setup Assistar
Authentications Reports	Adaptive Network Control			
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter (1)
0	0	0	0	0
Add or Remove Col	umns 🔻 😵 Refresh 💿 Reset Repeat Counts		Refresh Every 1 minute * Show Lat	test 20 records vithin Last 24 hours
Time v Status Details	Repeat Count Identity Endpoint ID	Endpoint Profile	Authorization Policy () Authorization Profiles ()	Network Device () Device Port
2015-09-08 06:13:44.636 🕕 🗋	0 jeppich 00:0C:29:C8:EB:4F	Microsoft-Workstatior		
2015-09-08 06:13:44.636 🕕 🛕	0 00:0C:29:5F:04:E 00:0C:29:5F:04:E0	VMWare-Device		
2015-09-08 06:13:44.625 🔽 🔽	00:0C:29:C8:EB:4F			sw
2015-09-08 06:08:40.474 🛛	jeppich 00:0C:29:C8:EB:4F	Microsoft-Workstatior Default >> Dot1X >> D	Default >> Basic_Auth PermitAccess	sw GigabitEthernet1/0/3

第7步: 通过选择详细信息按钮,我们看到端口根据 CiscoAVpair 属性进行禁用

DestinationPort					
	1700				
Protocol	tocol Radius				
Acct-Terminate-Cause	arminate-Cause Admin Reset				
Event-Timestamp	ent-Timestamp 1441692824				
AcsSessionID	sSessionID ise14sd/231029914/167				
PMSessionID 0A000010000043022EA41A					
ndPointMACAddress 00-0C-29-C8-EB-4F					
Location	Location#All Locations				
Device Type	Device Type#All Device Types				
Device IP Address	192.168.1.3				
CiscoAVPair	audit-session-id=0A00000100000043022EA41A, subscriber:command=disable-host-port				
Session Events	DADUIS Association also request				
2015-09-08 06:13:44.636	RADIOS Accounting stop request				
2015-09-08 06:13:44.625	Dynamic Autonization succeeded				
2015-09-08 06:08:40.976	RADIUS Accounting start request				
2015-09-08 06:08:40.474	Autnentication succeeded				
2015-09-08 06:08:13.178	RADIUS Accounting start request				
2015-09-08 06:08:13.178 2015-09-08 06:08:12.592	RADIUS Accounting start request Authentication succeeded				

第8步: 此外,还可以查看 FireSIGHT 管理中心系统日志事件来验证端口关闭缓解操作是否成功



第9步: 此外,在交换机上,您将在端口上看到"shutdown"

interface GigabitEthernet1/0/3									
switchport mode access									
<mark>shutdown</mark>									
authentication host-mode multi-auth									
authentication open									
authentication order dot1x mab									
authentication priority dot1x mab									
authentication port-control auto									
authentication fallback mab									
mab									



创建重新身份验证策略

第1步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->创建策略 (Create Policy)-> pxGrid ANC reAuthenticate->保存 (Save)

Overview Analysis	Policies Devices Objects AMP				🔺 Health System Help 🔻 admin
Access Control Intrusi	on Files Network Discovery SS	SL Application Detectors	Users Correlation	Actions •	
					Alerts Remediations Group
Policy Management	Rule Management White List	Traffic Profiles			<u>k</u>
		Task Not Task Status succeeded Sen task	tification Your task Installation Setup at Mon Sep 7 12:30:51 2015 sors are being registered. Che status to monitor progress.	X (Register) bck	
Correlation Policy I	nformation				Save Cancel
Policy Name	pxGrid_ANC_reAuthenticate				
Policy Description					
Default Priority	None +				
Policy Rules					O Add Rules

第2步: 策略 (Policies)->关联 (Correlation)->规则管理 (Rule Management)->创建规则 (Create Rule)->添加 规则名称->reAuthenticate_bySourceIP,并输入以下内容,然后保存 (Save)

Overview Analysis Policies	Devices Objects AN	мр				
Access Control Intrusion • Fil	es Network Discovery	SSL	Application Dete	ctors Us	ers Corr	elation
Policy Management Rule M	anagement White List	t Trai	fic Profiles			
				Task Notif Task Status Yo succeeded at Sensor task st	ication our task Insta Mon Sep 7 12 is are being re atus to monit	llation Setu :30:51 201 egistered. C or progress
Rule Information Rule Name IreAuthentical Rule Description	e_bySourceIP					
Rule Group Ungrouped	\$					
Select the type of event for	his rule					
If an intrusion event occurs	and it meets the following o	conditions				
Add condition	Add complex condition			_		
Source IP		¢] [Is	\$ 192.168	.1.8		

第3步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->pxGrid_ANC_reAuthenticate> 添加规则 (Add rules)->选择 "reAuthenticate_bySourceIP",添加规则



第4步: 接下来,我们将添加响应,点击响应 (Responses) 选项卡

Overview Analysis Policies Devices Objects AMP		🛕 Health System Help 🔻 admin v
Access Control Intrusion • Files Network Discovery SSL Application D	etectors Users Correlation Actions •	
		Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles	1	89
	Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.	
Correlation Policy Information		You have unsaved changes Save Cancel
Policy Name pxGrid_ANC_reAuthenticate Policy Description		
Policy Rules		O Add Rules
Rule	Responses	Priority
reAuthenticate bySourceIP	This rule does not have any responses.	Default 🗧 🅼

第 5 步: 选择策略 (Policies)->关联 (Correlation)->pxGrid_ANC_reAuthenticate,将 reAuthenticate 移至已 分配的响应(Assigned Responses)->更新 (Update)->保存 (Save)

Overview Analysis	Policies Devi	ces Objects A	MP		a an			
Access Control Intrusio	on 🔻 Files	Network Discovery	SSL	Application Detectors	Users	Correlation	Actions 🔻	
Dallar Management	Dulo Monog	White Lie		offic Drofiles				
Policy Management	Kule Manage	iment white Lis	st 11	ame Promes				
				Task M Task Sta succeed	Notificatio atus Your tas ed at Mon Se	DN sk Installation Setu ep 7 12:30:51 201	p (Register) 5	×
				Responses for rea	Authentio	cate_bySource	eIP	
				Assigned Respo	onses			
Correlation Policy In	nformation			reAuthenticate				
Policy Name	pxGrid_ANC_r	eAuthenticate						
Default Priority	None ‡			Unassigned Re	sponses	× ^		
Policy Rules				Quarantine_Source	IP			
Rule				Shutdown Terminate				
reAuthenticate_bySou	rceIP			UnQuarantine_by_S portBounce	SourceIP			
							Updat	e Cancel

第6步: 激活终止政策,点击将会打开该策略的以下按钮

Overview Analysis Policies Devices Objects AMP	lealth System Help v admin v
Access Control Intrusion - Files Network Discovery SSL Application Detectors Users Correlation Actions -	
	Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles	k
	Create Policy
Task Notification × Task Status Your task Installation Setup (Register) succeeded at Who sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.	
Success × Deactivated Policy: pxGrid_ANC_pontBounce	
	Sort by State +
pxGrid_ANC_reAuthenticate	🔍 🖉 🖉
pxGrid_ANC_portBounce	III // 13
pxGrid ANC_Quarantine	🗆 🖉 🗄
pxGrid_ANC_shutdown	🗆 🖉 🗄
pxGrid_ANC_Terminate	🗆 🗶 🗄
pxGrid_ANC_Unquarantine	ST 2 3

测试

最终用户将在其浏览器窗口中键入 <u>www.yahoo.com/cmd.exe</u>,这将会由于 FireSIGHT 的 pxGrid 入侵策略中发 生 "SERVER-IIS.cmd.exe 访问"规则违规而触发入侵事件。最终用户将根据分配到关联策略中所定义的重新 身份验证缓解响应重新进行身份验证。

第1步: 最终用户在其浏览器中输入 <u>www.yahoo.com/cmd.exe</u>

第2步: 这将触发"Web 应用攻击"(Web Application Attack)入侵事件

安全访问操作指南





第3步: 这还会触发"关联事件" 请注意,属于源 IP 地址的最终用户将重新进行身份验证。

<u>注意</u>:由于未开启网络发现主机和用户,因此没有任何用户信息。

Overview Ana	ysis Policie	es Device	s Objects	AMP								🔺 Health	System Help 🖲	adn
Context Explorer	Connections	 Intrus 	ions 🔻 🛛 Fi	iles 🔻 Hosts 🔻	Users •	Vulnerabilities •	Correlation •	Correlation Events	Custom •	Search				
Correlation	Events								Во	okmark This	Page Repo	rt Designer Dashbo	ard View Bookma	rks Se
						Task Notificati Task Status Your ta succeeded at Mon S Sensors are being r monitor progress.	ON Isk Installation Setup Sep 7 12:30:51 2019 registered. Check tas	X p (Register) 5 sk status to						
Correlation Events												2015-09-07 22:3	5:00 - 2015-09-0	<u>1 23:4</u> S
No Search Constraint	s (Edit Search)													
Jump to 🔻														
<u>Time</u>	×	Impact ×	Inline × Result	Source IP ×	Source × Country	Destination × IP	Destination × Country	Security Intelligence Category	× Source User	× <u>Destin</u> <u>User</u>	ation ×	Source Port / X ICMP Type	Destination F	<u>ort /</u> 3
2015-09	08 01:28:56	0		192 168 1 8		08 130 180 140						49637 / tcp	80 (http) / tco	_

第4步: 随着我们继续处理同一事件

请注意 pxGrid_Intrusion_Policy 规则中包含的规则违规。

Explorer	Connections •	Intrusions •	Files •	Hosts •	Users •	Vulnerabilities •	Correlation + Correlation Events	Custom •	Search		
											ţ
J											
											_

第5步: 随着我们继续深入处理同一事件 请注意已触发所分配的重新身份验证缓解响应的关联策略和关联规则

cisco.

192.168.1.51 eth2

oje	cts Al	МР												🔺 Health	System	Help 🔻	admin
	Files v	Hosts 🔻	Users v	Vulnerabilities v	Correlation	► Correlat	tion I	Events	Custom	▼ S	earch						
P	olicy ×		Rule ×		Priority ×	Source	×	Destinatio	m × 1	Ingress	×	Egress	×	Device ×	Ingress	× Egr	ress
						Host		Host	-	Security		Security			Interface	Int	erface

Passive

第6步: 要在 ISE 中查看响应,请选择操作 (Operations)->身份验证 (Authentications)

None

pxGrid_ANC_reAuthenticate reAuthenticate_bySourceIP

ahah			License Warning A ise14sd admin Logout	Feedback D
cisco Identity Services Engine	Home Operations	Policy Guest Access Administ	ration 🔻	Setup Assistar
Authentications III Reports	Republic Adaptive Network Control			*
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding (i)	Repeat Counter (i)
0	0	0	0	0
🔝 Show Live Sessions 🛛 🎡 Add or Remove Co	lumns 🔻 😵 Refresh 🛛 😨 Reset Repeat Counts		Refresh Every 1 minute Show Lat	est 20 records vithin Last 24 hours
Time	Repeat Count Identity () Endpoint ID ()	Endpoint Profile () Authentication Policy ()	Authorization Policy	Network Device Device Port
2015-09-08 05:29:03.133 🕕 🗋	0 jeppich 00:0C:29:C8:EB:4F	Microsoft-Workstatior		
2015-09-08 05:29:02.437	jeppich 00:0C:29:C8:EB:4F	Microsoft-Workstatior Default >> Dot1X >> D.	Default >> Basic_Auth PermitAccess	Sw GigabitEthernet1/0/3
2015-09-08 05:29:02.175 🗹 🗋	00:0C:29:C8:EB:4F		8	SW
2015-09-08 05:06:44.968 ()	0 00:0C:29:5F:04:E 00:0C:29:5F:04:E0	VMWare-Device		

第7步: 通过选择详细信息按钮,我们看到端口根据 CiscoAVpair 属性进行禁用

Other Attributes		
ConfigVersionId	41	
DestinationPort	1700	
Protocol	Radius	
Event-Timestamp	1441690142	
AcsSessionID	ise14sd/231029914/154	
CPMSessionID	0A0000010000004102092652	
EndPointMACAddress	00-0C-29-C8-EB-4F	
Location	Location#All Locations	
Device Type	Device Type#All Device Types	
Device IP Address	192.168.1.3	
CiscoAVPair	audit-session-id=0A0000010000004102092652, subscriber:command=reauthenticate	
Session Events		
2015-09-08 05:29:02.437	Authentication succeeded	
2015-09-08 05:29:02.175	Dynamic Authorization succeeded	
2015-09-08 05:02:37.896	RADIUS Accounting start request	
2015-09-08 05:02:37.353	Authentication succeeded	

第8步: 此外,还可以查看 FireSIGHT 管理中心系统日志事件来验证重新身份验证缓解操作是否成功

						_		
Overview Analysis Policies Devices	Objects AMP				🔺 Heal	th System	Help 🔻	admin v
			Local 🔻	Updates	Licenses	Monitoring	Syslog	Tools
		Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.		k	•			
Case-sensitive Exclusion	Messages							
	Sep 08 2015 01:36:00 Sourcefire3D SF	-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_histo	ory' closed output.					
Go	Sep 08 2015 01:36:00 Sourcefire3D SF	-IMS[15096]: [15096] pm:process [INFO] Started store_whitelist_	history (24188)					
	Sep 08 2015 01:31:00 Sourcefire3D SF	-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_histo	ory' closed output.					
	Sep 08 2015 01:31:00 Sourcefire3D SF	-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_histe	ory' closed output.					
	Sep 08 2015 01:31:00 Sourcefire3D SF	-IMS[15096]: [15096] pm:process [INFO] Started store_whitelist_	history (23616)					
	Sep 08 2015 01:28:56 Sourcefire3D SF	-IMS[11218]: pxgrid_agent.pl:normal [INFO] Mitigation Successful	I					
	Sep 08 2015 01:28:56 Sourcefire3D SF	-IMS[23376]: pxgrid_mitigation.pl:normal [INFO] Notification push	ned to the socket					
	Sep 08 2015 01:28:56 Sourcefire3D SF	-IMS[11218]: pxgrid_agent.pl:normal [INFO] Attempting Mitigation	n: action=reAuthenticate, i	p_address=192.16	58.1.8			
	Sep 08 2015 01:28:03 Sourcefire3D SF	-IMS[20715]: [29011] sftunneld:sf heartbeat [INFO] Saved SW VE	ERSION from peer 192.168	.1.51 (5.4.0)				

终止

创建终止关联策略

第1步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->创建策略 (Create Policy)-> pxGrid ANC Terminate->保存 (Save)

Overview Analysis Policies Devices Objects AMP		🛕 Health System Help 🔻 admin
Access Control Intrusion • Files Network Discovery SSL Application D	etectors Users Correlation Actions •	
Policy Management Rule Management White List Traffic Profiles		Alerts Remediations Group:
	Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensora are being registered. Check task status to monitor progress.	
Correlation Policy Information		Save Cancel
Policy Name pxGrid_ANC_Terminate		
Policy Description		
Default Priority None \$		
Policy Rules		O Add Rules

第2步: 策略 (Policies)->关联 (Correlation)->规则管理 (Rule Management)->创建规则 (Create Rule)->添加 规则名称->Terminate_by_SourceIP,并输入以下内容,然后保存 (Save)



第3步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->pxGrid ANC Terminate>添加 规则 (Add rules)->选择"Terminate_by_SourceIP",添加规则



第4步: 接下来,我们将添加响应,点击响应(Responses)选项卡

Dverview Analysis Policies Devices Objects AMP		🔺 Health System Help 🔻 admin 🔻
Access Control Intrusion • Files Network Discovery SSL Applica	ation Detectors Users Correlation Actions •	
		Alerts Remediations Groups
Policy Management Rule Management White List Traffic Pro	files	•
	× Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:12 2015 Sensors are being registered. Check task status to monitor progress.	
Correlation Policy Information		You have unsaved changes Save Cancel
Policy Name pxGrid_ANC_Terminate Policy Description		
Policy Rules		O Add Rules
Rule	Responses	Priority
terminate_bySourceIP	This rule does not have any responses.	Default 🗧 🏟 🛊

第5步: 选择策略 (Policies)->关联 (Correlation)->pxGrid_ANC_Terminate,将 Terminate 移至已分配的响 应(Assigned Responses)->更新 (Update)->保存 (Save)

Overview Analysis Policies Devices Objects	AMP
Access Control Intrusion • Files Network Discove	ery SSL Application Detectors Users Correlation Actions •
Policy Management Rule Management White	e List Traffic Profiles
	Task Notification ×
	Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015
	Responses for terminate_bySourceIP
	Assigned Responses
Correlation Policy Information	Terminate
Policy Name pxGrid_ANC_Terminate	
Policy Description Default Priority None	Unassigned Responses
Policy Rules	Quarantine_SourceIP
Rule	Shutdown UnQuarantine_by_SourceIP
terminate_bySourceIP	portBounce reAuthenticate
	Update Cancel

第6步: 激活终止政策,点击将会打开该策略的以下按钮

Overview Analysis Policies Devices Objects AMP	🔺 Health	System Help v admin
Access Control Intrusion - Files Network Discovery SSL Application Detectors Users Correlation Actions -		
Policy Management Rule Management White List Traffic Profiles	٨	Alerts Remediations Groups
		O Create Policy
Task Notification × Task Steps Your task Installation Setup (Register) succeeded at Who sep 7 12:0:51 2015 Sensors are being registered. Check task status to monitor progress.		
Success × Activated Policy: pxGrid_ANC_Terminate		
		Sort by State :
pxGrid_ANC_Terminate		CO / 6
pxGrid_ANC_portBounce		IN / 1
pxGrid_ANC_Quarantine		()X 🥖 🖯
pxGrid_ANC_reAuthenticate		()x 🥜 🖯
pxGrid_ANC_shutdown		() X 2
pxGrid_ANC_Unguaranting		()X) 🥜 🖯

测试

最终用户将在其浏览器窗口中键入 <u>www.yahoo.com/cmd.exe</u>,这将会由于 FireSIGHT 的 pxGrid 入侵策略中发 生 "SERVER-IIS.cmd.exe 访问"规则违规而触发入侵事件。最终用户的会话将根据分配到关联策略中所定义 的规则的终止缓解响应进行终止。

- 第1步: 最终用户在其浏览器中输入 <u>www.yahoo.com/cmd.exe</u>
- **第2步:** 这将触发"Web 应用攻击"(Web Application Attack)入侵事件

Overview Analysis Policies	Devices Objects	AMP						🔺 Health	System Help 🔻	admin
Context Explorer Connections •	Intrusions > Events	Files • Hosts •	Users • V	/ulnerabilities 🔻	Correlation •	Custom •	Search			
Events By Priority and	Classification (see	ritch workflow)					Bookmark This Pag	ge Report Designer Dashboa	rd View Bookmarks	Septch V
		×								
Drilldown of Event, Priority, and Clas	sification > Table View of Even	ents > Packets						2015-09-08 17	202:58 - 2015-09-0	Expanding
No Search Constraints (Edit Search)										
Jump to 🔻										
Message				▼ Priorit	¥	Clas	ssification		Count	
SERVER-IIS cmd.exe access	(1:1002)			high		Web	Application Attack		1	

- **第3步:** 这还会触发"关联事件" 请注意,属于源 IP 地址的最终用户会话将终止
- <u>注意</u>:由于未开启网络发现主机和用户,因此没有任何用户信息。

Overview Anal	ysis Policies	Devices	Objects	AMP							🛕 Health	System Help v admin
Context Explorer	Connections •	Intrusion	ns ▼ File	s ▼ Hosts ▼	Users •	Vulnerabilities •	Correlation •	Correlation Events	Custom •	Search		
Correlation	Events								Bo	okmark This Page R	eport Designer Dashboa	ard V Bookmarks Search
						Task Notificati Task Status Your to succeeded at Mon S Sensors are being i monitor progress.	ion ask Installation Setu Sep 7 12:30:51 201 registered. Check ta:	× p (Register) 5 sk status to				
Correlation Events											2015-09-07 22:3	5:00 - 2015-09-08 23:42:00 Static
No Search Constraints	s (Edit Search)											
Jump to 🔻												
▼ <u>Time</u>	× Im	pact × 1	Inline × Result	Source IP ×	Source × Country	Destination × IP	Destination × Country	Security Intelligence Category	× <u>Source</u> <u>User</u>	Contraction Destination Destination	Source Port / X ICMP Type	Destination Port / × ICMP Code

第5步:

第4步: 随着我们继续处理同一事件

请注意 pxGrid_Intrusion_Policy 规则中包含的规则违规。

context explorer	Connections •	Intrusions •	Files v	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation > Correlation Events	Custom •	Search			
1												
٥												
Description ¥												
Description A												
[1:1002:18] "SERVE	P-IIS cmd eve acces	" [Impact:] Inknow	n] From "197	2 168 1 51" at	t Tue Sen 8.0	5-43-31 2015 LITC [C	assification: Web Application Attack] [Driority	- 11 /tcn\ 192 1	68 1 8-49687	(unknown)=>98.1	139 180 149-8	0 (united stat
[1:1002:18] "SERVE	R-IIS cmd.exe acces	s" [Impact: Unknow	n] From "192	2.168.1.51" a	t Tue Sep 8 0	5:43:31 2015 UTC [C	assification: Web Application Attack] [Priority	: 1] {tcp} 192.1	68.1.8:49687	(unknown)->98.1	139.180.149:8	80 (united stat
[1:1002:18] "SERVE	R-IIS cmd.exe acces	s" [Impact: Unknow	n] From *192	2.168.1.51" a	<u>t Tue Sep 8 0</u>	5:43:31 2015 UTC [C	assification: Web Application Attack1 [Priority	: 1] {tcp} 192.1	68.1.8:49687	(unknown)->98.1	139.180.149:8	80 (united stat
^[1:1002:18] "SERVE 随着我们	^{R-IIS cmd.exe access} 门继续深	^{s" [Impact: Unknow} K入处理	/n] From *192	^{2.168.1.51"} ª	t Tue Sep 8 0	5:43:31 2015 UTC [C	assification: Web Application Attack] [Priority	: 1] {tcp} 192.1	68.1.8:49687	(unknown)->98.1	139.180.149:8	80 (united stat
[1:1002:18] "SERVE 随着我们 言注音 F	R-IIS cmd.exe access 门继续深 日妯发所	* [*] []mpact: Unknow 关入处理 关入配的	n] From *192 1 同 —	^{2.168.1.51"} •事件	t Tue Sep 8 0	5:43:31 2015 UTC [C	assification: Web Application Attack] [Priority 在 四文	: 1] {tcp} 192.1	<u>68.1.8:49687</u>	(unknown)->98.1	139.180.149:8	80 (united stat
(1:1002:18] "SERVE 随着我们 清注意已	^{R-115 cmd.exe access} 门继续深 己触发所	[。] [Impact: Unknow 、 、 、 、 い た の 、 の の 、 の の 、 の 、 の 、 の 、 の の の 、 の の の 、 の 、 の 、 の 、 の 、 の 、 の の 、 の の の 、 の の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 、 、 の 、 、 、 、 の 、 、 、 の 、 、 、 、 、 、 、 の 、 、 の 、 、 、 、 の 、 、 、 、 、 、 、 、 、 、 、 の 、 、 、	^{m] From *192} 1同一 1终止	2.168.1.51"。 ·事件 :缓解	_{t Tue Sep 8 0}	^{5:43:31 2015 UTC IC 的关联分}	asaification: Web Application Attack1 [Priority 策略和关联规则	: 1] {tcp} 192.1	68.1.8:49687	(unknown)->98.1	139.180.149:8	0 (united stat
[<u>1:1002:18]*SERVE</u> 随着我们 清注意已	R-IIS cmd.exe access 门继续深 已触发所	^{s" []mpact: Unknow} K入处理 f分配的	□] From *192 1] 同一] 终止	<u>2.168.1.51</u> 。 ·事件 :缓解	t Tue Sep 8 0	^{5:43:31 2015 UTC IC 的关联分}	asaffication: Web Application Attack] [Priority 宽略和关联规则	: 1] {tcp} 192.1	68.1.8:49687	(unknown)->98.1	139.180.149:8	80 (united stat
[1:1002:18] "SERVE 随着我们 清注意已	R-115 cmd.exe acces 门继续深 已触发所	^{a[*] IImpact: Unknow 至入处理 行分配的}	n] From *192 1同一 1终止	<u></u> ·事件 :缓解	t Tue Sep 8 0	^{5:43:31 2015 UTC [C}	assification: Web Application Attack] [Priority 寛略和关联规则	: 1] {tcp} 192.1	68.1.8:49687 68. 1.8:49687 elp ▼ adm	(unknown)->98.1	139.180.149:8	30 (united stat
[1:1002:18] *SERVE 随着我们 清注意已 jects AMP Files Hot	R-]IS cmd.exe access 门继续深 已触发所	** IImpact: Unknow 致入处理 行分配的 Vulnerabilities	n] From *192 1]同一]终止	2.168.1.51*。 •事件 :缓解	t Tue Sep 8 0	5:43:31 2015 UTC [C 的关联分	assification: Web Application Attack] [Priority 宦略和关联规则 ▲ Health Search	: 1] {tcp} 192.1 System H	68.1.8:49687 68. 1.8:49687 elp ▼ adm	(unknown)->98.1	139.180.149:8	30 (united stat
Li:1002:181*SERVE 道着我们 青注意已 jects AMP Files → Hor	R-115 cmd.exe access 门继续济 已触发所 sts、Users、	* [*] [Impact: Unknow 致入处理 行分配的 Vulnerabilities	n] From *192]同一]终止	2.168.1.51*ª ·事件 :缓解	t Tue Sep 8 0	5:43:31 2015 UTC [C 的关联分	astification: Web Application Attack] [Priority 食略和关联规则 ▲ Health ▼ Search	: 1] {tcp} 192,1	68.1.8:49687 elp v adm	(unknown)->98.1	139.180.149:6	10 (united stat

Policy ×	<u>Rule</u> ×	Priority ×	Source × Host Criticality	Destination × Host Criticality	Ingress × Security Zone	Egress X Security Zone	Device ×	Ingress × Interface	Egress Interface	¢
pxGrid ANC Terminate	terminate bySourceIP	None			Passive		192.168.1.51	eth2		

第6步: 要在 ISE 中查看响应,请选择"操作"(Operations)-"身份验证"(Authentications)

								Lie	anna Maraina 🔗 🚛 ia	alded L admin L	Loopert 1	Foodback 0	_
abab								00	ense warning AL T is	eraza i sonun i	Logout	reduced ())	
cisco Idei	ntity Services E	ngine		6	Home Operations	Policy V	Guest Access	Administration	•				
Authentica	ations 📑 Rep	oorts	Adaptive N	etwork Control	💊 Troubleshoot								
Misco	nfigured Supplicants		Ν	Aisconfigured Ne	twork Devices	RA	DIUS Drops		Client Stopp	ed Responding			Rep
	0			0			0		(D			
i Show Live S	U U U Image: Show Live Sessions [®] Add or Remove Columns ~ [®] Refresh [®] Reset Repeat Counts Refresh Every 1 minute ~ Show Latest 20 records ~												
Time	▼ Status	Details	Repeat Count	Identity (i)	Endpoint ID	Endpoint Profile	Authentication	Policy (i) Author	orization Policy (i)	Authorization Pro	files ()	Network Device	3
2015-09-08 05:4	43:34.043 🕕	ò	0	jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstati	or						
2015-09-08 05:4	43:33.832 🔽	ò		jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstati	or Default >> Do	t1X >> D Defau	ult >> Basic_Auth	PermitAccess	s	w	
2015-09-08 05:4	43:33.618 🔽	Q			00:0C:29:C8:EB:4F						s	w	
2015-09-08 05:2	29:02.437	ò		jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstati	or Default >> Do	t1X >> D Defau	It >> Basic_Auth	PermitAccess	5	św	-

第7步: 此外,还可以查看 FireSIGHT 管理中心系统日志事件来验证终止缓解操作是否成功

Overview Analysis Policies Devices O	Dbjects AMP				🔺 He	alth System Help v	admin 🔻
			Local •	Updates	Licenses	Monitoring ► Syslog	Tools •
		Task Notification × Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.				*	
Case-sensitive Exclusion	Messages						
	Sep 08 2015 01:43:28 Sourcefire3D 5	SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Mitigation Successful					
Go	Sep 08 2015 01:43:27 Sourcefire3D 5	SF-IMS[25338]: pxgrid_mitigation.pl:normal [INFO] Notification pushed to the so	ket				
	Sep 08 2015 01:43:27 Sourcefire3D 5	SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Attempting Mitigation: action=ter	minate, ip_ado	iress=192.168	.1.8		

取消隔离关联策略

取消隔离关联策略和规则的创建过程与其余关联策略相同。唯一区别在于将从"连接事件"而不是在"入侵" 事件上触发关联规则。当最终用户浏览至取消隔离规则中定义的 URL 时,取消隔离缓解响应将取消隔离终端。

我们还将需要创建"连接"规则,以便所有 HTTP/HTTPS 流量都受监控并进行记录,且分配到还包含 pxGrid 入侵策略的默认访问策略。

第1步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->创建策略 (Create Policy)-> pxGrid_ANC_Unquarantine->保存 (Save)

Overview Analysis Policies Devices Objects AMP	🔺 Health System Help 🔻 admin
Access Control Intrusion - Files Network Discovery SSL Application Detectors Users Correlation Actions -	
Policy Management Rule Management White List Traffic Profiles	Alerts Remediations Groups
Task Notification × Task Status Your task (retailation Setup (Register) succeeded at How Set 71 23:30:51 2015 Sensors are being registered. Check task status to monitor progress.	
Correlation Policy Information	Save Cancel
Policy Name pxGrid_ANC_Unquarantine	
Policy Description	
Default Priority None :	
Policy Rules	Add Rules

第2步: 策略 (Policies)->关联 (Correlation)->规则管理 (Rule Management)->创建规则 (Create Rule)->添加 规则名称->UnQuarantine_by_DestinationIP, 然后保存 (Save)

verview Analysis Policies Devices O	bjects AMP					
cess Control Intrusion • Files Networ	k Discovery SSL	Application D	Detectors	Users	Correlation	Actions
Policy Management Rule Management	White List T	rattic Profiles				
			Task N	lotificati	on	
			Task Sta succeede	tus Your ta sd at Mon S	sk Installation Setu ien 7 12:30:51 201	p (Register
			s	ensors are	being registered. C	- heck
			t	ask status I	to monitor progress	
Rule Information						
Rule Name UnQuarantine_by_SourceIP						
Rule Description						
Duk Cours						
Congrouped •						
Select the type of event for this rule						
Select the type of event for this full						
If a connection event occurs + at either the be	sginning or the end of th	e connection :	and it me	ets the fo	llowing condition	9:
Add condition Add complex	condition					
X URL	\$ is		: http://	192.168.1	14/Unguarantine/u	

第3步: 策略 (Policies)->关联 (Correlation)->策略管理 (Policy Management)->pxGrid_ANC_Unquarantine-> 添加规则 (Add rules)->UnQuarantine_by_DestinationIP, 然后保存 (Save) 更改



第4步: 接下来,我们将添加响应,点击响应(Responses)选项卡

Overview Analysis Policies Devices Objects AMP		🔺 Health System Help 🔻 admin
Access Control Intrusion • Files Network Discovery SSL Application Det	tectors Users Correlation Actions •	
		Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles		.
	Task Notification × Task Status Your task installation Setup (Register) succeeded at No. 66 7 12:30:51 > Sensors are being registered. Check task status to monitor progress. >	•
Correlation Policy Information		You have unsaved changes Save Cancel
Policy Name pxGrid_ANC_Unquarantine		
Policy Description		
Default Priority None :		
Policy Rules		O Add Rules
Rule	Responses	Priority
UnQuarantine_by_SourceIP	This rule does not have any responses.	Default 🗧 🧃 🗒

第5步: 选择策略 (Policies)->关联 (Correlation)->UnQuarantine_by_DestinationIP,将 UnQuarantine_SourceIP 移至已分配的响应 (Assigned Responses)->更新 (Update)->保存 (Save)

Overview Analysis	Policies Dev	vices Objects	AMP					
Access Control Intrusio	on 🔻 🛛 Files	Network Discov	ery SSL	Application Detec	tors Users	Correlation	Actions •	
Policy Management	Rule Manag	ement Whit	e List T	raffic Profiles				<u> </u>
				Т	ask Notificat	ion		×
				I s	ask Status Your t ucceeded at Mon	ask Installation Setu Sep 7 12:30:51 201	up (Register) L5	
				Responses f	or UnQuaran	tine_by_Sourc	eIP	
				Assigned	Responses			
Correlation Policy Ir	formation			UnQuarantin	e_by_SourceIP			
Policy Name	pxGrid_ANC_	Unquarantine						
Policy Description								
Default Priority	None ‡			Unassigne	d Responses	* ^		
Policy Rules				Quarantine_	SourceIP			
Rule				Terminate				
UnQuarantine_by_Sou	rceIP			reAuthentica	te			
							Updat	e Cancel

第6步: 激活策略

Overview Analysis Policies Devices Objects AMP		🔺 Health System Help 🔻 admin
Access Control Intrusion • Files Network Discovery SSL Application	Detectors Users Correlation Actions •	
		Aluxis Remediations Groups
Policy Management Rule Management White List Traffic Profile	s	
		Create Policy
	Task Notification <u>Task Status</u> Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.	×
	Success Activated Policy: pxGrid_ANC_Unquarantine	×
		Sort by State ÷
pxGrid_ANC_Unquarantine		C 2 6
pxGrid_ANC_portBounce		
pxGrid_ANC_Quarantine		
pxGrid_ANC_reAuthenticate		
pxGrid_ANC_shutdown		
pxGrid_ANC_Terminate		

测试

最终用户将在其浏览器窗口中键入 <u>www.yahoo.com/cmd.exe</u>,这将会由于 FireSIGHT 的 pxGrid 入侵策略中发 生 "SERVER-IIS.cmd.exe 访问"规则违规而触发入侵事件。终端将根据分配到关联策略中所定义的规则的取 消隔离缓解响应来取消隔离。

- **第1步:** 最终用户在其浏览器中输入 http://192.168.1.14/Unquarantine/unquarantine.htm
- 第2步: 这将触发"连接"事件

_															
C	verview	Analysis Polic	ies Devices Ob	jects /	AMP								🛕 Health 🛛 Sys	tem Help 🔻	ad
С	ontext E>	plorer Connectio	ons ► Events Int	rusions 🔻	Files 🔻	Hosts 🔻 U	sers 🔻 V	/ulnerabilities 🔻	Correlation •	Custom •	Search				
											Bookmark	This Page Report I	Designer D board Vi	ew Bookmarks	Sea
C	Conne	ction Events	(switch workflow)				Task Not Task Status succeeded a Sensors are monitor pro	tification Your task Installat at Mon Sep 7 12:30 a being registered. (ggress.	ion Setup (Register :51 2015 Check task status tr	×)			Malicious URLs Possible Database Acc Risky Applications with Standard HTTP Standard Mail Standard SSL 2015-09-08 17:02:0	ess h Low Business I 0 - 2015-09-09	telev
•	Search Co	onstraints (Edit Search S	Save Search)	onnecuon E	vents										5
ľ		→ <u>First Packet</u>	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zor	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	<u>C</u>
		2015-09-08 19:43:26	2015-09-08 19:45:22	Allow		192.168.1.7		192.168.1.14	1	Passive		53348 / tcp	80 (http) / tcp	HTTP	
ſ	L 🗌	2015-09-08 19:39:36	2015-09-08 19:43:03	Allow		192.168.1.7		192.168.1.14	1	Passive		53334 / tcp	80 (http) / tcp	HTTP :	
															a

第3步: 此处是连接事件的持续

					🔺 Health	System	Help 🔻	admin 🔻
ilities 🔻	Correlation •	Custom •	Search					
Search v								
10.45.00								
Static								
Client	Web	URL			URL	URL	De	evice
	Application				category	Reputa		
Firefo	<u>Web Browsin</u>	g <u>http://19</u>	2.168.1.14/f	avicon.ico			<u>19</u>	2.168.1.51
Firefo	x Web Browsine	g http://19	2.168.1.14/L	Inquarantine/unquarantine.htm			19	2.168.1.51

第5步:

第6步:

第4步: 这还会触发"关联事件" 请注意,源IP地址将取消隔离。

orrelation Events							Bookmark This Page Re	eport Designer Dasl	hboard View Bookmark	
				Task Notifica Task Status Succeeded at Mon Sensors are being monitor progress.	tion task Installation Set o Sep 7 12:30:51 20 o registered. Check t	x up (Register) 15 ask status to		2015-09-08 1	7:02:00 - 2015-09-09	
rrelation Events Search Constraints (Edit Search)										
Iump to • • Time × Impa	act × Inline × Result	Source IP ×	Source × Country	Destination × IP	Destination × Country	Security Intelligence × Category	Source User ×	Destination × User	Source Port / × ICMP Type	
2015-09-08 19:42:58		i <u>92.168.1.7</u>		192.168.1.14			John Eppich (jeppich, LDAP)		53334 / tcp	
有社息生按手	中件 o evices Objects	АМР							🔺 Health System	Help v adm
「打社思注好事 View <mark>Analysis</mark> Policies Dd ⊄ Explorer Connections・」 Search	中一十 o evices Objects Intrusions v Fil	AMP es • Hosts •	Users ▼	Vulnerabilitie	s v Correlati	ion > Correlation Event	ts Custom ▼ Search		🔺 Health System	Help v adm
肩壮思进按手 /ew <mark>Analysis</mark> Policies Dd d Explorer Connections・1 Search	中1牛 o evices Objects Intrusions・ Fil	AMP es • Hosts •	Users ▼	Vulnerabilitie:	s v Correlati	ion > Correlation Event	ts Custom ▼ Search		▲ Health System	Help v adm
肩社思进按手 View Analysis Policies Do At Explorer Connections ▼ Search	・1牛 。 evices Objects Intrusions • Fil	AMP es • Hosts •	Users V	Vulnerabilitie	s • Correlati	ion • Correlation Event	ts Custom • Search		▲ Health System	Help v adm
肩汁.思. 建按手 view Analysis Policies Do t Explorer Connections • 1 Search Static Destination Port / × Descriptio	・1牛。 evices Objects Intrusions・ Fil	AMP es • Hosts •	Users •	Vulnerabilitie	Correlati	ion > Correlation Event	ts Custom • Search		▲ Health System	Heip▼ adm
「行社.思.廷按手 view Analysis Policies Do at Explorer Connections ▼ 1 Search Search Destination Port / × Descriptio ECRPF Code 80 (http://tog Connection.	n × Type: FireSiGHT	AMP es • Hosts •	Users •	Vulnerabilitie	s v Correlati	ion > Correlation Event	ts Custom • Search		▲ Health System	Heip v adm
「行社思 建按手 View Analysis Policies Do at Explorer Connections・ Search Search Destination Port / × Descriptio ICMP Code Big (http://tog Connection	evices Objects Intrusions · Fil max Type: FireSIGHT	AMP es • Hosts • Hosts •	Users ▼	Vulnerabilitie	s v Correlat	ion + Correlation Event	ts Custom • Search		▲ Health System	Help • adm

ts AMP								🔺 Health	System	Help 🔻	admin y
Files • Hosts •	Jsers • Vulnerabilities •	Correlation	• • Correlation	Events Cu	stom 🔻	Search					
Policy ×	<u>Rule</u> ×	Priority ×	Source X Host Criticality	Destination × Host Criticality	Ingres Securi Zone	iss × ty	Egress X Security Zone	<u>Device</u> ×	<u>Ingress</u> Interface	× Eq Int	ress × terface
pxGrid_ANC_Unquaranti	ne UnQuarantine_by_SourceIP	None	None	None	Passive			192.168.1.51	eth2		

第7步: 要在 ISE 中查看响应,请选择操作 (Operations)->身份验证 (Authentications)

رابدان cisco Identity Services Engine	Home Operations	▼ Policy I ▼ Guest Access I ▼ Adm	. Ucense Warning \hat{j}_{1} ise14sd admin Logout Feed inistration $\mid \Psi$	back 🔎 Setup Assista
Authentications III Reports	Adaptive Network Control 💦 Troubleshoot			
Misconfigured Supplicants (i)	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding (i)	Repeat Counter (i)
0	0	0	0	0
🗐 Show Live Sessions 🙀 Add or Remove Co	lumns 🔻 🍪 Refresh 💿 Reset Repeat Counts		Refresh Every 1 minute Show Latest 20	records vithin Last 24 hours
Time Status Details	Repeat Count Identity () Endpoint ID ()	Endpoint Profile (i) Authentication Policy	Authorization Policy Authorization Profiles Netwo	rk Device ⁽¹⁾ Device Port ⁽¹⁾
2015-09-08 23:43:06.661 🕕 🗋	0 jeppich 00:0C:29:C8:EB:4F	Microsoft-Workstatior		
2015-09-08 23:43:06.289 🔽 🗋	jeppich 00:0C:29:C8:EB:4F	Microsoft-Workstatior Default >> Dot1X >>	D Default >> Basic_Auth PermitAccess sw	GigabitEthernet1/0/3
2015-09-08 23:43:05.772	00:0C:29:C8:EB:4F		SW	

第8步: 此外,还可以查看 FireSIGHT 管理中心系统日志事件来验证取消隔离缓解操作是否成功

Overview Analysis Policies Devices	Dbjects AMP		🔺 Hea	lth System Help •
		Local Up	dates Licenses	Monitoring > Syslog
	× <u>Task Notification</u> × <u>Task Status</u> Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015 Sensors are being registered. Check task status to monitor progress.	k		
Case-sensitive Exclusion	Messages			
	Sep 08 2015 19:42:59 sd SF-IMS[5214]: pxgrid_agent.pl:normal [INFO] Mitigation Successful			
Go	Sep 08 2015 19:42:58 sd SF-IMS[24297]: pxgrid_mitigation.pl:normal [INFO] Notification pushed to the socket			
	Sep 08 2015 19:42:58 sd SF-IMS[5214]: pxgrid_agent.pl:normal [INFO] Attempting Mitigation: action=unquarantine, ip_	address=192.168.1	1.7	
	Sep 08 2015 19:41:48 sd SF-IMS[3890]: [4674] SFDataCorrelator:imcloudpool [WARN] bad txid: 0			



故障排除

ISE pxGrid 服务未显示

解决方法:在 ISE pxGrid 节点上运行/停止"application stop ise"。

pxGrid 代理证书错误消息

解决方法:查看 FireSIGHT 管理中心系统日志消息以了解证书错误消息。 确保证书的完整路径正确:/Volume/home/admin/…。 确保 FireSIGHT 管理中心和 ISE pxGrid 节点之间的时间同步。 FireSIGHT、ISE pxGrid 节点和终端全都应可解析 DNS

FireSiGHT 管理中心未与 ISE 进行通信

解决方法: FireSIGHT、ISE pxGrid 节点和终端全都应可解析 DNS 确保 FireSIGHT 管理中心、传感器和 ISE pxGrid 节点之间的时间同步。 重新启动 FireSIGHT 管理中心

在 FireSIGHT 管理中心内未出现关联事件

解决方法:确保 FireSIGHT 管理中心、传感器和 ISE pxGrid 节点之间的时间同步

FireSIGHT 尝试缓解失败

解决方法:确保 FireSIGHT 管理中心、传感器和 ISE pxGrid 节点之间的时间同步。 重新启动 FireSIGHT 管理中心

缓解"查询失败"尝试

解决方法:确保设备的 IP 地址已通过 ISE 进行身份验证。已为源配置补救类型。
从 FireSIGHT 管理控制台发出表明 pxGrid 尝试连接失败的系统日志错误消息

解决方法:通过在 FireSIGHT 管理控制台 CLI 上运行以下命令来确保 ISE pem 文件包含证书

```
openssl x509 -noout -text -in isel4lab.pem
```

pem 文件应包含证书

```
Certificate:
   Data:
        Version: 3 (0x2)
        Serial Number:
           56:19:bf:90:00:00:00:ab:b7:4f:a0:57:21:a0:03
   Signature Algorithm: shalWithRSAEncryption
        Issuer: CN=ise14.lab8.com
       Validity
           Not Before: Oct 11 01:46:56 2015 GMT
           Not After : Oct 10 01:46:56 2016 GMT
       Subject: CN=ise14.lab8.com
        Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
               Modulus:
                    00:a3:9e:b5:4e:68:e7:f9:db:4b:c6:3f:f4:f9:12:
                    e8:6f:ba:05:4d:b6:0b:13:fc:3c:35:61:ed:d6:d1:
                    Od:65:f4:e5:38:3d:5a:55:ac:94:e6:34:57:44:30:
                    64:75:9c:35:6f:f2:9c:0a:d6:f4:86:9d:94:10:2f:
                    b6:eb:ba:76:e2:33:84:77:70:20:71:a0:23:21:4b:
                    af:cc:6a:d9:c2:ba:9a:9c:eb:27:e6:b3:64:a7:e5:
                    29:31:65:03:23:06:d8:39:b9:74:48:32:75:de:6a:
                    5c:71:6a:27:8e:e6:d3:58:d0:44:e6:52:ec:3f:d8:
                    38:5b:d2:fc:c2:d6:90:02:e8:5a:9f:a7:a2:dc:44:
                    81:31:fc:5e:fd:60:41:40:e6:57:09:9b:d6:11:0e:
                    a6:93:1b:b0:c1:c5:9b:c4:98:45:af:78:1b:9c:55:
                    02:d3:e5:91:48:8b:1c:77:46:e6:49:d5:f0:5f:4c:
                    51:6c:d0:9b:82:25:b3:32:3b:ab:64:32:49:e5:b7:
                    45:db:9e:2c:c4:87:dc:d1:ff:9c:f8:99:d7:88:be:
                    c6:9d:7c:c6:ea:74:bd:b0:c5:a2:b5:a4:d4:fd:04:
                    64:61:db:c5:cb:07:69:d3:c7:72:8f:17:a7:2e:04:
                    11:d5:58:0d:00:aa:26:3a:5f:c3:08:2c:dc:a0:26:
                    e8:87
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints:
                CA:TRUE
           X509v3 Key Usage:
                Digital Signature, Key Encipherment, Key Agreement, Certificate Sign
           X509v3 Subject Key Identifier:
                8E:C0:5C:25:3A:5C:4E:9F:C4:6F:66:41:33:C3:6A:27:4C:00:A1:17
            X509v3 Extended Key Usage:
               TLS Web Server Authentication, TLS Web Client Authentication
           Netscape Cert Type:
                SSL Server
   Signature Algorithm: sha1WithRSAEncryption
        40:cc:1b:4d:94:94:d9:68:7b:95:6e:36:e4:3a:41:41:6c:f1:
        4e:f0:1a:fa:3e:42:7e:b0:73:80:ad:0f:4a:bb:d4:ce:cd:da:
        ef:32:f9:d0:58:f0:c4:90:0c:97:20:88:26:f5:9c:96:d7:61:
        fe:05:09:40:0a:f6:33:04:dc:30:ec:10:d2:82:f2:ec:5d:f9:
        b2:d1:69:5e:ed:ae:a5:b4:6d:b1:c4:16:bf:67:14:e9:ec:4f:
        9c:83:07:35:64:26:9d:e4:41:bb:65:5e:77:7b:e5:da:d1:98:
        9c:c0:50:fc:ba:a4:dc:51:c4:e5:49:28:55:9f:40:0c:61:20:
        1d:49:e3:ca:a5:a2:35:74:5c:57:71:17:32:71:2c:2b:51:2c:
        cf:49:30:9e:31:28:19:4a:62:1b:4a:86:21:0d:54:73:b8:86:
         92:df:8c:ae:3d:92:91:5f:70:d5:17:4c:14:07:d1:0c:59:0b:
        3d:6d:6a:16:ca:a9:3a:06:b8:37:f1:28:af:c5:03:32:30:82:
```



```
3d:53:8b:77:ed:e7:8a:5a:38:b6:3b:0e:c0:93:63:c1:f6:2e:
a3:ce:33:a4:0a:82:d4:f7:8f:0f:c2:99:9e:96:36:c5:89:a2:
9f:f3:66:01:12:da:13:53:d4:92:ef:17:9e:2b:26:4b:3c:7d:
1f:6f:a3:b4
```

如果您没有看到上述内容,请导出 ISE 身份自签名公钥/私钥对,提供密码,将 ISE 身份自签名证书添加到 FMC 受信任 CA 库。

通过将自签名证书导入到 ISE 系统库中进行验证

解决方法:这未必是一个问题,不过,可以将供应商的公钥/私钥对导入到 ISE 受信任系统库中。这是由于从 pxGrid SDK 使用 ISE 样本证书所导致,这些证书应仅用于测试,不建议用于生产。请使用**配置自签名证书的** FireSIGHT 管理中心中的步骤来配置自签名证书。

第1步:将 FireSIGHT 内部 CA 公钥/私钥对导入到 ISE 证书系统库中。将需要私钥密码。
 管理 (Administration)->系统 (System)->证书 (Certificates)->系统证书 (System Certificates),并导入
 FireSIGHT 内部公钥/私钥对。输入私钥密码

cisco Identity Services	Engine	A Home	Operations V Policy	▼ Guest Access ▼	Administration	warning AL isez+ aumin
🔆 System 🛛 👰 Identity	Management	Network Resources	evice Portal Management	D pxGrid Services	Reed Service	≗¦≝ pxGrid Identity Mapping
Deployment Licensing	Certificates	Logging Maintenance	Backup & Restore	Admin Access Set	tings	
Certificate Management		Import Server Certificate				
Overview						
System Certificates		* Select No	ode ise14	<u> </u>		
Endpoint Certificates		* Certificate F	File Browse fmc2.ce	r		
Enupoint Certificates		* Private Key F	File Browse fmc2.ke	У		
Trusted Certificates		Passwo	ord			
OCSP Client Profile		Friendly Na	me			
Certificate Signing Requests		Allow Wildcard Certifica	Allow wildcard is on the pyGrid is not support wildcard is not support wildcard is not sure pyGrid is not support support sure pyGrid is not support support sure pyGrid is not support	disabled when pxGrid is sele ard certificates. If you want checked.	ected and vice versa. This to use wildcard with othe	is because pxGrid does er usage type(s), make
Certificate Authority		Validate Certificate Extensio	ons 🗌 🛈			
Internal CA Settings		Usa	ge			
Certificate Templates			Admin: Use certif	icate to authenticate the IS	E Admin Portal	
External CA Settings			EAP Authentication	n: Use certificate for EAP p icate for the pxGrid Control	rotocols that use SSL/TLS	tunneling
			Portal: Use for po	rtal		
				_		

- **第2步:**为证书"用途"选择->pxGrid,然后提交(Submit)
- 第3步: 您应该看到以下内容:

安全访问操作指南



uluulu cisco Identity Services Engine								License Warning A ise1	4 admin Logout Feedback	Ω		
			🟠 Home	Operations •	Policy •	Guest Access	 Administrati 	ion 🔻		Setu	up Assistant 🕶	
🙀 System 🛛 💆 I	dentity Management	Network R	tesources 🛃	Device Portal Mana	gement	👼 pxGrid Servi	ces 🔂 Feed	Service	entity Mapping		k	
Deployment Lice	ensing Certificates	Logging	Maintenance	Backup & Res	tore Adn	nin Access	Settings					
Certificate Managen	ent	System Certificates A For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.										
Overview System Certificates		/ Edit	Generate Self Si	gned Certificate	🕂 Import	Export	K Delete 🔎 V	fiew				
		Friendly	/ Name	Used By	Portal group	o tag	Issued To	Issued By	Valid From	Expiration Date	е	
		▼ ise14										
Endpoint Certificates		Default ertificat	self-signed server c	Admin, Portal, EAP Authentication	Default Port Group (i)	al Certificate	ise14.lab7.com	ise14.lab7.com	Sat, 22 Aug 2015	Sun, 21 Aug 20	016 🔽	
Trusted Certificates		G sd.lab7. 00001	.com#sd.lab7.com#	pxGrid			sd.lab7.com	sd.lab7.com	Mon, 31 Aug 2015	Wed, 30 Sep 20	015	



解决方案警告

pxGrid 和身份映射服务重新启动

说明:只要从 ISE 部署的信任库导入/删除证书,pxGrid 和身份映射服务就会在 ISE pxGrid 节点上重新启动

<u>提交的缺陷</u>: CSCuv43145

解决方法:无需任何操作,因为将自动重新启动服务,但在服务处于重新启动状态时,将不处理新的隔离 事件。

解析计划: ISE Carlsbad 2016 年春季版本

主动 pxGrid 节点未反映在 GUI 中; 它反映在 CLI 中

<u>说明</u>:当 pxGrid HA 部署中提供两个 pxGrid 节点时,一个处于主动状态,另一个处于待机状态。识别哪个节 点处于主动状态,并且管理员需要在 CLI 中审查 pxGrid 状态。状态在 UI 部署页面中不可视。将在 Carlsbad 中进行此添加。

解决方法:使用 CLI 确定主动/被动状态

解析计划: ISE Carlsbad 2016 年春季版本

参考

在分布式 ISE 环境中配置 pxGrid: <u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-</u> <u>Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf</u>

如何使用思科 pxGrid 部署证书: 配置 CA 签名的 ISE pxGrid 节点和 CA 签名的 pxGrid 客户端: <u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-</u> CA signed pxGridISEnode CAsigned pxGridclient.pdf

如何使用思科 pxGrid 部署证书: ISE pxGrid 节点和 pxGrid 客户端的自签名证书: <u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-</u><u>Self_signed_pxGridClient_selfsigned_pxGrid.pdf</u>