Cisco FireSIGHT 和 ISE 快速威胁控制解决方案

目录

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

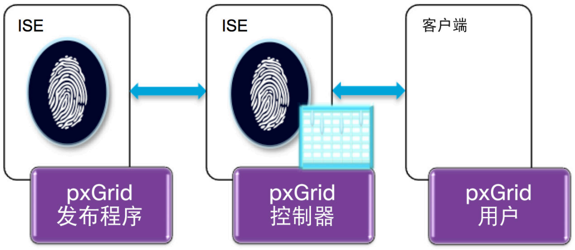
思科的平台交换网格 (pxGrid) 在 IT 基础设施中启用多供应商、跨平台网络系统协作。它允许例如安全监控和检测系统、网络策略平台、资产和配置管理、身份和访问管理平台以及几乎任何其他 IT 操作平台。pxGrid 使用身份服务引擎 (ISE) 策略服务器提供身份验证、授权和访问控制 (AAA)。

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

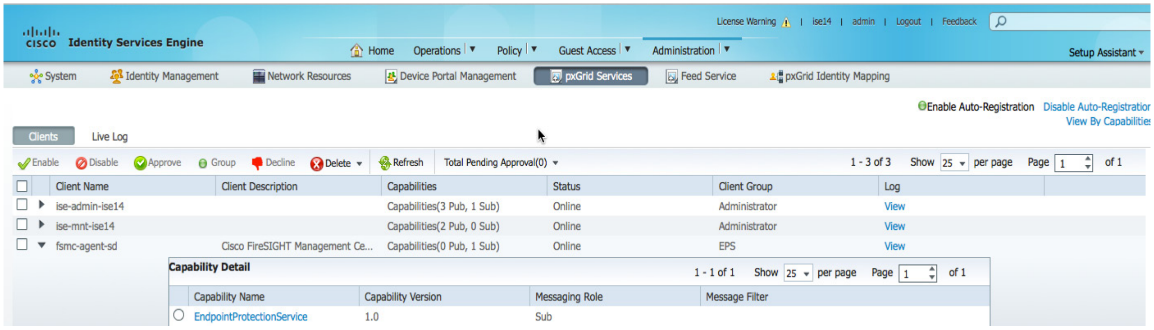
取消隔离

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。



□		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 Management Ce...	Capabilities(0 Pub, 1 Sub)	Online	EPS	View

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	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。

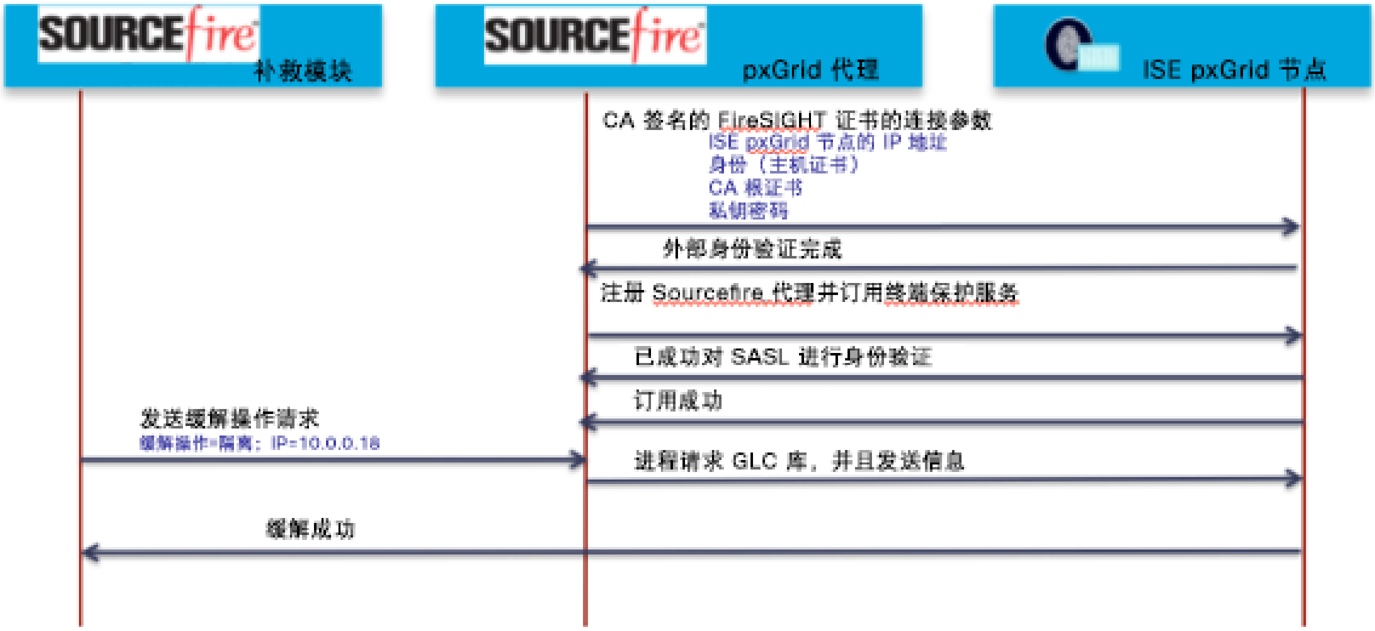
pxGrid 代理安装有三个作用：

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



SOURCEfire 补救模块

SOURCEfire pxGrid 代理

ISE pxGrid 节点

CA 签名的 FireSIGHT 证书的连接参数

ISE pxGrid 节点的 IP 地址

身份（主机证书）

CA 根证书

私钥密码

外部身份验证完成

注册 Sourcefire 代理并订用终端保护服务

已成功对 SASL 进行身份验证

订用成功

发送缓解操作请求

缓解操作=隔离：IP=10.0.0.18

进程请求 GLC 库，并且发送信息

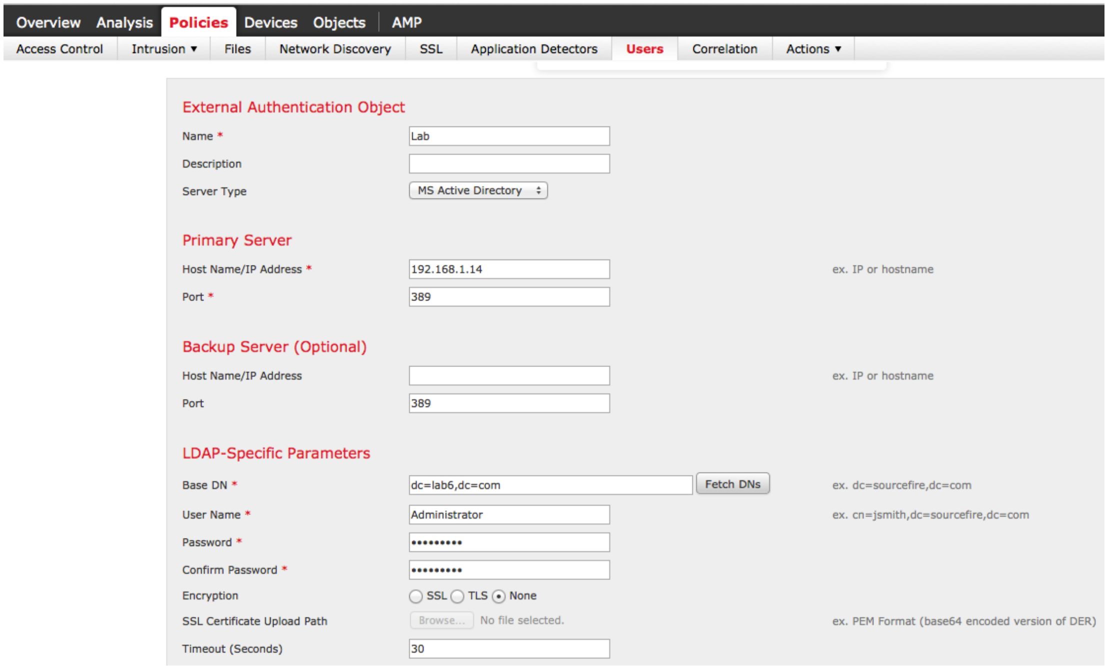
缓解成功

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：



External Authentication Object

Name *	Lab	
Description		
Server Type	MS Active Directory	

Primary Server

Host Name/IP Address *	192.168.1.14	ex. IP or hostname
Port *	389	

Backup Server (Optional)

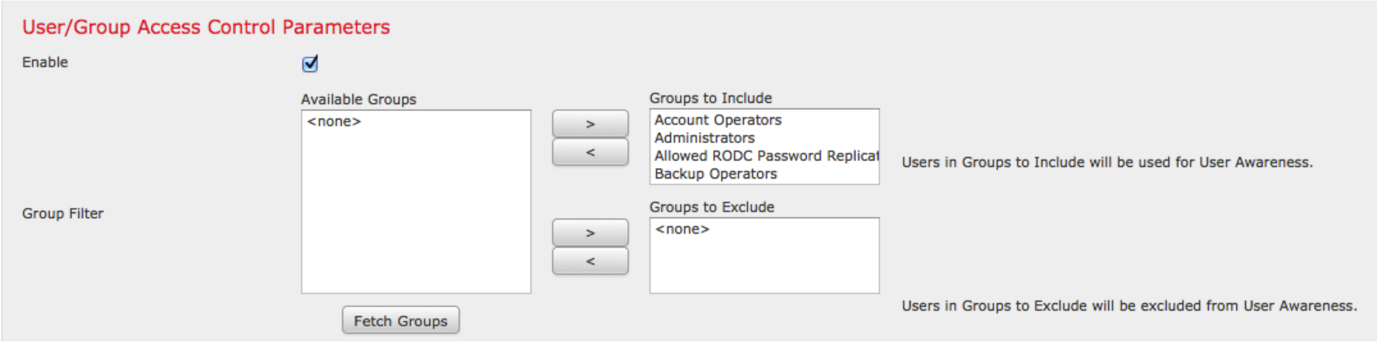
Host Name/IP Address		ex. IP or hostname
Port	389	

LDAP-Specific Parameters

Base DN *	dc=lab6,dc=com	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	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)

注意：请为“用户感知”(User Awareness) 包含所有组



User/Group Access Control Parameters

Enable ☑

Group Filter

Available Groups
<none>

Groups to Include
Account Operators
Administrators
Allowed RODC Password Replicat
Backup Operators

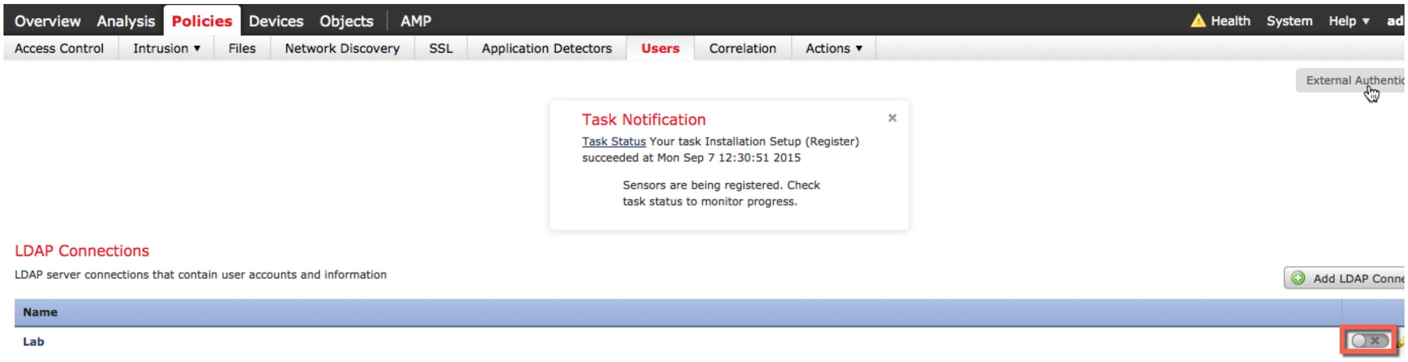
Users in Groups to Include will be used for User Awareness.

Groups to Exclude
<none>

Users in Groups to Exclude will be excluded from User Awareness.

第 3 步： 测试和保存

第 4 步： 激活 LDAP 连接，**点击->以下按钮**



Task Notification ×

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

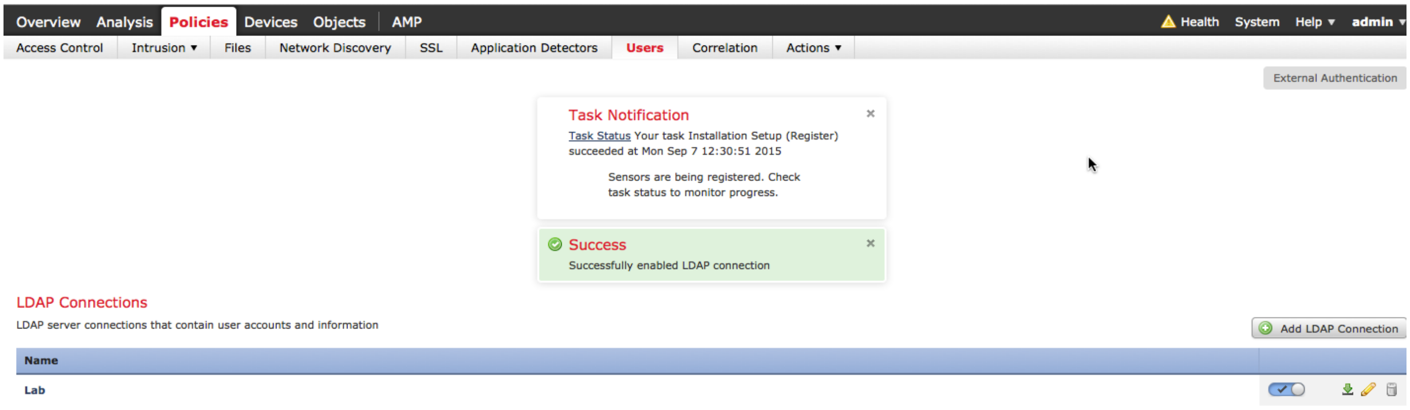
Sensors are being registered. Check task status to monitor progress.

LDAP Connections

LDAP server connections that contain user accounts and information

Name
Lab

第 5 步： 您应该看到以下内容：



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 ×

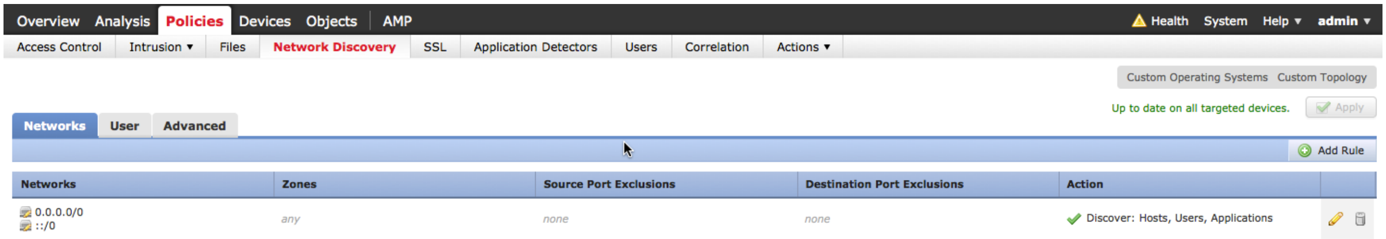
Successfully enabled LDAP connection

LDAP Connections

LDAP server connections that contain user accounts and information

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)**

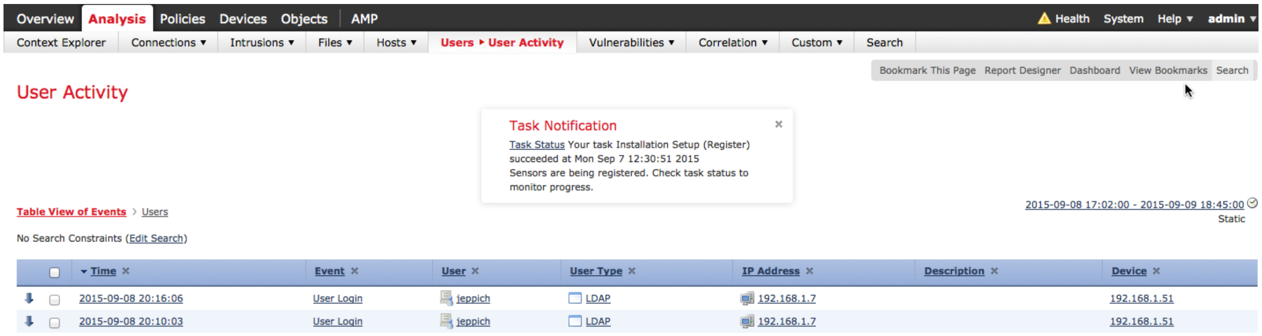


Up to date on all targeted devices.

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Hosts, Users, Applications

用户 LDAP 信息样本

“用户活动” (User Activity) 屏幕显示最终用户信息



User Activity

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.

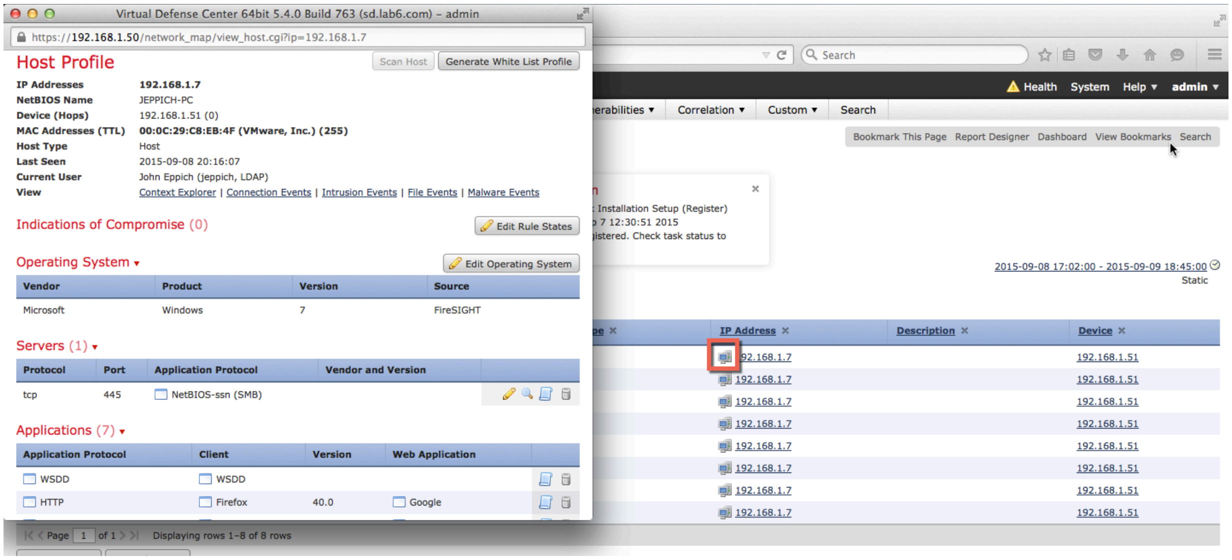
Table View of Events › Users

2015-09-08 17:02:00 - 2015-09-09 18:45:00
Static

No Search Constraints (Edit Search)

	Time	Event	User	User Type	IP Address	Description	Device
☐	2015-09-08 20:16:06	User Login	jeppich	LDAP	192.168.1.7		192.168.1.51
☐	2015-09-08 20:10:03	User Login	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”



Host Profile

IP Addresses	192.168.1.7
NetBIOS Name	JEPPICH-PC
Device (Hops)	192.168.1.51 (0)
MAC Addresses (TTL)	00:0C:29:C8:EB:4F (VMware, Inc.) (255)
Host Type	Host
Last Seen	2015-09-08 20:16:07
Current User	John Eppich (jeppich, LDAP)
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (0)

Operating System ▾

Vendor	Product	Version	Source
Microsoft	Windows	7	FireSIGHT

Servers (1) ▾

Protocol	Port	Application Protocol	Vendor and Version
tcp	445	NetBIOS-ssn (SMB)	

Applications (7) ▾

Application Protocol	Client	Version	Web Application
WSDD	WSDD		
HTTP	Firefox	40.0	Google

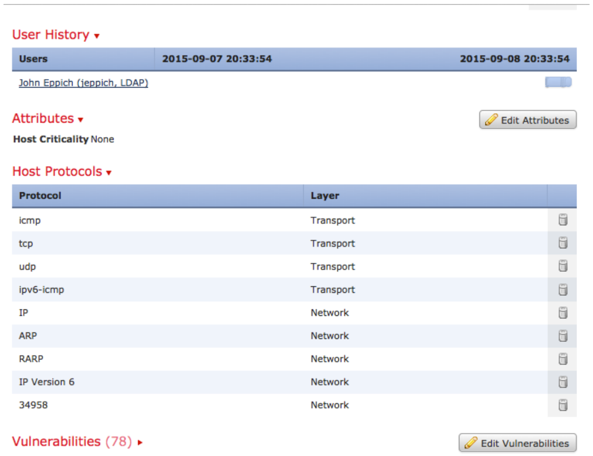
Installation Setup (Register)
7 12:30:51 2015
istered. Check task status to

2015-09-08 17:02:00 - 2015-09-09 18:45:00
Static

IP Address	Description	Device
92.168.1.7		192.168.1.51
192.168.1.7		192.168.1.51
192.168.1.7		192.168.1.51
192.168.1.7		192.168.1.51
192.168.1.7		192.168.1.51
192.168.1.7		192.168.1.51
192.168.1.7		192.168.1.51
192.168.1.7		192.168.1.51

Page 1 of 1 Displaying rows 1–8 of 8 rows

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。



User History ▾

Users	2015-09-07 20:33:54	2015-09-08 20:33:54
John Eppich (jeppich, LDAP)		

Attributes ▾

Host Criticality None

Host Protocols ▾

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
ipv6-icmp	Transport
IP	Network
ARP	Network
RARP	Network
IP Version 6	Network
34958	Network

Vulnerabilities (78) ▸

在使用 pxGrid 的独立环境中配置自签名证书的 ISE

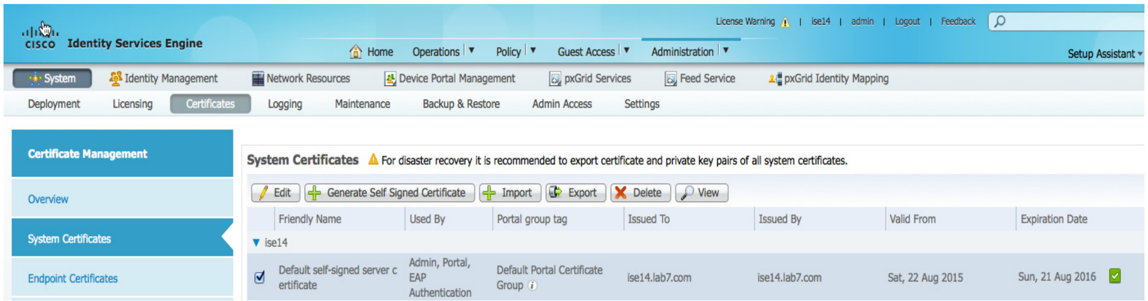
本节分步说明在使用 pxGrid 的独立环境中使用自签名证书配置 ISE 的过程。

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。

注意：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**

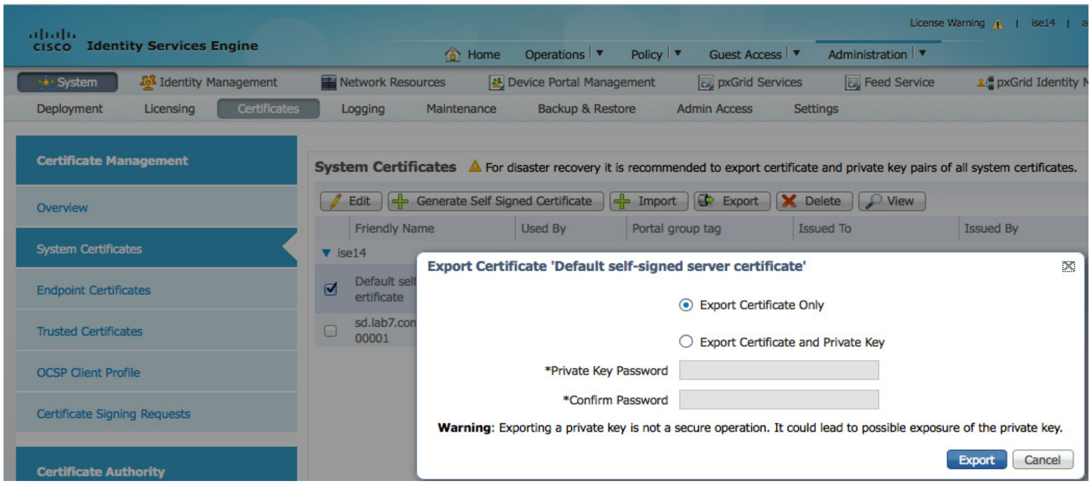


cisco Identity Services Engine
License Warning | ise14 | admin | Logout | Feedback
Home | Operations | Policy | Guest Access | Administration
Setup Assistant
System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | pxGrid Identity Mapping
Deployment | Licensing | Certificates | Logging | Maintenance | Backup & Restore | Admin Access | Settings
Certificate Management
Overview
System Certificates
Endpoint Certificates
Edit | Generate Self Signed Certificate | Import | Export | Delete | View

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
▼ ise14							
☑	Default self-signed server certificate	Admin, Portal, EAP Authentication	Default Portal Certificate Group ⓘ	ise14.lab7.com	ise14.lab7.com	Sat, 22 Aug 2015	Sun, 21 Aug 2016 ✓

第 2 步： 仅导出证书，**点击->导出 (Export)**



cisco Identity Services Engine
License Warning | ise14 |
Home | Operations | Policy | Guest Access | Administration
System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | pxGrid Identity M
Deployment | Licensing | Certificates | Logging | Maintenance | Backup & Restore | Admin Access | Settings
Certificate Management
Overview
System Certificates
Endpoint Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Authority
Edit | Generate Self Signed Certificate | Import | Export | Delete | View
Friendly Name | Used By | Portal group tag | Issued To | Issued By
ise14
Default sel certificate
sd.lab7.con 00001

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Export Certificate 'Default self-signed server certificate'

● Export Certificate Only

○ Export Certificate and Private Key

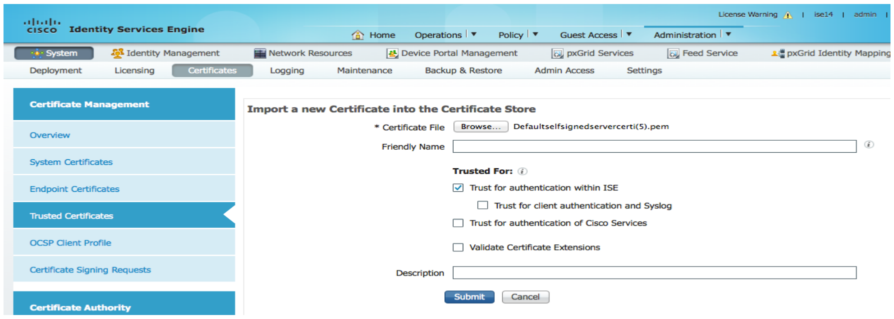
*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

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)



Import a new Certificate into the Certificate Store

* Certificate File Browse... Defaultselfsignedservercerti(5).pem

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

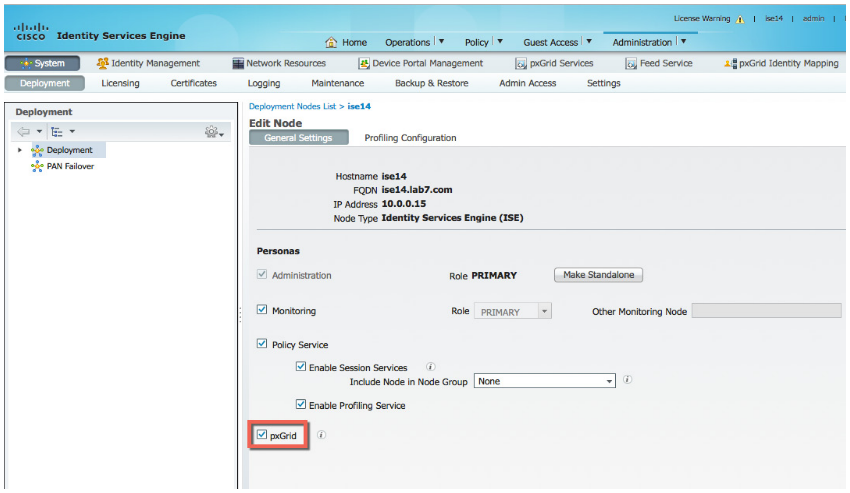
☐ Validate Certificate Extensions

Description

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)



Edit Node

Hostname **ise14**

FQDN **ise14.lab7.com**

IP Address **10.0.0.15**

Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration Role **PRIMARY**

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

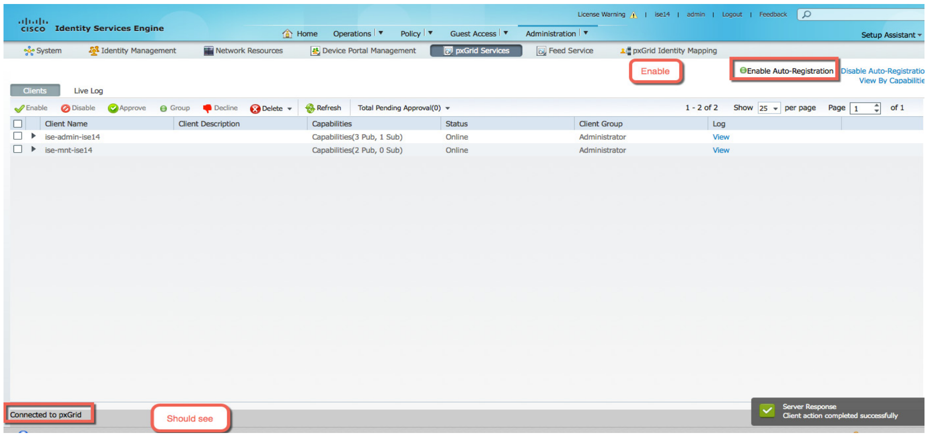
☑ Enable Profiling Service

☑ pxGrid

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)

注意：这可能需要几秒钟时间才能连接



1 - 2 of 2 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

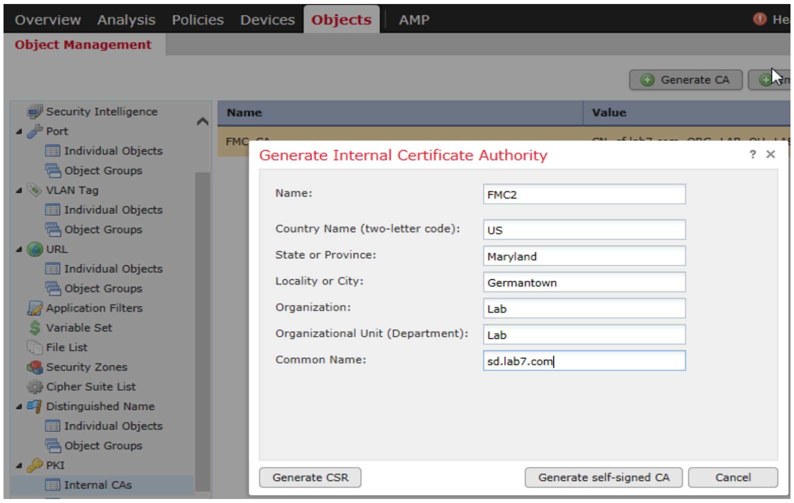
Connected to pxGrid

Server Response
Client action completed successfully

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。

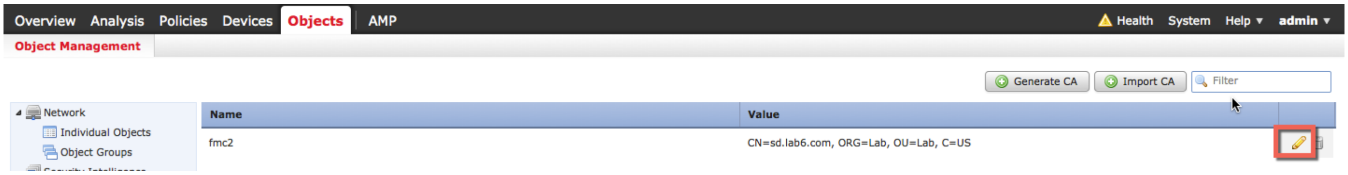
第 1 步： **选择->对象 (Objects) > 对象管理 (Object Management) > PKI -> 内部 CA (Internal CAs) ->生成 CA (Generate CA)->** 提供以下认证信息：
在本例中，FMC2 是指定给内部 CA 的名称



Generate Internal Certificate Authority

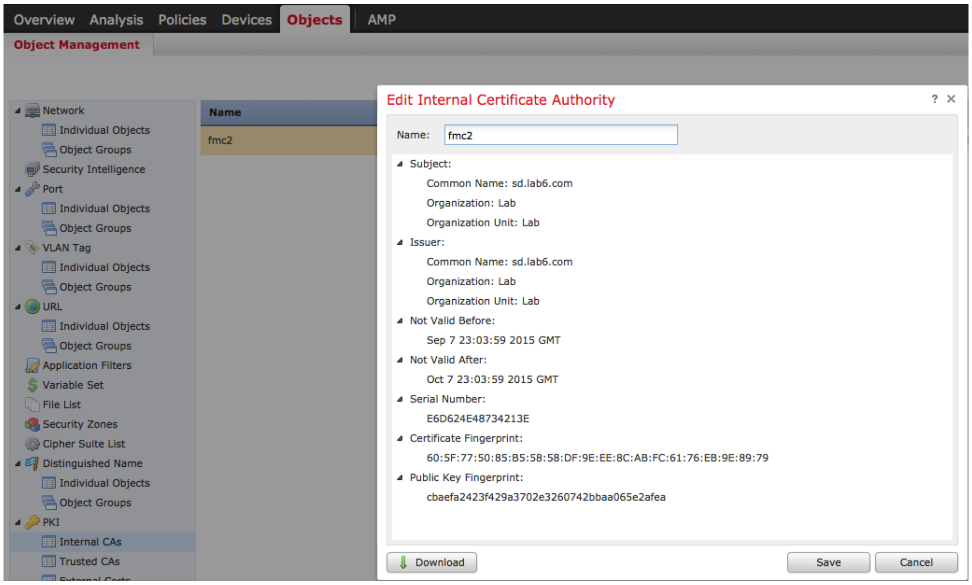
Name: FMC2
Country Name (two-letter code): US
State or Province: Maryland
Locality or City: Germantown
Organization: Lab
Organizational Unit (Department): Lab
Common Name: sd.lab7.com

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：**



Name	Value
fmc2	CN=sd.lab6.com, ORG=Lab, OU=Lab, C=US

第 4 步： 选择下载 (Download)



Edit Internal Certificate Authority

Name: fmc2

Subject:
Common Name: sd.lab6.com
Organization: Lab
Organization Unit: Lab

Issuer:
Common Name: sd.lab6.com
Organization: Lab
Organization Unit: Lab

Not Valid Before:
Sep 7 23:03:59 2015 GMT

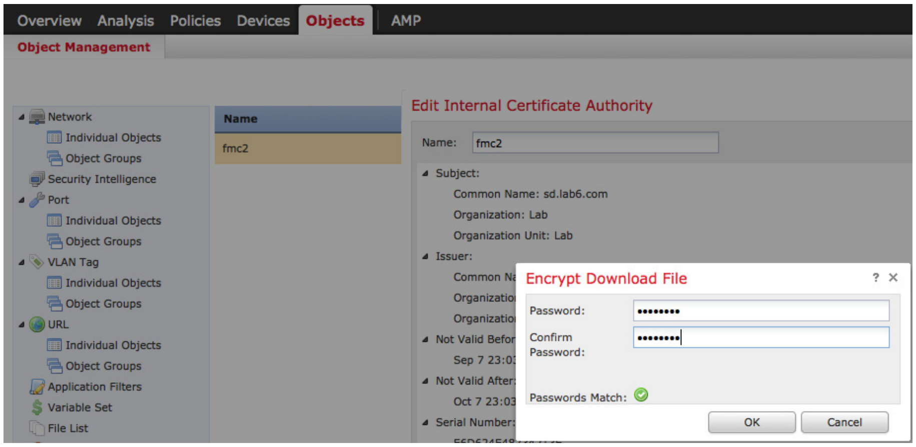
Not Valid After:
Oct 7 23:03:59 2015 GMT

Serial Number:
E6D624E48734213E

Certificate Fingerprint:
60:5F:77:50:85:B5:58:58:DF:9E:EE:8C:AB:FC:61:76:EB:9E:89:79

Public Key Fingerprint:
cbaefa2423f429a3702e3260742bbaa065e2afea

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



Edit Internal Certificate Authority

Name: fmc2

Subject:
Common Name: sd.lab6.com
Organization: Lab
Organization Unit: Lab

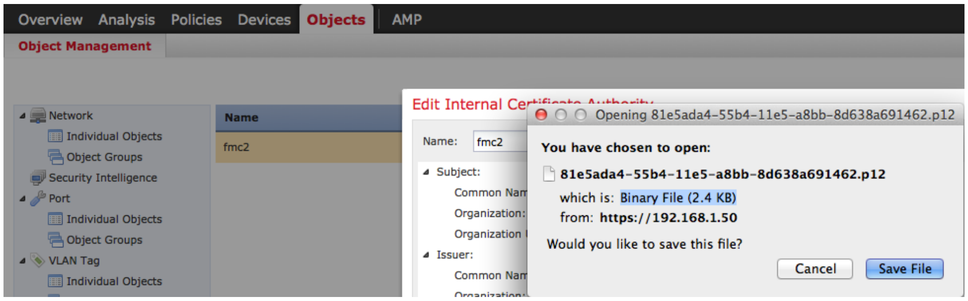
Encrypt Download File

Password: ••••••••

Confirm Password: ••••••••

Passwords Match: ✓

第 6 步： 在本地保存 .p12 文件



Opening 81e5ada4-55b4-11e5-a8bb-8d638a691462.p12

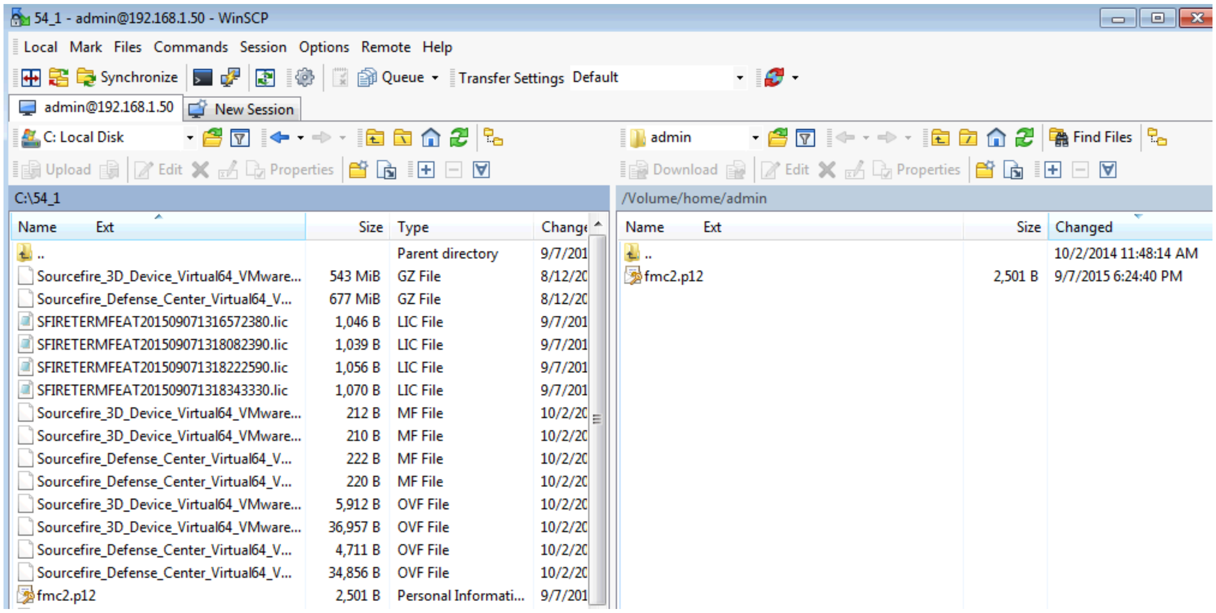
You have chosen to open:

81e5ada4-55b4-11e5-a8bb-8d638a691462.p12
which is: Binary File (2.4 KB)
from: https://192.168.1.50

Would you like to save this 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



54_1 - admin@192.168.1.50 - WinSCP

C:\54_1

Name Ext	Size	Type	Change
..		Parent directory	9/7/201
Sourcefire_3D_Device_Virtual64_VMware...	543 MiB	GZ File	8/12/20
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
fmc2.p12	2,501 B	Personal Informati...	9/7/201

/Volume/home/admin

Name Ext	Size	Changed
..		10/2/2014 11:48:14 AM
fmc2.p12	2,501 B	9/7/2015 6:24:40 PM

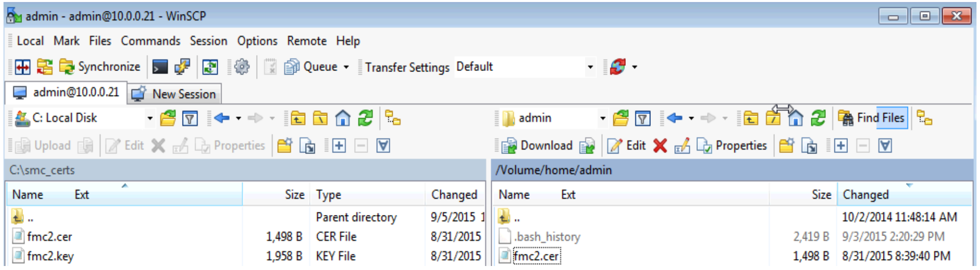
第 9 步： 通过 SSH 传输到 FireSIGHT 管理控制台

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@10.0.0.21 - WinSCP

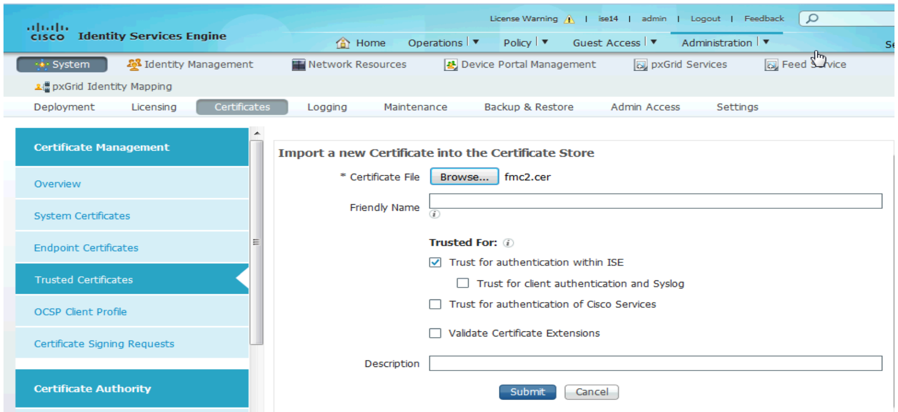
C:\smc_certs

Name Ext	Size	Type	Changed
..		Parent directory	9/5/2015 1
fmc2.cer	1,498 B	CER File	8/31/2015
fmc2.key	1,958 B	KEY File	8/31/2015

/Volume/home/admin

Name Ext	Size	Changed
..		10/2/2014 11:48:14 AM
.bash_history	2,419 B	9/3/2015 2:20:29 PM
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**


Identity Services Engine
License Warning | ise14 | admin | Logout | Feedback
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
Overview
System Certificates
Endpoint Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Authority

Import a new Certificate into the Certificate Store

* Certificate File Browse... fmc2.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

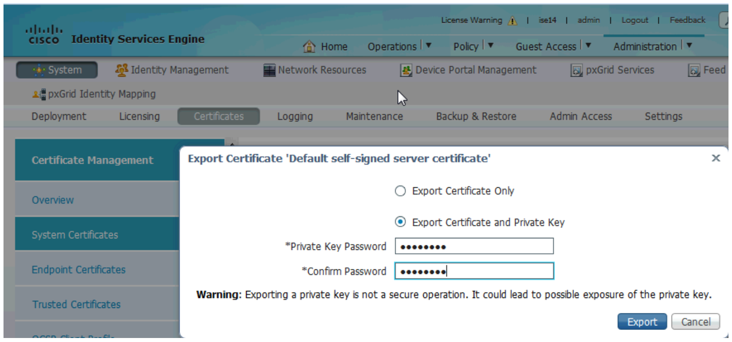
Description

Submit Cancel

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


Identity Services Engine
License Warning | ise14 | admin | Logout | Feedback
Home Operations ▼ Policy ▼ Guest Access ▼ Administration ▼
System Identity Management Network Resources Device Portal Management pxGrid Services Feed
pxGrid Identity Mapping
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management
Overview
System Certificates
Endpoint Certificates
Trusted Certificates

Export Certificate 'Default self-signed server certificate'

○ Export Certificate Only

● Export Certificate and Private Key

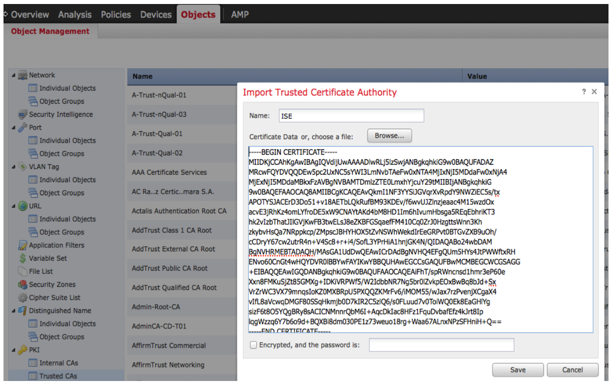
*Private Key Password ••••••••

*Confirm Password ••••••••

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

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)。



Import Trusted Certificate Authority

Name: ISE

Certificate Data or, choose a file: Browse...

```
-----BEGIN CERTIFICATE-----
MIIDKjCCAhKgAwIBAgIQVdijUwAAAADlwRLj5lzSwjANBgkqhkiG9w0BAQUFADAZ
MRcwFQYDVQQDEw5pc2UxNC5sYWI3LmNvbTAeFw0xNTA4MjIxNjI5MDdaFw0xNjA4
MjExNjI5MDdaMBkxFzAVBgNVBAMTDmlzZTE0LmxhYjcuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvQkmI1NF3YYSiJGVqrXvRpdY9NWZiEC5s/tx
APOTYSJACErD3Do51+v18AETbLQkRufBM93KDEv/f6wvUJZlnzjeaac4M15wzdOx
acvE3jRhKz4omLYfroDE5xW9CNAYtAKd4bM8HD1Im6hIvumHbsga5REqEbhriKT3
hk2vIzbThatJIIGVjKwFB3twELsJ8eZKBFGSqaefFM410Cq0ZrJ0HzgttsWnn3Kh
zkybvHsQa7NRppkcp/ZMpscJBHYHOX5tZvNSWhWekdIrEeGRPvt0BTGvZXB9uOh/
cCDryY67cw2utrR4n+V4Sc8+r+i4/SofL3YPrHiA1hnjGK4N/QIDAQABo24wbDAM
BgNVHRMEBTADAQH/MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUm5HYs4JtPWWftxRH
ENvo60CnGt4wHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEGCWCGSAGG
+EIBAQQEAwIGQDANBgkqhkiG9w0BAQUFAAOCAQEAiFhT/spRWncnsd1hmr3eP60e
Xxn8FMKuSjZt85GMXg+IDKiVRPWf5/W2IdbbNR7Ng5br0lZvkpEOxBwBq8bJd+Sx
VrZrWC3VX79mnqsIoKZ0MXBRpU5PXQQZKMrFv6/iMOM55/wJax7rzPvenjXCgaX4
vIfL8aVcwqDMGF80SSqHkmjb0D7kIR2C5zlQ6/s0FLuud7v0ToiWQ0Ek8EaGHlYg
sizF6t8O5YQgBRy8sACICNMnnrQbM6I+AqcDkIac8HFz1FquDvbafEfz4kJrt8Ip
lqgWzzq6Y7b6o9d+BQXBi8dm030PE1z73weuo18rg+Waa67ALnxNPzSFHniH+Q==
-----END CERTIFICATE-----
```

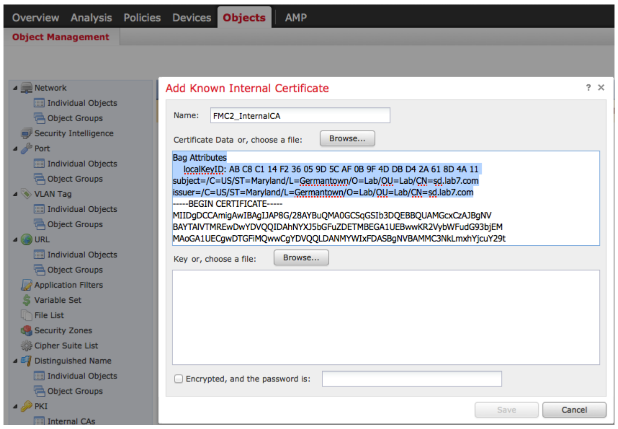
□ Encrypted, and the password is:

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



Name: FMC2_InternalCA

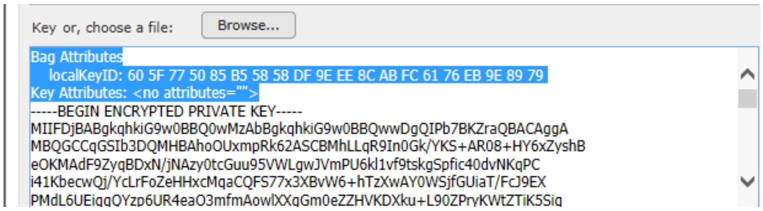
Certificate Data or, choose a file:

```
Bag Attributes
    localKeyID: AB C8 C1 14 F2 36 05 9D 5C AF 0B 9F 4D DB D4 2A 61 8D 4A 11
subject=/C=US/ST=Maryland/L=Germantown/O=Lab/OU=Lab/CN=sd.lab7.com
issuer=/C=US/ST=Maryland/L=Germantown/O=Lab/OU=Lab/CN=sd.lab7.com
-----BEGIN CERTIFICATE-----
MIIDgDCCAmigAwIBAgIJAP8G/28AYBuQMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVTMREwDwYDVQQIDAhNYXJ5bGFuZDETMBEGA1UEBwwKR2VybWFudG93bjEM
MAoGA1UECgwDTGFiMQwwCgYDVQQLDANMYWIxFDASBgNVBAMMC3NkLmxhYjcuY29t
```

Key or, choose a file:

☐ Encrypted, and the password is:

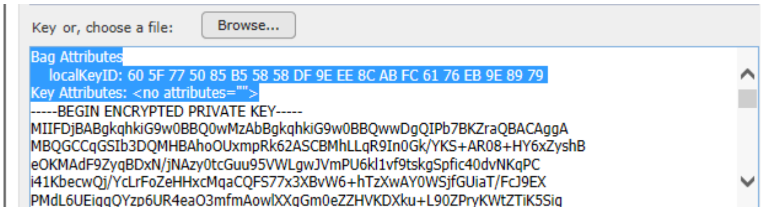
第 17 步： 请删除密钥文件的袋属性，直至您正好位于“---Begin…”之前。



Key or, choose a file:

```
Bag Attributes
    localKeyID: 60 5F 77 50 85 B5 58 58 DF 9E EE 8C AB FC 61 76 EB 9E 89 79
Key Attributes: <no attributes="">
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIPb7BKZraQBACAggA
MBQGCCqGSIb3DQMHBAhoOUxmpRk62ASCBMhLLqR9In0Gk/YKS+AR08+HY6xZyshB
eOKMAdF9ZyqBDxN/jNAzy0tcGuu95VWLgwJVmPU6kl1vf9tskgSpfic40dvNKqPC
i41KbecwQj/YcLrFoZeHHxcMqaCQFS77x3XBvW6+hTzXwAY0WSjfGUiaT/FcJ9EX
PMdL6UEiqqQYzp6UR4eaO3mfmAowlXXqGm0eZZHVKDXku+L90ZPryKWtZTiK5Siq
```

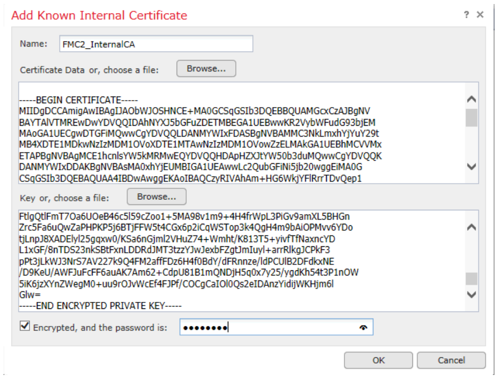
第 18 步： 另请删除 </no> 并输入加密密码



Key or, choose a file:

```
Bag Attributes
    localKeyID: 60 5F 77 50 85 B5 58 58 DF 9E EE 8C AB FC 61 76 EB 9E 89 79
Key Attributes: <no attributes="">
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIPb7BKZraQBACAggA
MBQGCCqGSIb3DQMHBAhoOUxmpRk62ASCBMhLLqR9In0Gk/YKS+AR08+HY6xZyshB
eOKMAdF9ZyqBDxN/jNAzy0tcGuu95VWLgwJVmPU6kl1vf9tskgSpfic40dvNKqPC
i41KbecwQj/YcLrFoZeHHxcMqaCQFS77x3XBvW6+hTzXwAY0WSjfGUiaT/FcJ9EX
PMdL6UEiqqQYzp6UR4eaO3mfmAowlXXqGm0eZZHVKDXku+L90ZPryKWtZTiK5Siq
```

第 19 步： 您应看到以下内容，点击“确定”(OK) 以完成



Name: FMC2_InternalCA

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDgDCCAmigAwIBAgIJAObWJOSHNCE+MA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVTMREwDwYDVQQIDAhNYXJ5bGFuZDETMBEGA1UEBwwKR2VybWFudG93bjEM
MAoGA1UECgwDTGFiMQwwCgYDVQQLDANMYWIxFDASBgNVBAMMC3NkLmxhYjYuY29t
MB4XDTE1MDkwNzIzMDM1OVoXDTE1MTAwNzIzMDM1OVowZzELMAkGA1UEBhMCVVMx
ETAPBgNVBAgMCE1hcnlsYW5kMRMwEQYDVQQHDApHZXJtYW50b3duMQwwCgYDVQQK
DANMYWIxDDAKBgNVBAsMA0xhYjEUMBIGA1UEAwwLc2QubGFiNi5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzyRIVAhAm+HG6WkjYFlRrrTDvQep1
```

Key or, choose a file:

```
FtlgQtlFmT7Oa6UOeB46c5l59cZoo1+5MA98v1m9+4H4frWpL3PiGv9amXL5BHGn
Zrc5Fa6uQwZaPHPKP5j6BTjFFW5t4CGx6p2iCqWSTop3k4QgH4m9bAiOPMvv6YDo
tjLnpJ8XADElyl25gqxw0/KSa6nGjml2VHuZ74+Wmht/K813T5+yivfTfNaxncYD
L1xGF/8nTDS23nkSBtFxnLDDRdJMT3tzzYJwJexbFZgtJmIuyl+arrRlkgJCPkF3
pPt3jLkWJ3NrS7AV227k9Q4FM2affFDz6H4f0BdY/dFRnnze/ldPCUlB2DFdkxNE
/D9KeU/AWFJuFcFF6auAK7Am62+CdpU81B1mQNDjH5q0x7y25/ygdKh54t3P1nOW
5iK6jzXYnZWegM0+uu9rOJvWcEf4FJPf/COCgCaIOl0Qs2eIDAnzYidijWKHjm6l
Glw=
-----END ENCRYPTED PRIVATE KEY-----
```

☑ Encrypted, and the password is: ••••••••

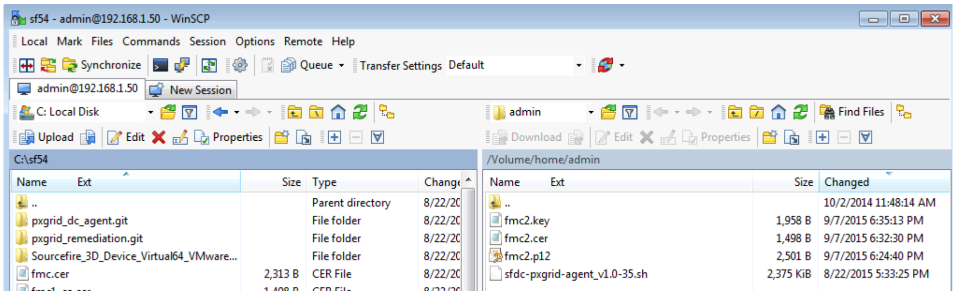
使用自签名证书配置 pxGrid 代理

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。



C:\sf54

Name	Ext	Size	Type	Change
..			Parent directory	8/22/20
pxgrid_dc_agent.git			File folder	8/22/20
pxgrid_remediation.git			File folder	8/22/20
Sourcefire_3D_Device_Virtual64_VMware...			File folder	8/22/20
fmc.cer		2,313 B	CER File	8/22/20

/Volume/home/admin

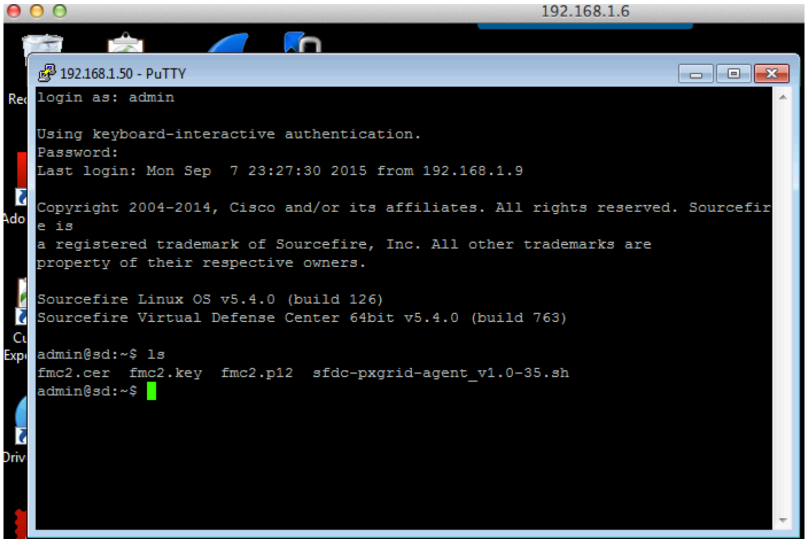
Name	Ext	Size	Changed
..			10/2/2014 11:48:14 AM
fmc2.key		1,958 B	9/7/2015 6:35:13 PM
fmc2.cer		1,498 B	9/7/2015 6:32:30 PM
fmc2.p12		2,501 B	9/7/2015 6:24:40 PM
sfdc-pxgrid-agent_v1.0-35.sh		2,375 KiB	8/22/2015 5:33:25 PM

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

注意：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
```

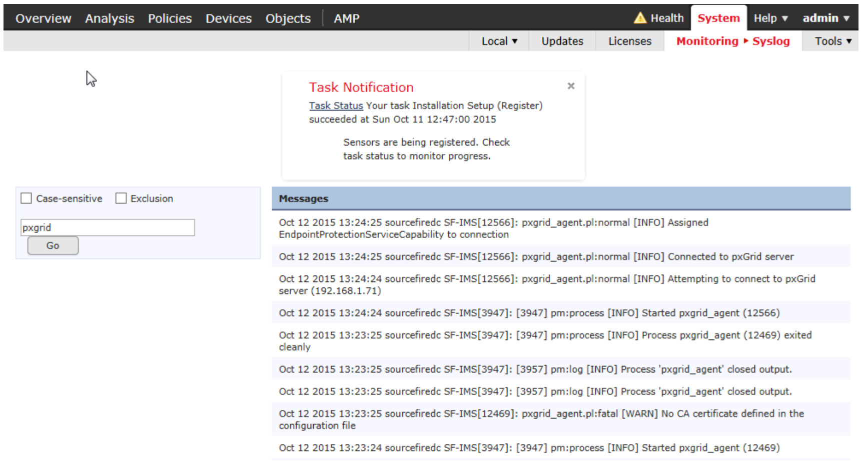


```
login as: admin

Using keyboard-interactive authentication.
Password:
Last login: Mon Sep  7 23:27:30 2015 from 192.168.1.9

Copyright 2004-2014, Cisco and/or its affiliates. All rights reserved. Sourcefir
e is
a registered trademark of Sourcefire, Inc. All other trademarks are
property of their respective owners.

Sourcefire Linux OS v5.4.0 (build 126)
Sourcefire Virtual Defense Center 64bit v5.4.0 (build 763)

admin@sd:~$ ls
fmc2.cer  fmc2.key  fmc2.p12  sfdc-pxgrid-agent_v1.0-35.sh
admin@sd:~$
```

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
> 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



Task Notification

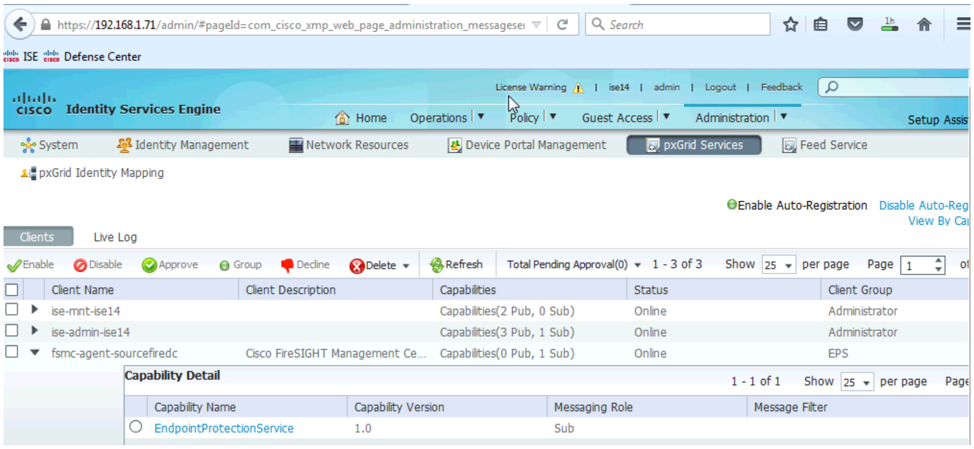
Task Status Your task Installation Setup (Register) succeeded at Sun Oct 11 12:47:00 2015

Sensors are being registered. Check task status to monitor progress.

Messages

```
Oct 12 2015 13:24:25 sourcefiredc SF-IMS[12566]: pxgrid_agent.pl:normal [INFO] Assigned
EndpointProtectionServiceCapability to connection
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 SF-IMS[12566]: pxgrid_agent.pl:normal [INFO] Attempting to connect to pxGrid
server (192.168.1.71)
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 SF-IMS[3947]: [3947] pm:process [INFO] Process pxgrid_agent (12469) exited
cleanly
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 SF-IMS[12469]: pxgrid_agent.pl:fatal [WARN] No CA certificate defined in the
configuration file
Oct 12 2015 13:23:24 sourcefiredc SF-IMS[3947]: [3947] pm:process [INFO] Started 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



☐		Client Name	Client Description	Capabilities	Status	Client Group
☐	▶	ise-mnt-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator
☐	▶	ise-admin-ise14		Capabilities(3 Pub, 1 Sub)	Online	Administrator
☐	▼	fsmc-agent-sourcefiredc	Cisco FireSIGHT Management Ce...	Capabilities(0 Pub, 1 Sub)	Online	EPS

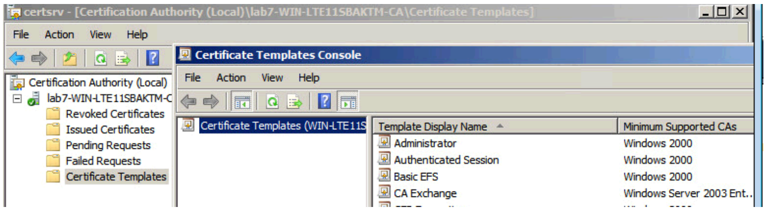
Capability Detail 1 - 1 of 1 Show 25 per page Page

	Capability Name	Capability Version	Messaging Role	Message Filter
○	EndpointProtectionService	1.0	Sub	

CA 签名操作的自定义 pxGrid 模板

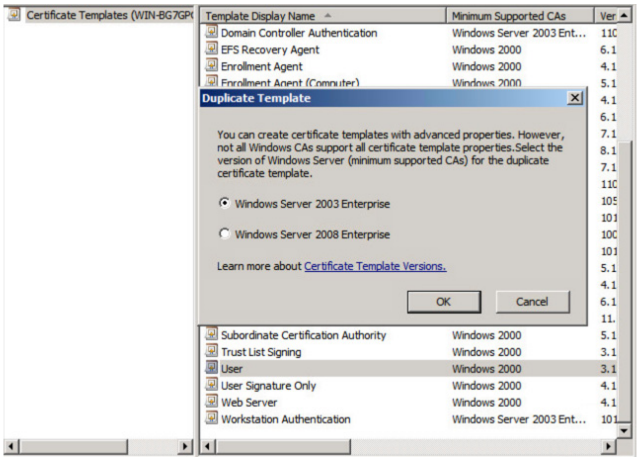
同时具有客户端身份验证和服务器身份验证的增强型密钥用法 (EKU) 的自定义 pxGrid 模板对于 pxGrid 客户端、FireSIGHT 管理中心和 ISE pxGrid 节点之间的 pxGrid 操作是必需的。这对于 FireSIGHT 管理中心和 ISE pxGrid 节点均由同一 CA 进行签名的证书颁发机构 (CA) 签名环境是必需的。

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 Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]
File
Action
View
Help
Certification Authority (Local)
lab7-WIN-LTE11SBAKTM-C
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Certificate Templates Console
Certificate Templates (WIN-LTE11S

Template Display Name	Minimum Supported CAs
Administrator	Windows 2000
Authenticated Session	Windows 2000
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)**



Template Display Name	Minimum Supported CAs	Ver
Domain Controller Authentication	Windows Server 2003 Ent...	110
EFS Recovery Agent	Windows 2000	6.1
Enrollment Agent	Windows 2000	4.1
Enrollment Agent (Computer)	Windows 2000	5.1
Subordinate Certification Authority	Windows 2000	5.1
Trust List Signing	Windows 2000	3.1
User	Windows 2000	3.1
User Signature Only	Windows 2000	4.1
Web Server	Windows 2000	4.1
Workstation Authentication	Windows Server 2003 Ent...	101

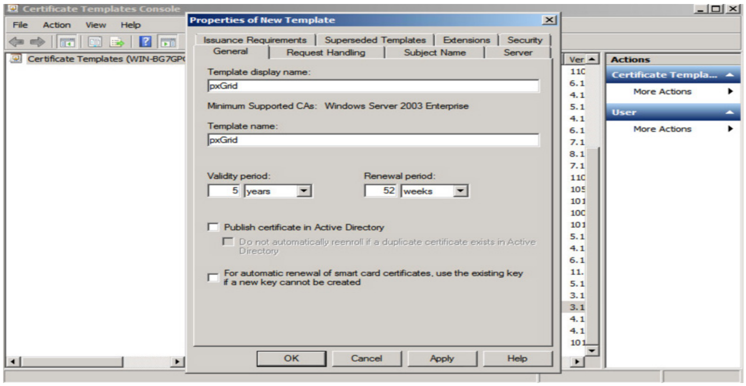
You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● Windows Server 2003 Enterprise

○ Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

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。**



Template display name:
pxGrid

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name:
pxGrid

Validity period: 5 years

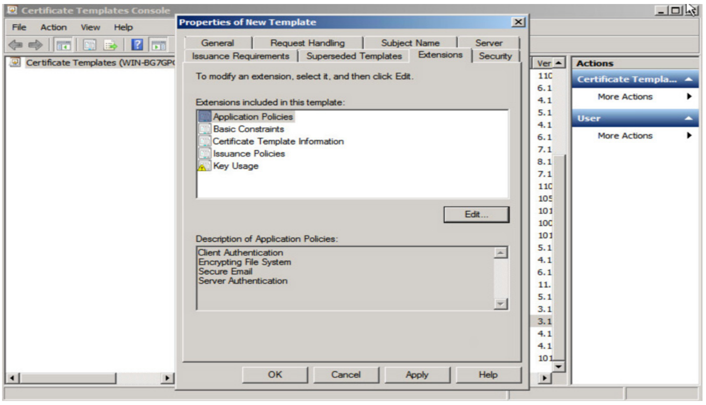
Renewal period: 52 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

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)



To modify an extension, select it, and then click Edit.

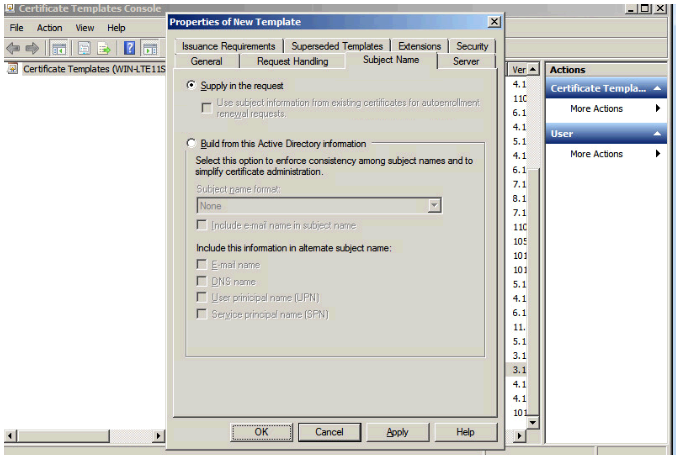
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Client Authentication
Encrypting File System
Secure Email
Server Authentication

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



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

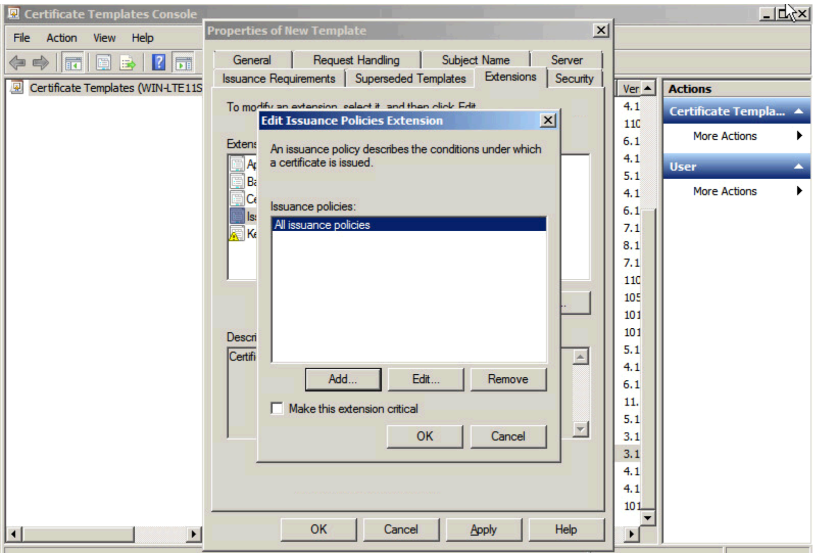
Subject name format: None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name
□ DNS name
□ User principal name (UPN)
□ Service principal name (SPN)

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)



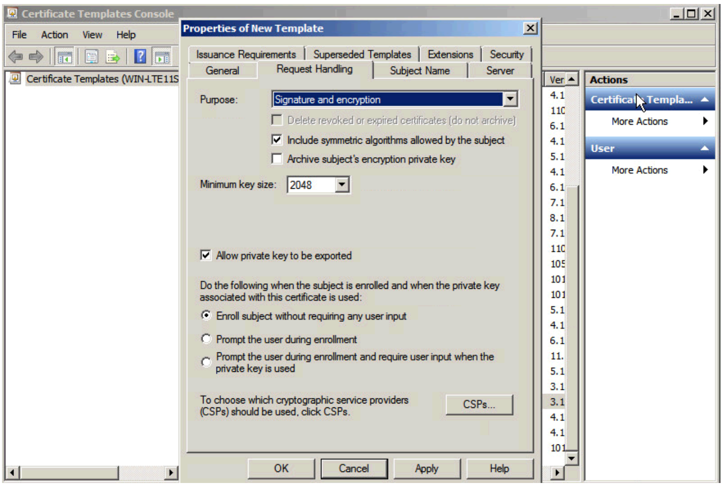
An issuance policy describes the conditions under which a certificate is issued.

Issuance policies:

- All issuance policies

□ Make this extension critical

第 7 步： 保留请求处理的默认设置


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-LTE11S
Properties of New Template
Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Subject Name | Server
Ver
4.1
110
6.1
4.1
5.1
4.1
6.1
7.1
8.1
7.1
110
105
101
101
5.1
4.1
6.1
11.
5.1
3.1
3.1
4.1
4.1
101
Actions
Certificate Templa...
More Actions
User
More Actions
CSPs...
OK
Cancel
Apply
Help

Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

☑ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

Minimum key size: 2048

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

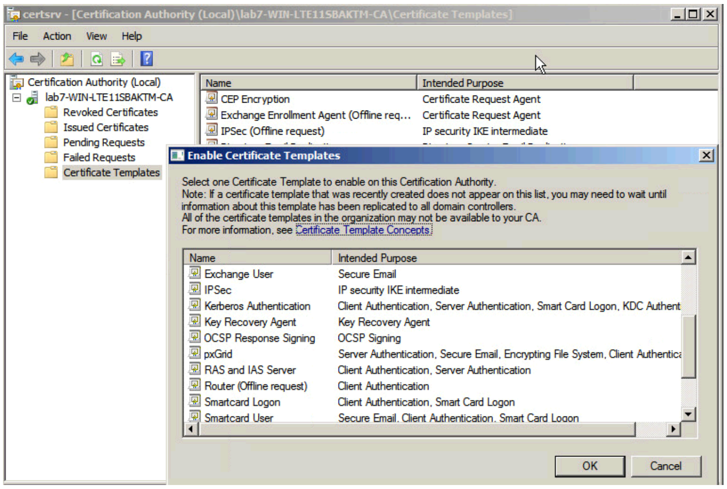
○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

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

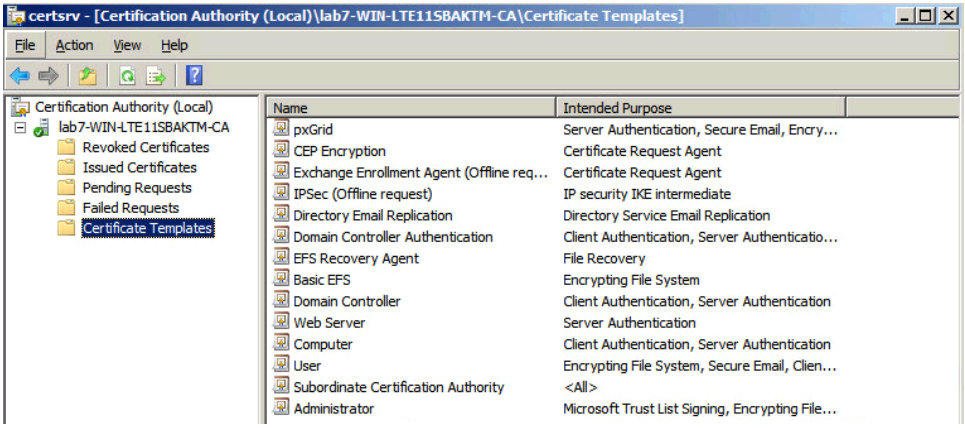

certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]
File Action View Help
Certification Authority (Local)
lab7-WIN-LTE11SBAKTM-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Enable Certificate Templates
OK
Cancel

Name	Intended Purpose
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Exchange User	Secure Email
IPSec	IP security IKE intermediate
Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon, KDC Authent
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
pxGrid	Server Authentication, Secure Email, Encrypting File System, Client Authentica
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon

第 10 步： 您应该看到 pxGrid 模板



Name	Intended Purpose
pxGrid	Server Authentication, Secure Email, Encry...
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

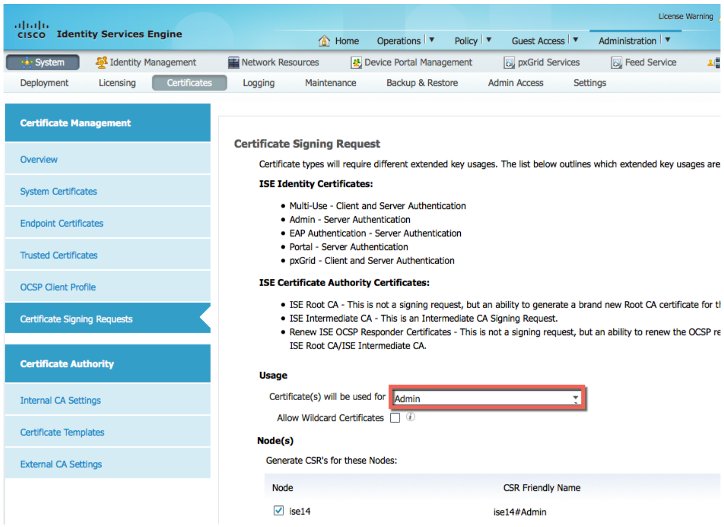
在使用 pxGrid 的独立环境中配置 CA 签名证书的 ISE

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)

注意：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。



Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are

ISE Identity Certificates:

- Multi-Use - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for tl
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP re ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: Admin

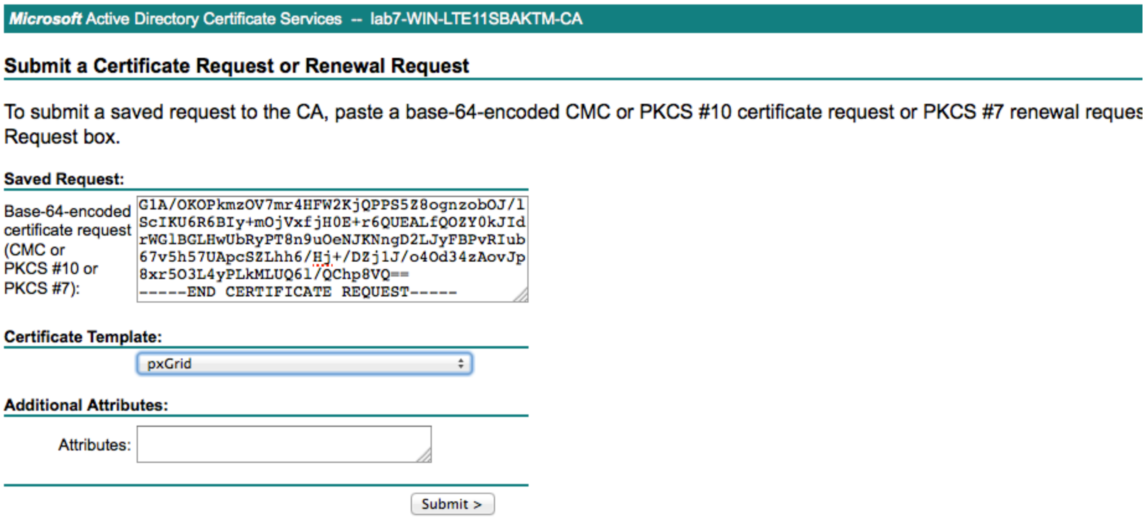
Allow Wildcard Certificates □

Node(s)

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)**


Microsoft Active Directory Certificate Services -- lab7-WIN-LTE11SBAKTM-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal reques Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

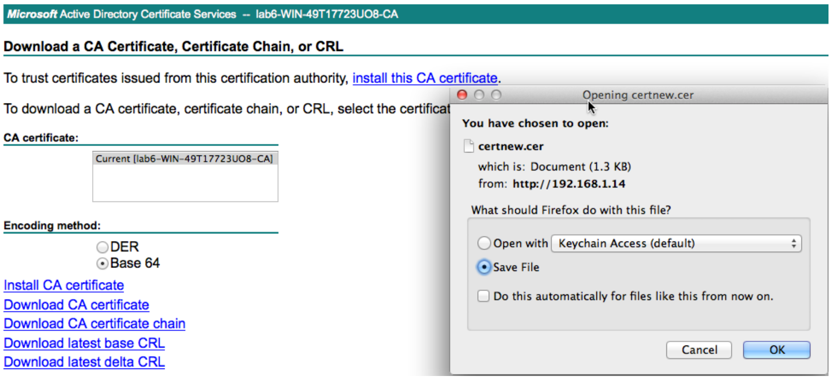
```
GlA/OKOPkmzOV7mr4HFW2KjQPPS5Z8ognzobOJ/l
ScIKU6R6BIy+mOjVxfjH0E+r6QUEALfQOZY0kJId
rWGlBGLHwUbRyPT8n9uOeNJKNngD2LJyFBPvRIub
67v5h57UApcSZLhh6/Hj+/DZj1J/o4Od34zAovJp
8xr5O3L4yPLkMLUQ6l/QChp8VQ==
-----END CERTIFICATE REQUEST-----
```

Certificate Template: pxGrid

Additional Attributes:

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 certificate.

To download a CA certificate, certificate chain, or CRL, select the certificat

CA certificate: Current [lab6-WIN-49T17723UO8-CA]

Encoding method:
○ DER
● Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Opening certnew.cer

You have chosen to open:

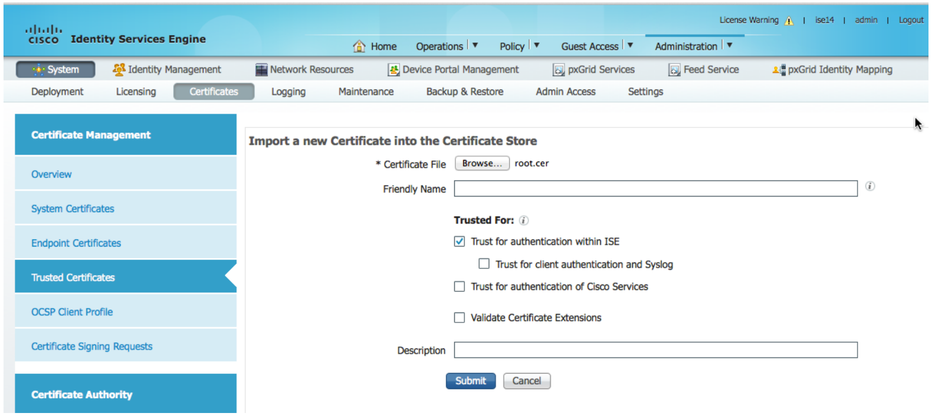
certnew.cer
which is: Document (1.3 KB)
from: http://192.168.1.14

What should Firefox do with this file?

○ Open with Keychain Access (default)
● Save File

□ Do this automatically for files like this from now on.

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



Import a new Certificate into the Certificate Store

* Certificate File Browse... root.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

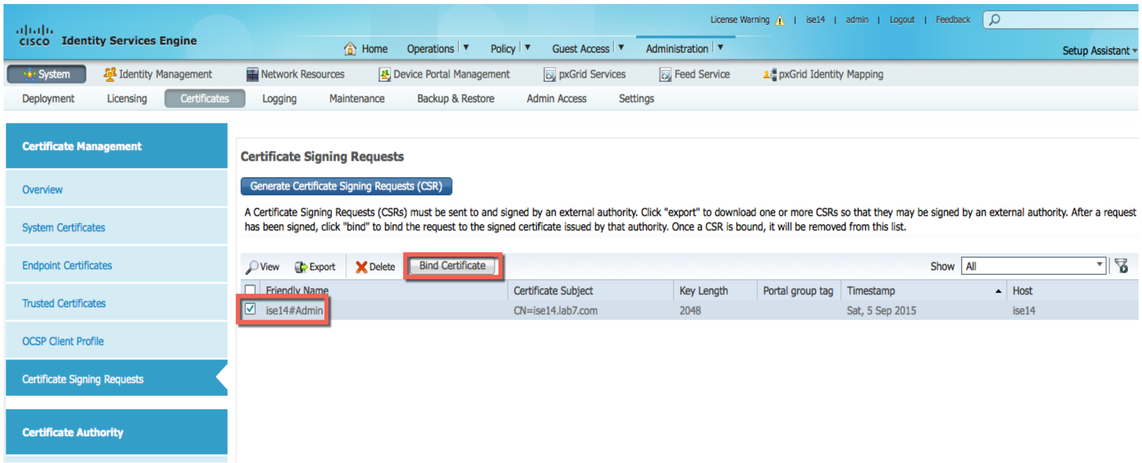
□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description

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



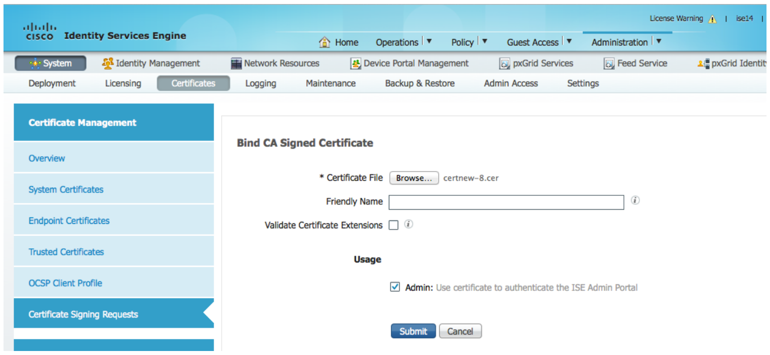
Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

Show All

	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
☑	ise14#Admin	CN=ise14.lab7.com	2048		Sat, 5 Sep 2015	ise14

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



Bind CA Signed Certificate

* Certificate File certnew-8.cer

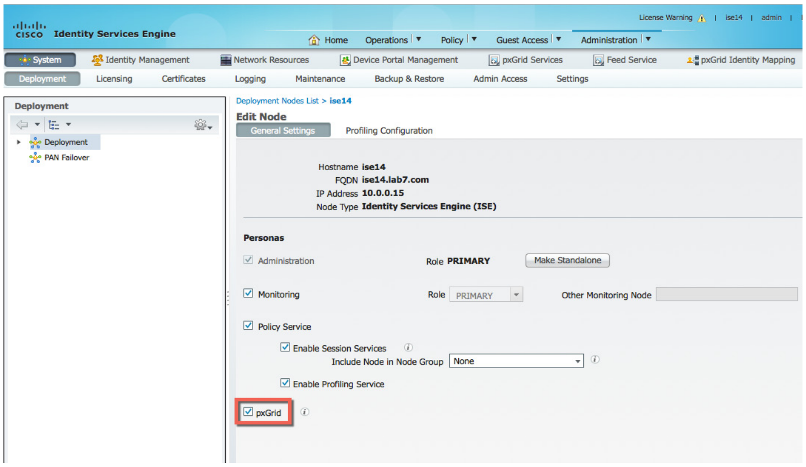
Friendly Name

Validate Certificate Extensions □

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

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



Edit Node

Hostname **ise14**
FQDN **ise14.lab7.com**
IP Address **10.0.0.15**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration Role **PRIMARY**

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

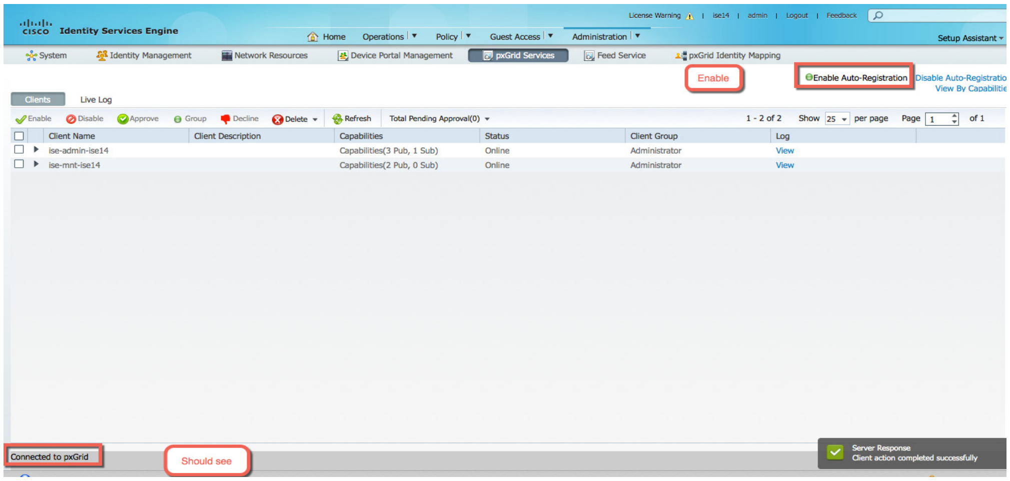
☑ Enable Session Services
Include Node in Node Group None

☑ Enable Profiling Service

☑ pxGrid

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)

注意：可能需要几秒钟时间才会出现 pxGrid 服务



□	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

Server Response
Client action completed successfully

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

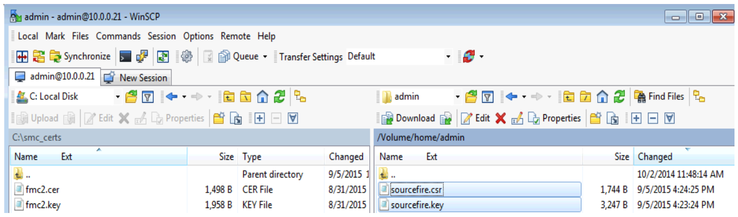
注意：此处的密码将在 pxGrid 代理配置中进行定义

```
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

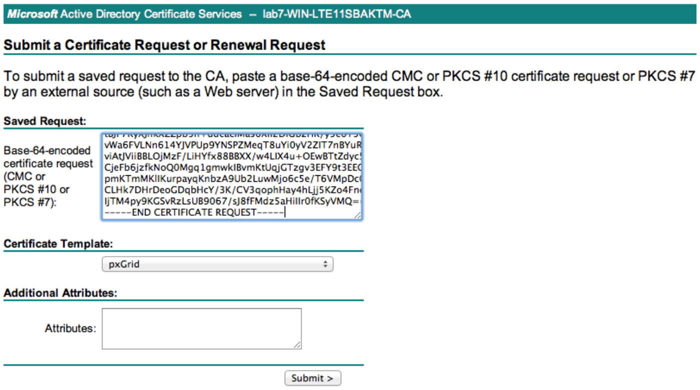
C:\smc_certs

Name Ext	Size	Type	Changed
..		Parent directory	9/5/2015 1
fmc2.cer	1,498 B	CER File	8/31/2015
fmc2.key	1,958 B	KEY File	8/31/2015

/Volume/home/admin

Name Ext	Size	Changed
..		10/2/2014 11:48:14 AM
sourcefire.csr	1,744 B	9/5/2015 4:24:25 PM
sourcefire.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


Microsoft Active Directory Certificate Services -- lab7-WIN-LTE11SBAKTM-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
vWa6FVLNn614YJVPUp9YNSPZMeqT8uYi0yV2ZIT7nBYuR
viAtJViiBBLOjMzF/LiHYfx88BBXX/w4LIX4u+OEwBTtZdyc
CjeFb6jzfkNoQ0Mgq1gmwklBvmKtUqjGTzgv3EFY9t3EE
pmKTmMKlIKurpayqKnbzA9Ub2LuwMjo6c5e/T6VMpDc
CLHk7DHrDeoGDqbHcY/3K/CV3qophHay4hLjj5KZo4Fn
IjTM4py9KGSvRzLsUB9067/sJ8fFMdz5aHiIlr0fKSyVMQ=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

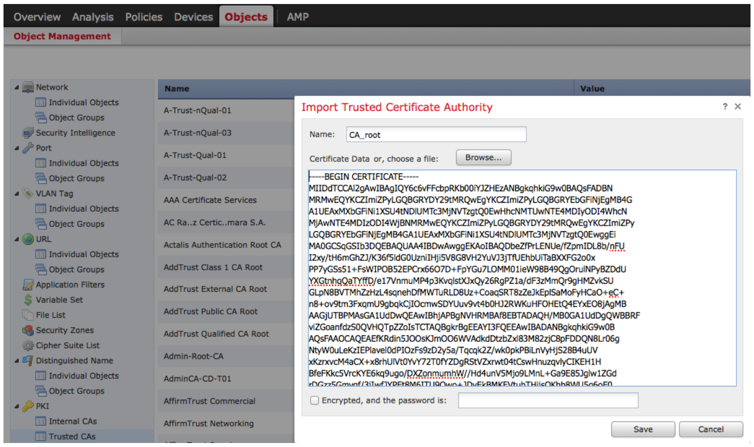
pxGrid

Additional Attributes:

Attributes:

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)



Import Trusted Certificate Authority

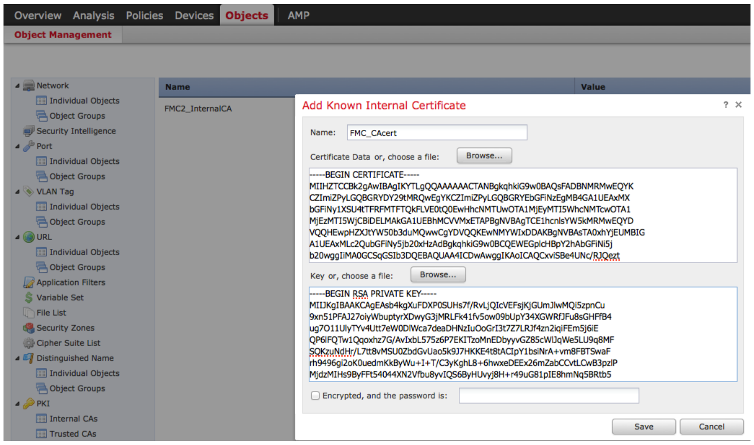
Name: CA_root

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgIQY6c6vFFcbpRKb00iYJZHEzANBgkqhkiG9w0BAQsFADBN
MRMwEQYKCZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPyLGQBGRYEbGFiNjEgMB4G
A1UEAxMXbGFiNi1XSU4tNDlUMTc3MjNVTzgtQ0EwHhcNMTUwNTE4MDIyODI4WhcN
MjAwNTE4MDIzODI4WjBNMRMwEQYKCZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPy
LGQBGRYEbGFiNjEgMB4GA1UEAxMXbGFiNi1XSU4tNDlUMTc3MjNVTzgtQ0EwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDbeZfPrLENUe/fZpmIDL8b/nFU
I2xy/tH6mGhZJ/K36f5ldG0UzniIHji5V8G8VH2YuVJ3jTfUEhbUiTaBXXFG2o0x
PP7yGSs51+FsWIPOB52EPCrx66O7D+FpYGu7LOMM01ieW98B49QgOrulNPyBZDdU
YXGtnhqQaTYffD/e17VnmuMP4p3KvqlstXJxQy26RgPZ1a/dF3zMmQr9gHMZvkSU
GLpN8BVTMhZzHzL4sqnehDfMWTuRLD8Uz+CoaqSRT8zZeJkEplSaMoFyHCaO+eC+
n8+ov9tm3FxqmU9gbqkCjIOcmwSDYUuv9vt4b0HJ2RWKuHFOHEtQ4EYxEO8jAgMB
AAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRF
viZGoanfdzS0QVHQTpZZoIsTCTAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B
AQsFAAOCAQEAEfKRdin5JOOsKJmOO6WVAdkdDtzbZxl83M82zjC8pFDDQN8Lr06g
NtyW0uLeKzIEPlavel0dPIOzFs9zD2y5a/Tqcqk2Z/wk0pkPBiLnVyHjS28B4uUV
xKzrxvcM4aCX+x8rhUlVt0YvY72T0fYZDgRStVZxrwt04tCswHnuzqvlyCIKEH1H
BfeFKkc5VrcKYE6kq9ugo/DXZonmumhW//Hd4unV5Mjo9LMnL+Ga9E85Jglw1ZGd
```

☐ Encrypted, and the password is:

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)



Add Known Internal Certificate

Name: FMC_CAcert

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIHZTCCBk2gAwIBAgIKYTLgQQAAAAAACTANBgkqhkiG9w0BAQsFADBNMRMwEQYK
CZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPyLGQBGRYEbGFiNzEgMB4GA1UEAxMX
bGFiNy1XSU4tTFRFMTFTQkFLVE0tQ0EwHhcNMTUwOTA1MjEyMTI5WhcNMTcwOTA1
MjEzMTI5WjCBiDELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE1hcnlsYW5kMRMwEQYD
VQQHEwpHZXJtYW50b3duMQwwCgYDVQQKEwNMYWIxDDAKBgNVBAsTA0xhYjEUMBIG
A1UEAxMLc2QubGFiNy5jb20xHzAdBgkqhkiG9w0BCQEWEGplcHBpY2hAbGFiNi5j
b20wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCxviSBe4UNc/RJQezt
```

Key or, choose a file:

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKgIBAAKCAgEAsb4kgXuFDXP0SUHs7f/RvLjQIcVEFsjKjGUmJlwMQi5zpnCu
9xn51PFAJ27oiyWbuptyrXDwyG3jMRLFk41fv5ow09bUpY34XGWRfJFu8sGHFfB4
ug7O11UlyTYv4Utt7eW0DlWca7deaDHNzIuOoGrI3t7Z7LRJf4zn2iqiFEm5j6iE
QP6lFQTw1Qqoxhz7G/AvIxbL575z6P7EKITzoMnEDbyyvGZ85cWlJqWe5LU9q8MF
SQKzuNdHr/L7tt8vMSU0ZbdGvUao5k9J7HKKE4t8tACIpY1bsiNrA+vm8FBTSwaF
rh9496gi2oK0uedmKkByWu+I+T/C3yKghL8+6hwxeDEEx26mZabCCvtLCwB3pzlP
MjdzMIHs9ByFFt54044XN2Vfbu8yvIQS6ByHUvyj8H+r49uG81pIE8hmNq5BRtb5
```

☐ Encrypted, and the password is:

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

注意：大写/小写语法予以保留

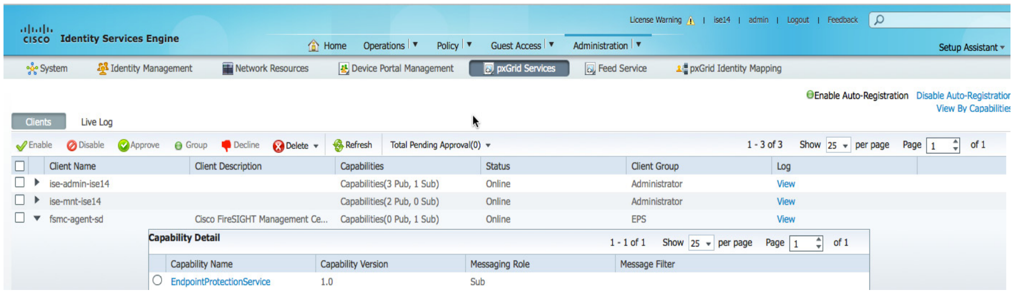
第 3 步： 通过 SSH 传输到 FireSIGHT 管理中心并键入以下内容：

```
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)**



□		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 Management Ce...	Capabilities(0 Pub, 1 Sub)	Online	EPS	View

Capability Detail 1 - 1 of 1 Show 25 per page Page 1 of 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	EndpointProtectionService	1.0	Sub	

FireSIGHT pxGrid 补救模块

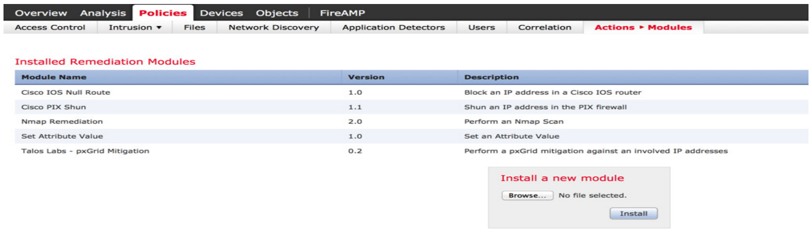
在本节中，pxGrid 缓解补救模块上传到 FireSIGHT 管理中心。系统将创建 pxGrid 实例并定义补救类型。这些补救类型在作为响应分配到其各自的关联策略时提供 pxGrid ANC 功能。

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。



Installed Remediation Modules

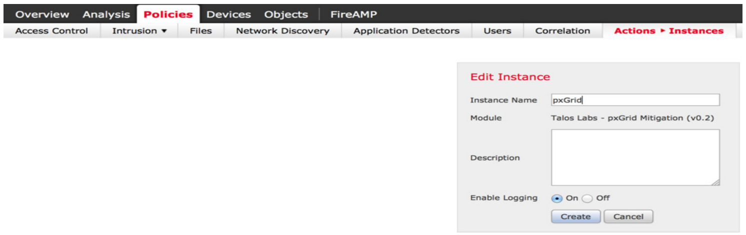
Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Cisco PIX Shun	1.1	Shun an IP address in the PIX firewall
Nmap Remediation	2.0	Perform an Nmap Scan
Set Attribute Value	1.0	Set an Attribute Value
Talos Labs - pxGrid Mitigation	0.2	Perform a pxGrid mitigation against an involved IP addresses

Install a new module

Browse... No file selected.

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)**



Edit Instance

Instance Name: pxGrid

Module: Talos Labs - pxGrid Mitigation (v0.2)

Description:

Enable Logging: ● On ○ Off

创建 FireSIGHT pxGrid 缓解类型

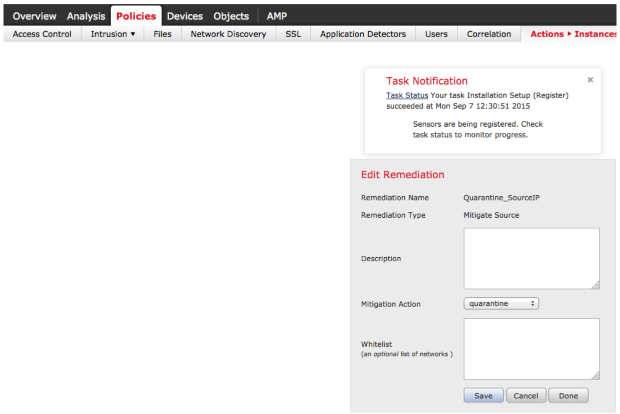
这些补救类型定义作为响应分配到用于在终端上触发补救操作的关联规则的 pxGrid ANC 缓解操作

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)**



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.

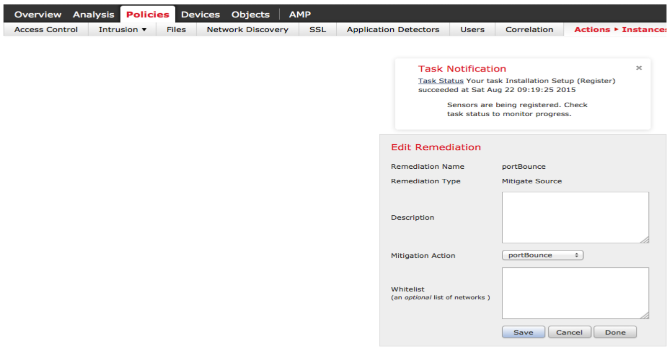
Edit Remediation

Remediation Name Quarantine_SourceIP
Remediation Type Mitigate Source
Description
Mitigation Action quarantine
Whitelist
(an *optional* list of networks)

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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Sat Aug 22 09:19:25 2015

Sensors are being registered. Check task status to monitor progress.

Edit Remediation

Remediation Name portBounce

Remediation Type Mitigate Source

Description

Mitigation Action portBounce

Whitelist
(an *optional* list of networks)

重新身份验证

根据缓解源创建重新身份验证缓解操作

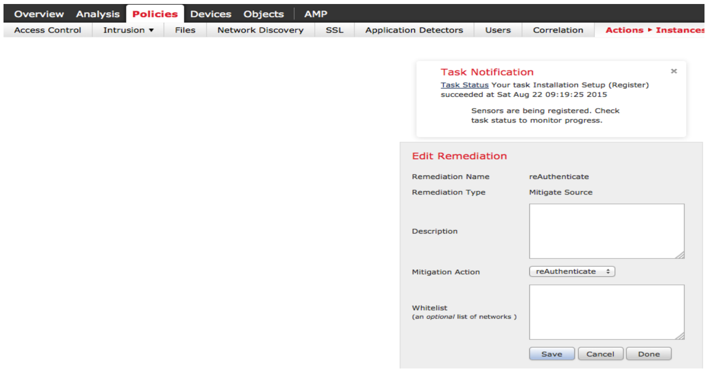
第 1 步：　策略 (Policies)->操作 (Actions)->实例 (Instances)，点击已配置的实例 (Configured Instances) 下的“pxGrid”旁边的放大镜

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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Sat Aug 22 09:19:25 2015

Sensors are being registered. Check task status to monitor progress.

Edit Remediation

Remediation Name reAuthenticate

Remediation Type Mitigate Source

Description

Mitigation Action reAuthenticate

Whitelist
(an *optional* list of networks)

关闭

根据缓解源创建关闭缓解操作

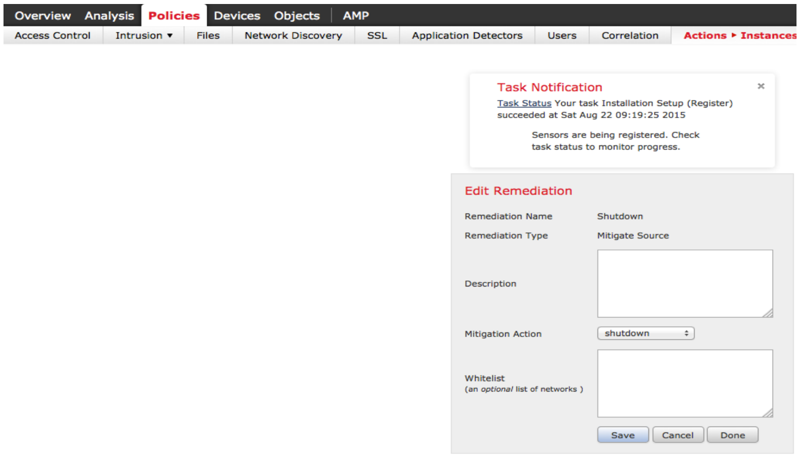
第 1 步：　策略 (Policies)->操作 (Actions)->实例 (Instances)，点击已配置的实例 (Configured Instances) 下的“pxGrid”旁边的放大镜

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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Sat Aug 22 09:19:25 2015

Sensors are being registered. Check task status to monitor progress.

Edit Remediation

Remediation Name: Shutdown

Remediation Type: Mitigate Source

Description:

Mitigation Action: shutdown

Whitelist (an *optional* list of networks):

终止

根据缓解源创建终止缓解操作

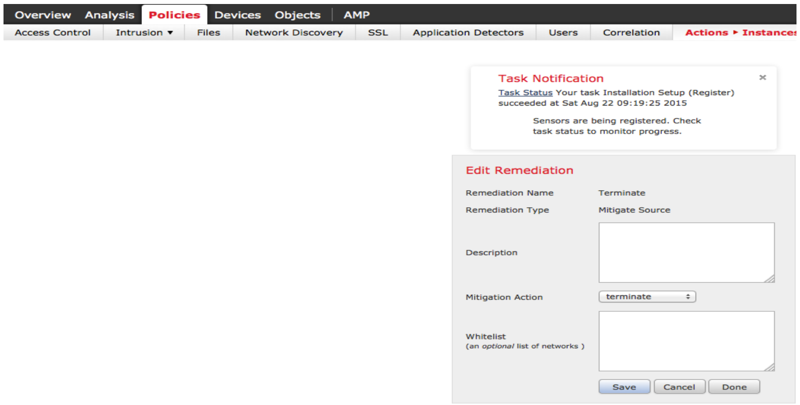
第 1 步： **策略 (Policies)->操作 (Actions)->实例 (Instances)，点击已配置的实例 (Configured Instances) 下的“pxGrid”旁边的放大镜**

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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Sat Aug 22 09:19:25 2015

Sensors are being registered. Check task status to monitor progress.

Edit Remediation

Remediation Name: Terminate

Remediation Type: Mitigate Source

Description:

Mitigation Action: terminate

Whitelist (an *optional* list of networks):

取消隔离

根据缓解源创建取消隔离缓解操作

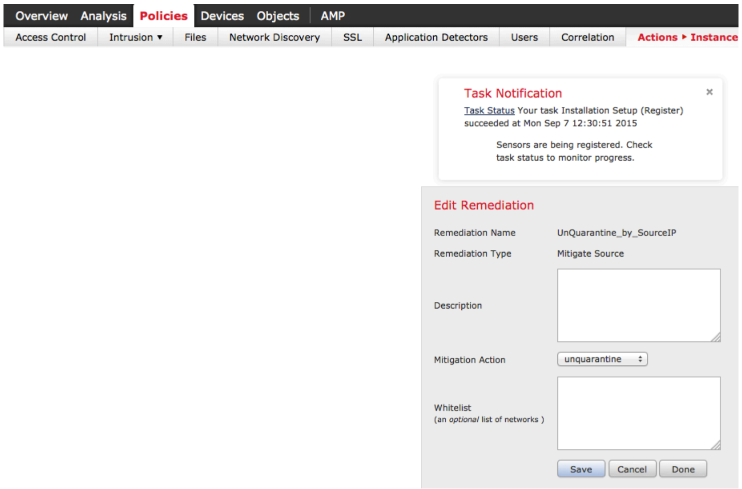
第 1 步： **策略 (Policies)->操作 (Actions)->实例 (Instances)，点击已配置的实例 (Configured Instances) 下的“pxGrid”旁边的放大镜**

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)**



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.

Edit Remediation

Remediation Name: UnQuarantine_by_SourceIP

Remediation Type: Mitigate Source

Description:

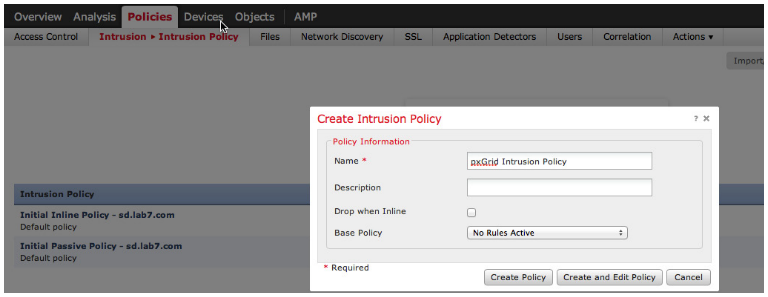
Mitigation Action: unquarantine

Whitelist (an *optional* list of networks):

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 www.yahoo.com/cmd.exe 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)**



Create Intrusion Policy

Policy Information

Name * pxGrid Intrusion Policy

Description

Drop when Inline □

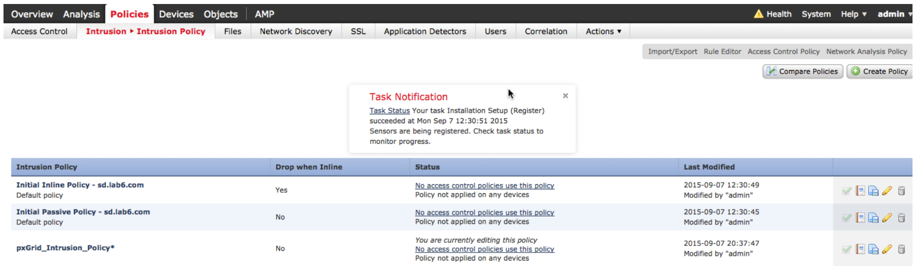
Base Policy No Rules Active

* Required

Create Policy | Create and Edit Policy | Cancel

Intrusion Policy
Initial Inline Policy - sd.lab7.com Default policy
Initial Passive Policy - sd.lab7.com Default policy

第 5 步： **点击->pxGrid_Intrusion_Policy** 以进行编辑

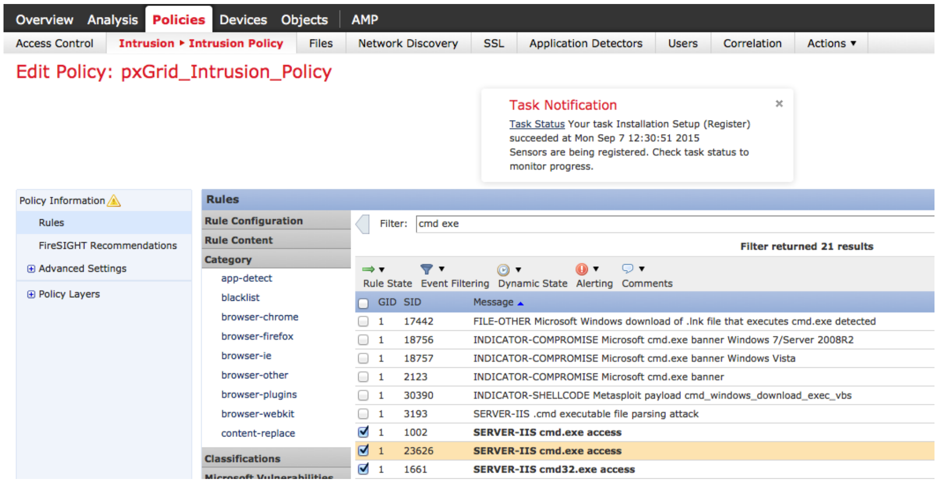


Task Notification

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.

Intrusion Policy	Drop when Inline	Status	Last Modified
Initial Inline Policy - sd.lab6.com Default policy	Yes	No access control policies use this policy Policy not applied on any devices	2015-09-07 12:30:49 Modified by "admin"
Initial Passive Policy - sd.lab6.com Default policy	No	No access control policies use this policy Policy not applied on any devices	2015-09-07 12:30:45 Modified by "admin"
pxGrid_Intrusion_Policy*	No	*You are currently editing this policy* No access control policies use this policy Policy not applied on any devices	2015-09-07 20:37:47 Modified by "admin"

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



Edit Policy: pxGrid_Intrusion_Policy

Task Notification

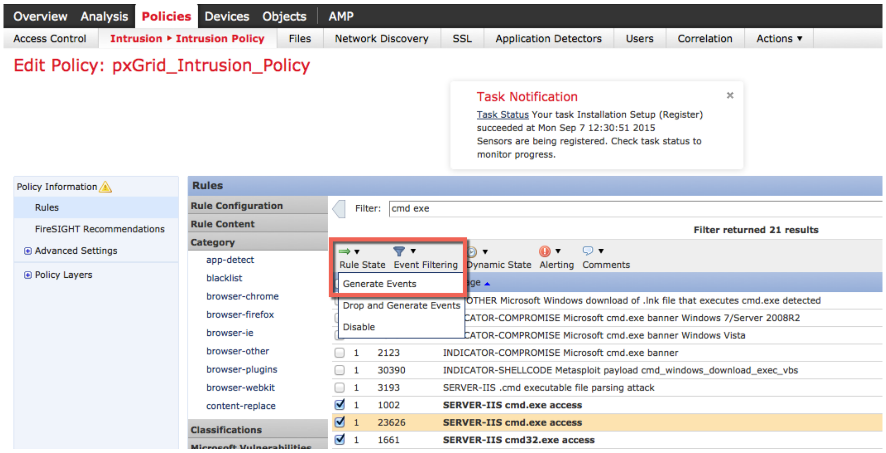
Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015
Sensors are being registered. Check task status to monitor progress.

Filter: cmd exe

Filter returned 21 results

□	GID	SID	Message ▲
□	1	17442	FILE-OTHER Microsoft Windows download of .lnk file that executes cmd.exe detected
□	1	18756	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows 7/Server 2008R2
□	1	18757	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows Vista
□	1	2123	INDICATOR-COMPROMISE Microsoft cmd.exe banner
□	1	30390	INDICATOR-SHELLCODE Metasploit payload cmd_windows_download_exec_vbs
□	1	3193	SERVER-IIS .cmd executable file parsing attack
☑	1	1002	**SERVER-IIS cmd.exe access**
☑	1	23626	**SERVER-IIS cmd.exe access**
☑	1	1661	**SERVER-IIS 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)**



Edit Policy: pxGrid_Intrusion_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.

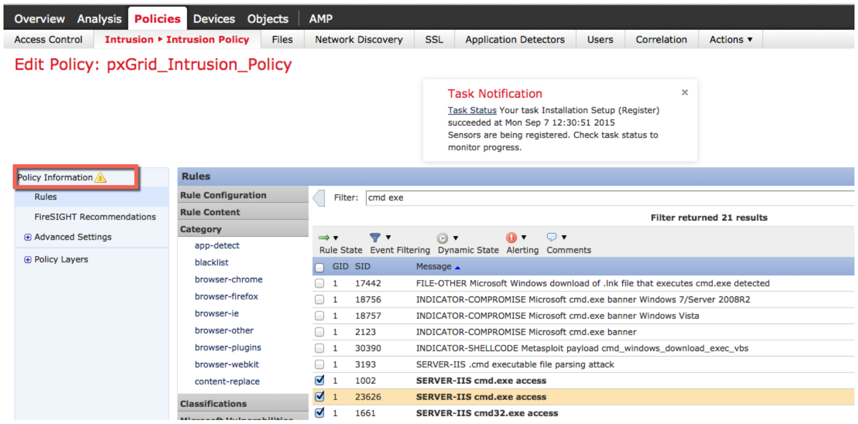
Filter: cmd exe

Filter returned 21 results

			...age ▲
			...OTHER Microsoft Windows download of .lnk file that executes cmd.exe detected
			...CATOR-COMPROMISE Microsoft cmd.exe banner Windows 7/Server 2008R2
			...CATOR-COMPROMISE Microsoft cmd.exe banner Windows Vista
□	1	2123	INDICATOR-COMPROMISE Microsoft cmd.exe banner
□	1	30390	INDICATOR-SHELLCODE Metasploit payload cmd_windows_download_exec_vbs
□	1	3193	SERVER-IIS .cmd executable file parsing attack
☑	1	1002	**SERVER-IIS cmd.exe access**
☑	1	23626	**SERVER-IIS cmd.exe access**
☑	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)**



Edit Policy: pxGrid_Intrusion_Policy

Task Notification

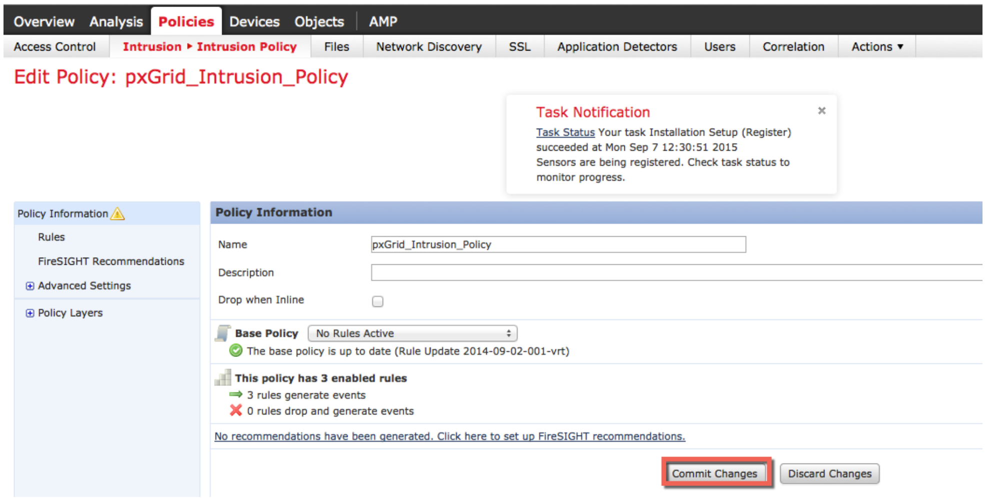
Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015
Sensors are being registered. Check task status to monitor progress.

Filter: cmd exe

Filter returned 21 results

□	GID	SID	Message ▲
□	1	17442	FILE-OTHER Microsoft Windows download of .lnk file that executes cmd.exe detected
□	1	18756	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows 7/Server 2008R2
□	1	18757	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows Vista
□	1	2123	INDICATOR-COMPROMISE Microsoft cmd.exe banner
□	1	30390	INDICATOR-SHELLCODE Metasploit payload cmd_windows_download_exec_vbs
□	1	3193	SERVER-IIS .cmd executable file parsing attack
☑	1	1002	**SERVER-IIS cmd.exe access**
☑	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)**



Edit Policy: pxGrid_Intrusion_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.

Policy Information

Name: pxGrid_Intrusion_Policy

Description:

Drop when Inline □

Base Policy No Rules Active

The base policy is up to date (Rule Update 2014-09-02-001-vrt)

This policy has 3 enabled rules

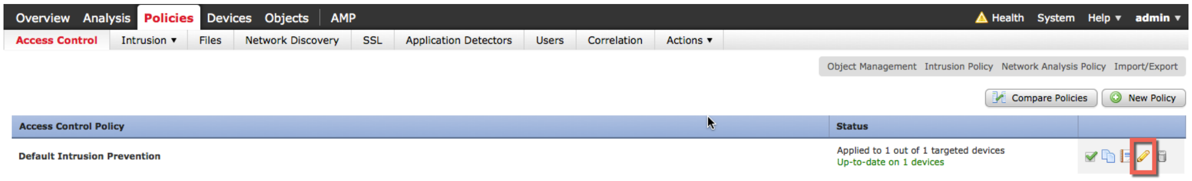
3 rules generate events

0 rules drop and generate events

No recommendations have been generated. Click here to set up FireSIGHT recommendations.

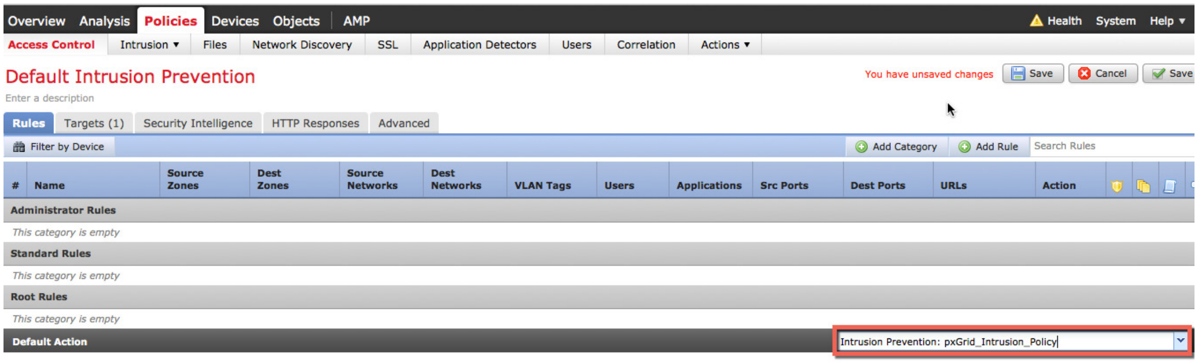
第 11 步： 点击**确定 (OK)**

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)**


Overview Analysis Policies Devices Objects AMP
Health System Help ▾ admin ▾
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾
Object Management Intrusion Policy Network Analysis Policy Import/Export
Compare Policies New Policy

Access Control Policy	Status
Default Intrusion Prevention	Applied to 1 out of 1 targeted devices Up-to-date on 1 devices

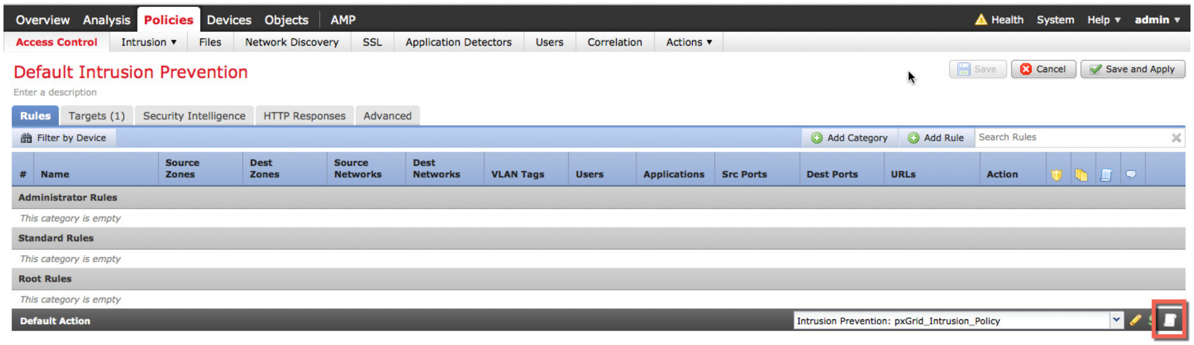
第 13 步： 在“默认操作”(Default actions) 下，从下拉列表中选择 **pxGrid_Intrusion_Policy**


Overview Analysis Policies Devices Objects AMP
Health System Help ▾
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾
Default Intrusion Prevention
Enter a description
You have unsaved changes
Save
Cancel
Save
Rules Targets (1) Security Intelligence HTTP Responses Advanced
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

Administrator Rules
This category is empty
Standard Rules
This category is empty
Root Rules
This category is empty
Default Action: Intrusion Prevention: pxGrid_Intrusion_Policy

第 14 步： 点击**保存 (Save)**

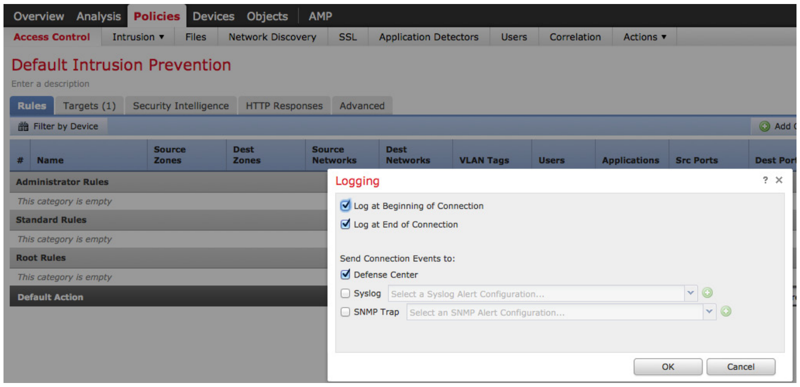
第 15 步： 点击表右下方的**日志记录 (Logging)** 图标


Overview Analysis Policies Devices Objects AMP
Health System Help ▾ admin ▾
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾
Default Intrusion Prevention
Enter a description
Save
Cancel
Save and Apply
Rules Targets (1) Security Intelligence HTTP Responses Advanced
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

Administrator Rules
This category is empty
Standard Rules
This category is empty
Root Rules
This category is empty
Default Action: Intrusion Prevention: pxGrid_Intrusion_Policy

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 Devices Objects AMP
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾
Default Intrusion Prevention
Enter a description
Rules Targets (1) Security Intelligence HTTP Responses Advanced
Filter by Device
# Name Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applications Src Ports Dest Por
Administrator Rules
This category is empty
Standard Rules
This category is empty
Root Rules
This category is empty
Default Action
OK
Cancel

Logging

☑ Log at Beginning of Connection

☑ Log at End of Connection

Send Connection Events to:

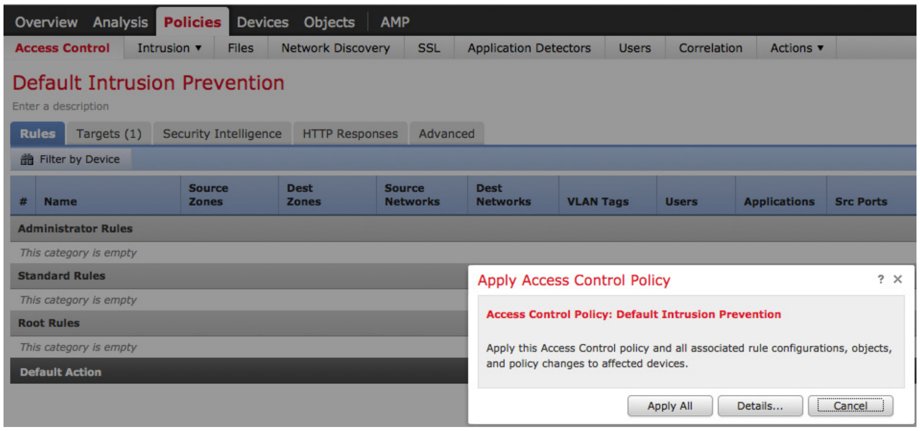
☑ Defense Center

□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

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：



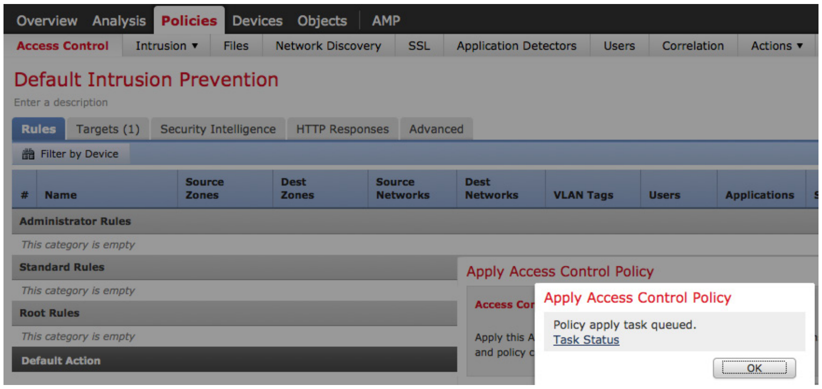
Apply Access Control Policy

Access Control Policy: Default Intrusion Prevention

Apply this Access Control policy and all associated rule configurations, objects, and policy changes to affected devices.

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

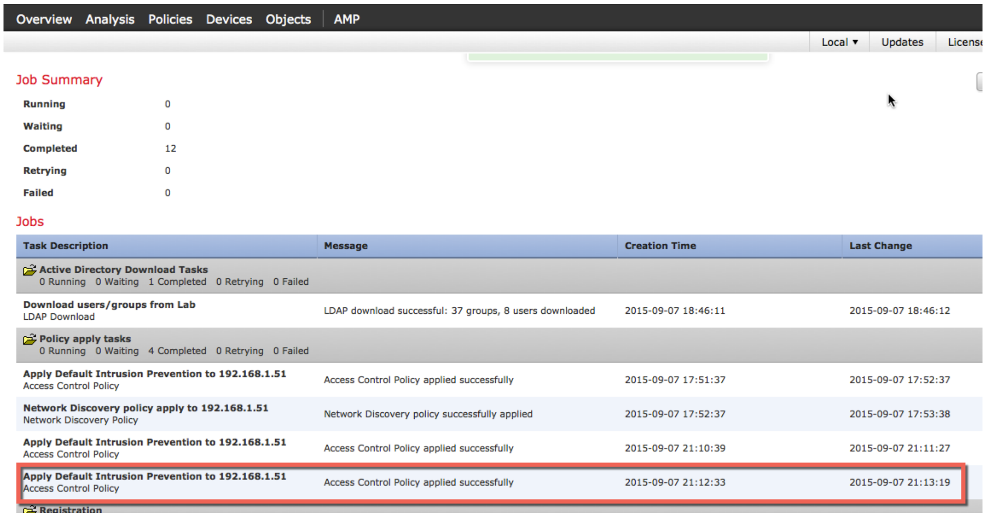


Apply Access Control Policy

Policy apply task queued.
Task Status

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



Job Summary

Running	0
Waiting	0
Completed	12
Retrying	0
Failed	0

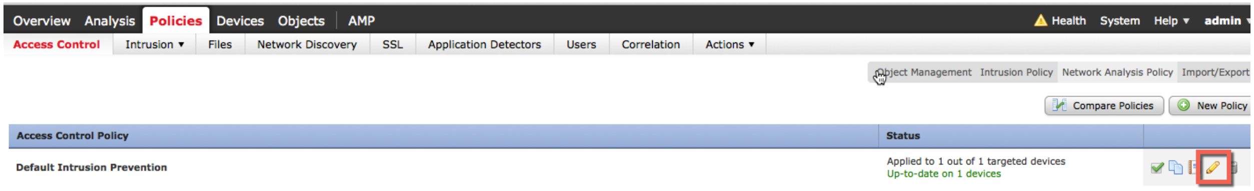
Jobs

Task Description	Message	Creation Time	Last Change
Active Directory Download Tasks 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed			
Download users/groups from Lab LDAP Download	LDAP download successful: 37 groups, 8 users downloaded	2015-09-07 18:46:11	2015-09-07 18:46:12
Policy apply tasks 0 Running 0 Waiting 4 Completed 0 Retrying 0 Failed			
Apply Default Intrusion Prevention to 192.168.1.51 Access Control Policy	Access Control Policy applied successfully	2015-09-07 17:51:37	2015-09-07 17:52:37
Network Discovery policy apply to 192.168.1.51 Network Discovery Policy	Network Discovery policy successfully applied	2015-09-07 17:52:37	2015-09-07 17:53:38
Apply Default Intrusion Prevention to 192.168.1.51 Access Control Policy	Access Control Policy applied successfully	2015-09-07 21:10:39	2015-09-07 21:11:27
Apply Default Intrusion Prevention to 192.168.1.51 Access Control Policy	Access Control Policy applied successfully	2015-09-07 21:12:33	2015-09-07 21:13:19
Registration			

FireSIGHT 连接规则

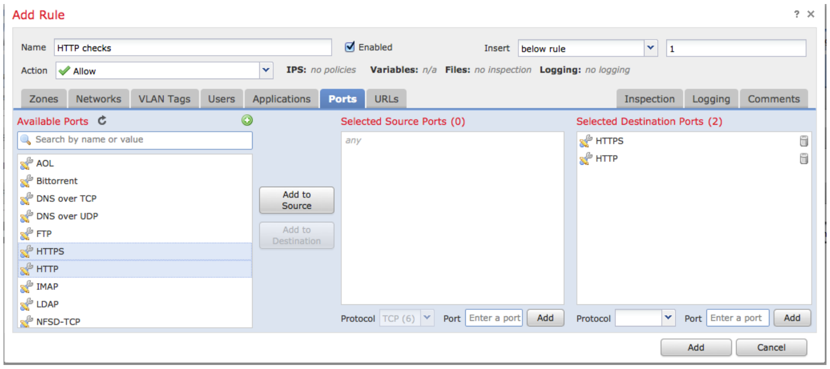
在本节中，我们定义要添加到默认访问策略中的连接规则。此默认访问策略还包括 pxGrid 入侵策略。此连接规则通过 HTTP/HTTPS 监控连接事件，并将这些连接详细信息记录到 FireSIGHT 管理中心。此连接规则将由 UnQuarantine 策略用于监控触发 unquarantine 补救类型的连接事件。

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)**



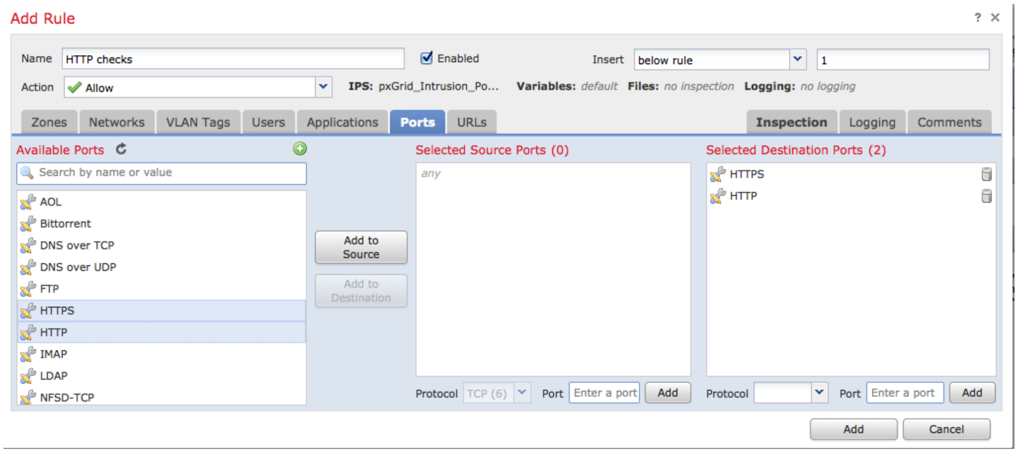
Access Control Policy	Status
Default Intrusion Prevention	Applied to 1 out of 1 targeted devices Up-to-date on 1 devices

第 3 步： 点击**添加规则 (Add Rule)**
第 4 步： 将规则命名为 **“HTTP Checks”**
第 5 步： 选择**端口 (Ports)** 选项卡
第 6 步： 选择 **HTTP** 和 **HTTPS** 作为目标端口



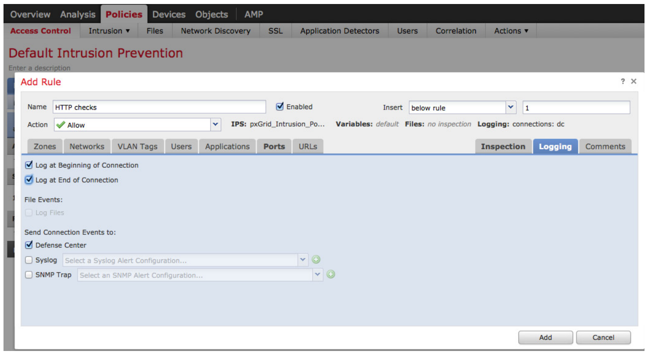
Name: HTTP checks ☑ Enabled Insert: below rule 1
Action: ✓ Allow IPS: no policies Variables: n/a Files: no inspection Logging: no logging
Selected Source Ports (0): any
Selected Destination Ports (2): HTTPS, HTTP
Protocol: TCP (6)

第 7 步： 点击 **IPS** 并选择 **pxGrid_Intrusion_Policy**



Name: HTTP checks ☑ Enabled Insert: below rule 1
Action: ✓ Allow IPS: pxGrid_Intrusion_Po... Variables: default Files: no inspection Logging: no logging
Selected Source Ports (0): any
Selected Destination Ports (2): HTTPS, HTTP
Protocol: TCP (6)

第 8 步： 选择日志记录 (Logging)


Overview Analysis Policies Devices Objects AMP
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾

Default Intrusion Prevention

Enter a description

Add Rule

Name: HTTP checks ☑ Enabled Insert: below rule 1

Action: ✓ Allow IPS: pxGrid_Intrusion_Po... Variables: *default* Files: *no inspection* Logging: connections: dc

Zones Networks VLAN Tags Users Applications Ports URLs Inspection Logging Comments

☑ Log at Beginning of Connection

☑ Log at End of Connection

File Events:

□ Log Files

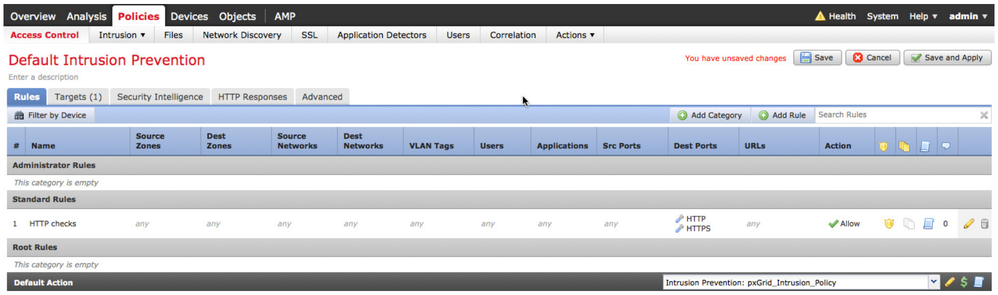
Send Connection Events to:

☑ Defense Center

□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

第 9 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 Application Detectors Users Correlation Actions ▾

Default Intrusion Prevention

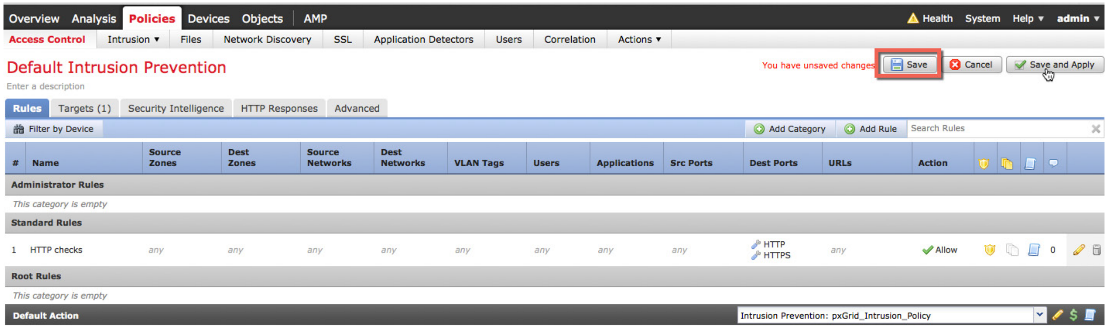
Enter a description

You have unsaved changes

Save Cancel Save and Apply
Rules Targets (1) Security Intelligence HTTP Responses Advanced
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
Administrator Rules												
This category is empty												
Standard Rules												
1	HTTP checks	any	any	any	any	any	any	any	any	HTTP HTTPS	any	✓ Allow
Root Rules												
This category is empty												
Default Action												Intrusion Prevention: pxGrid_Intrusion_Policy

第 10 步： 选择保存 (Save)


Overview Analysis Policies Devices Objects AMP Health System Help ▾ admin ▾
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾

Default Intrusion Prevention

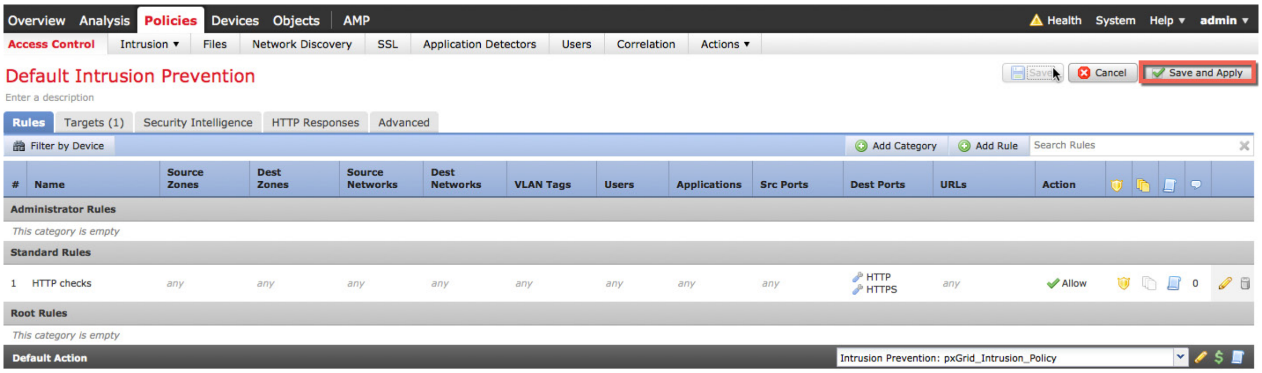
Enter a description

You have unsaved changes

Save Cancel Save and Apply
Rules Targets (1) Security Intelligence HTTP Responses Advanced
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
Administrator Rules												
This category is empty												
Standard Rules												
1	HTTP checks	any	any	any	any	any	any	any	any	HTTP HTTPS	any	✓ Allow
Root Rules												
This category is empty												
Default Action												Intrusion Prevention: pxGrid_Intrusion_Policy

第 11 步： 选择保存并应用 (Save and Apply)


Overview Analysis Policies Devices Objects AMP Health System Help ▾ admin ▾
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾

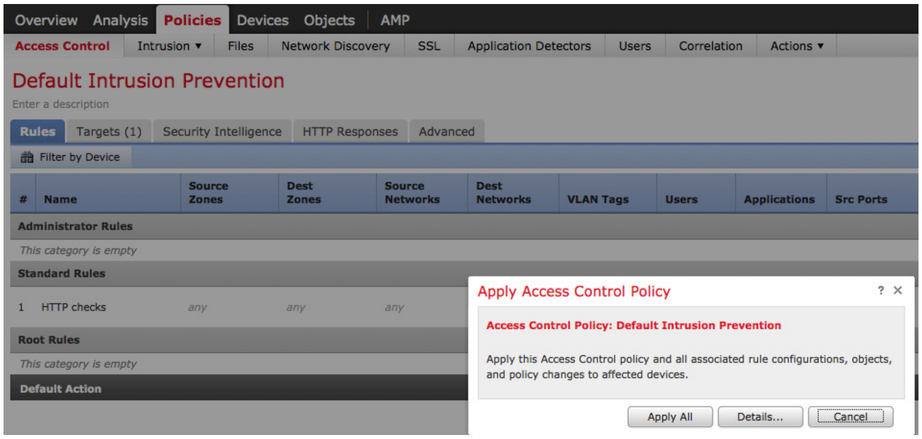
Default Intrusion Prevention

Enter a description

Save Cancel Save and Apply
Rules Targets (1) Security Intelligence HTTP Responses Advanced
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
Administrator Rules												
This category is empty												
Standard Rules												
1	HTTP checks	any	any	any	any	any	any	any	any	HTTP HTTPS	any	✓ Allow
Root Rules												
This category is empty												
Default Action												Intrusion Prevention: pxGrid_Intrusion_Policy

第 12 步： 点击全部应用 (Apply All)



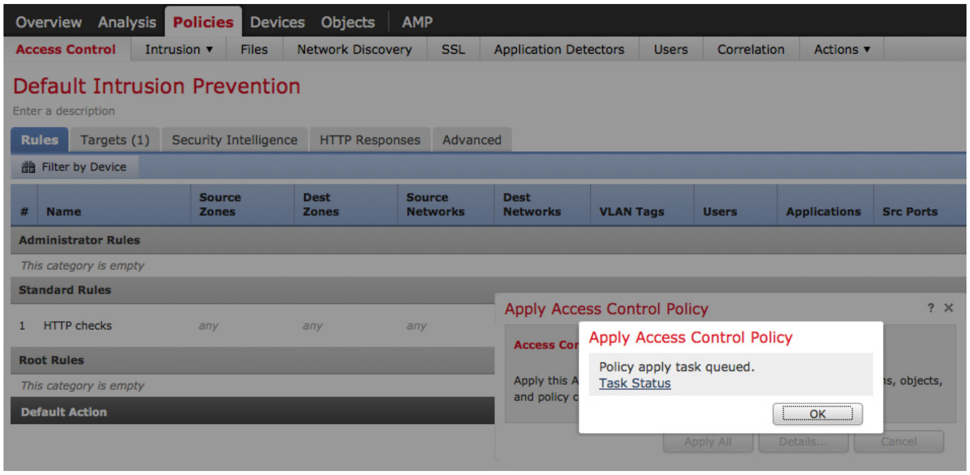
Apply Access Control Policy

Access Control Policy: Default Intrusion Prevention

Apply this Access Control policy and all associated rule configurations, objects, and policy changes to affected devices.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports
Administrator Rules									
This category is empty									
Standard Rules									
1	HTTP checks	any	any	any					
Root Rules									
This category is empty									
Default Action									

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)**



Apply Access Control Policy

Policy apply task queued.
Task Status

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports
Administrator Rules									
This category is empty									
Standard Rules									
1	HTTP checks	any	any	any					
Root Rules									
This category is empty									
Default Action									

配置 ISE EPS 服务和隔离授权策略

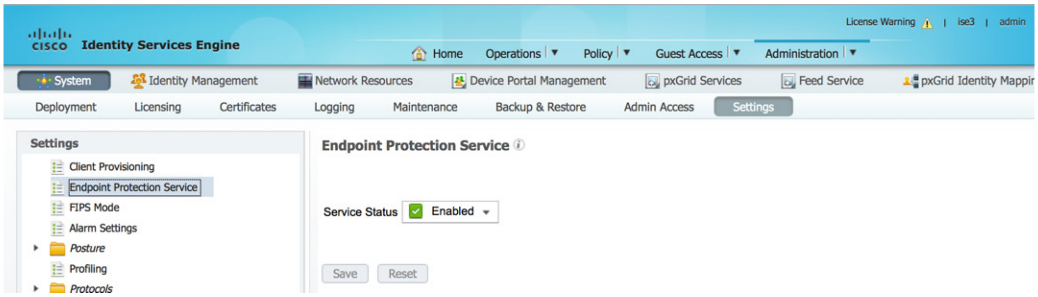
本节说明在 ISE 中启用 EPS 以及在 ISE 中创建隔离授权策略的步骤。在 ISE 1.4 中，“终端保护服务”重命名为“自适应网络控制”。在 ISE 2.0 中，默认情况下会启用此重命名，在“管理”(Administration) 下没有自适应网络控制服务设置。

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)

注意：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

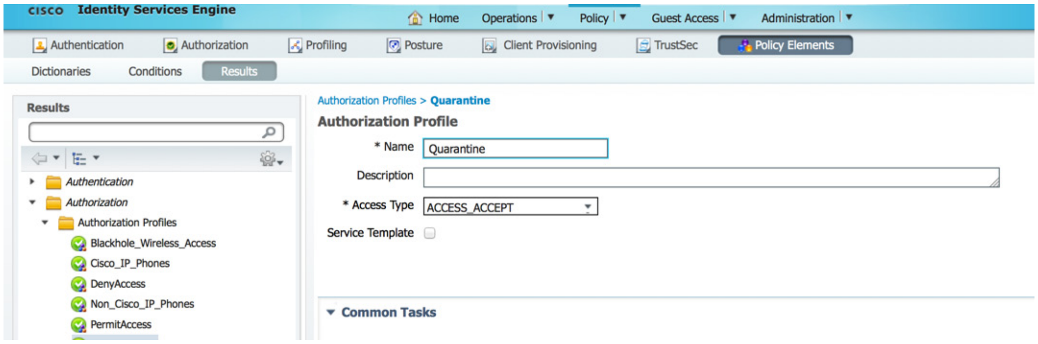


Endpoint Protection Service

Service Status ☑ Enabled

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)



Authorization Profiles > Quarantine

Authorization Profile

* Name Quarantine

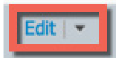
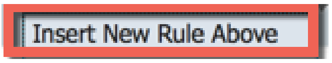
Description

* Access Type ACCESS_ACCEPT

Service Template □

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

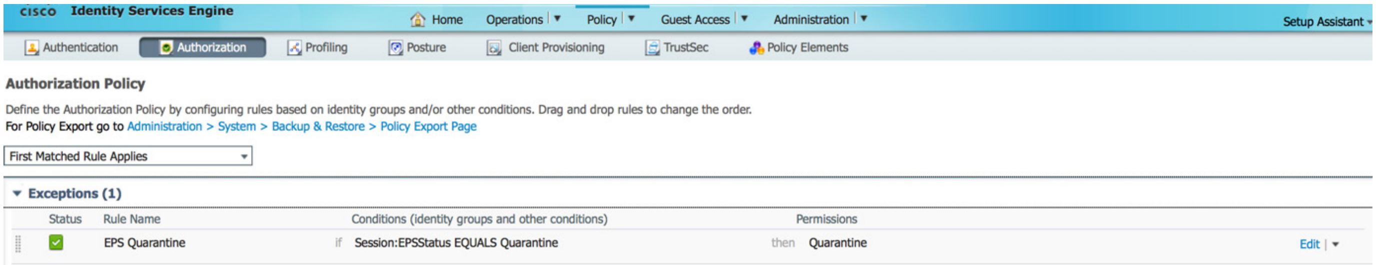
策略 (Policy)->授权 (Authorization)->例外 (Exceptions)->  Edit ▾ **->**  Insert New Rule Above 并输入以下内容：

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)**



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 ▾

▾ Exceptions (1)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	EPS Quarantine	if	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。

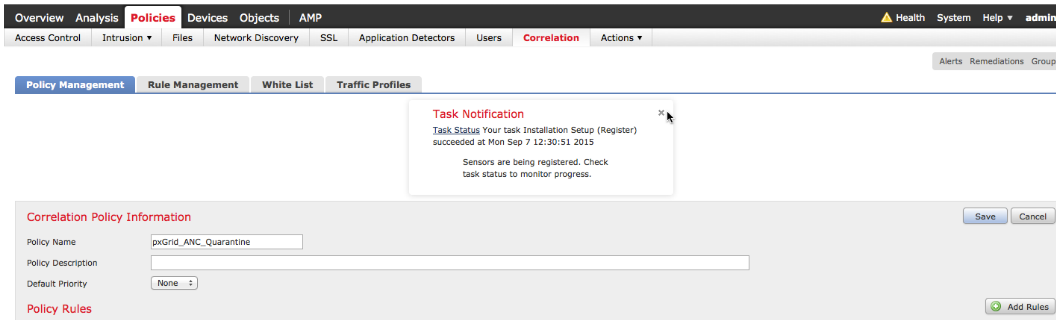
端口跳转、重新身份验证、端口关闭、终止策略将遵循同一流程。

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)



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

Policy Name: pxGrid_ANC_Quarantine

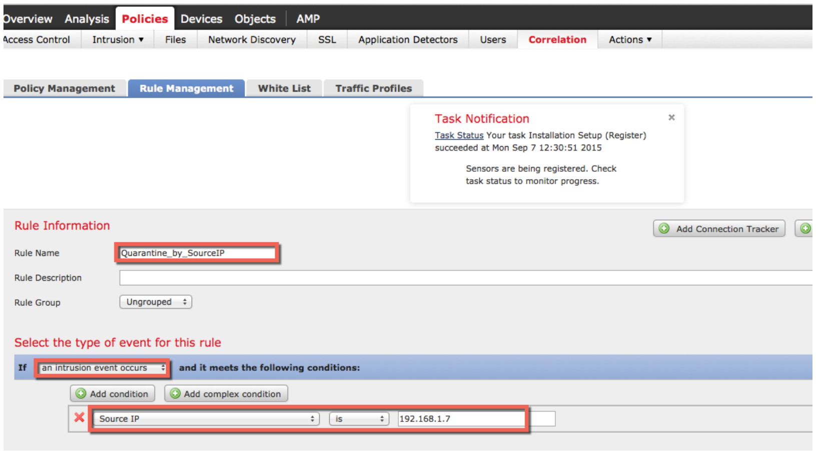
Policy Description:

Default Priority: None

Policy 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



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.

Rule Information

Rule Name: Quarantine_by_SourceIP

Rule Description:

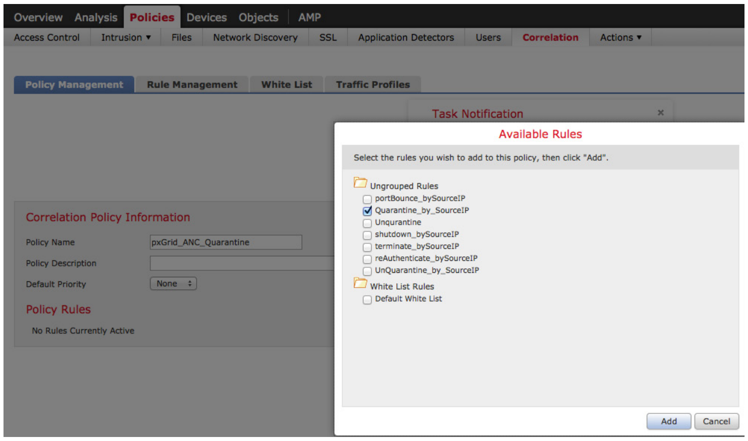
Rule Group: Ungrouped

Select the type of event for this rule

If an intrusion event occurs and it meets the following conditions:

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)



Available Rules

Select the rules you wish to add to this policy, then click "Add".

Ungrouped Rules
- □ portBounce_bySourceIP
- ☑ Quarantine_by_SourceIP
- □ Unqurantine
- □ shutdown_bySourceIP
- □ terminate_bySourceIP
- □ reAuthenticate_bySourceIP
- □ UnQuarantine_by_SourceIP

White List Rules
- □ Default White List

Correlation Policy Information

Policy Name: pxGrid_ANC_Quarantine

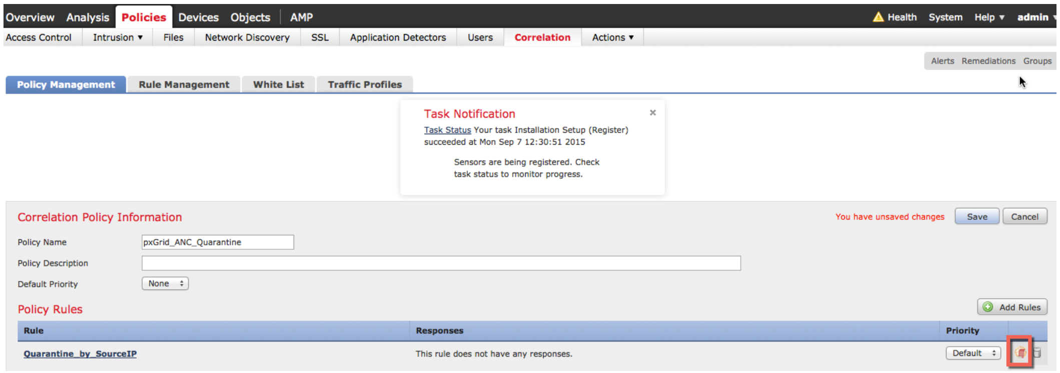
Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

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



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

Policy Name: pxGrid_ANC_Quarantine

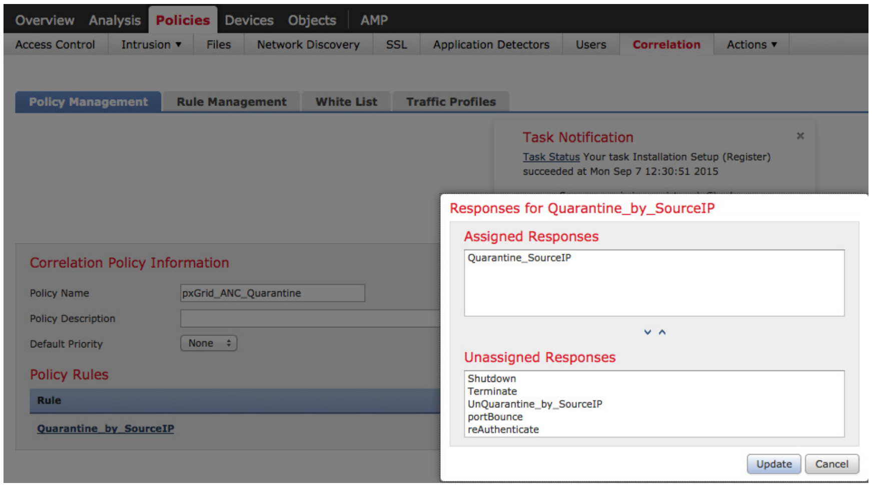
Policy Description:

Default Priority: None

Policy 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 ▾
Policy Management Rule Management White List Traffic Profiles
Update
Cancel

Task Notification

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

Correlation Policy Information

Policy Name: pxGrid_ANC_Quarantine

Policy Description:

Default Priority: None

Policy Rules

Rule

Quarantine_by_SourceIP

Responses for Quarantine_by_SourceIP

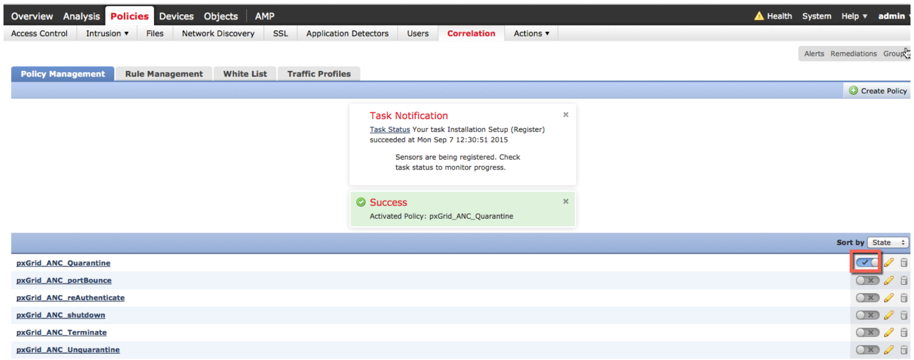
Assigned Responses

Quarantine_SourceIP

Unassigned Responses

Shutdown
Terminate
UnQuarantine_by_SourceIP
portBounce
reAuthenticate

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 Groups
Policy Management Rule Management White List Traffic Profiles
Create Policy
Sort by State

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

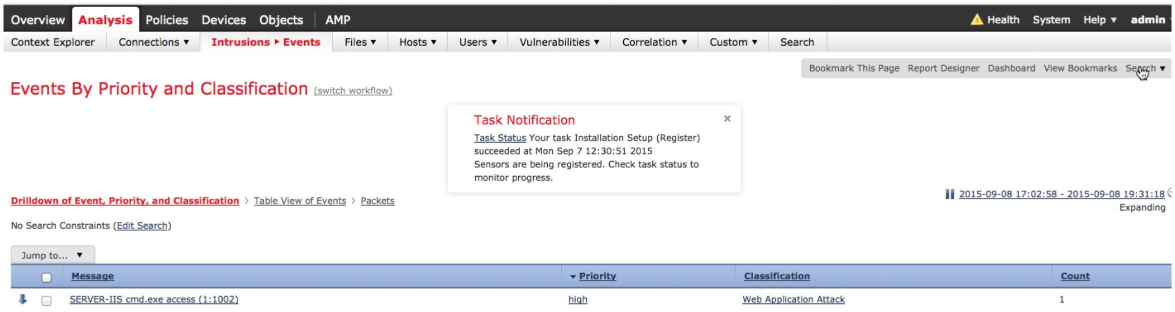
Activated Policy: pxGrid_ANC_Quarantine

pxGrid_ANC_Quarantine
pxGrid_ANC_portBounce
pxGrid_ANC_reAuthenticate
pxGrid_ANC_shutdown
pxGrid_ANC_Terminate
pxGrid_ANC_Unquarantine

测试

最终用户将在其浏览器窗口中键入 www.yahoo.com/cmd.exe，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 Analysis Policies Devices Objects AMP
Health System Help ▾ admin
Context Explorer Connections ▾ Intrusions ▸ Events Files ▾ Hosts ▾ Users ▾ Vulnerabilities ▾ Correlation ▾ Custom ▾ Search
Bookmark This Page Report Designer Dashboard View Bookmarks Search ▾
Jump to... ▾

Events By Priority and Classification (switch workflow)

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.

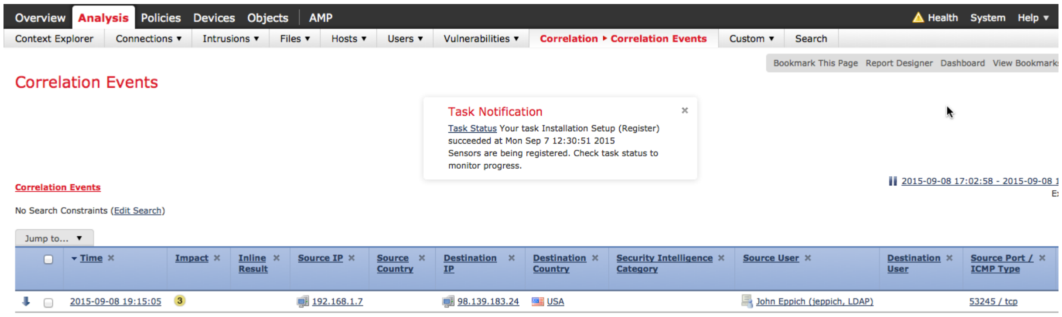
Drilldown of Event, Priority, and Classification > Table View of Events > Packets

2015-09-08 17:02:58 - 2015-09-08 19:31:18
Expanding

No Search Constraints (Edit Search)

	Message	▾ Priority	Classification	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。



Correlation Events

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.

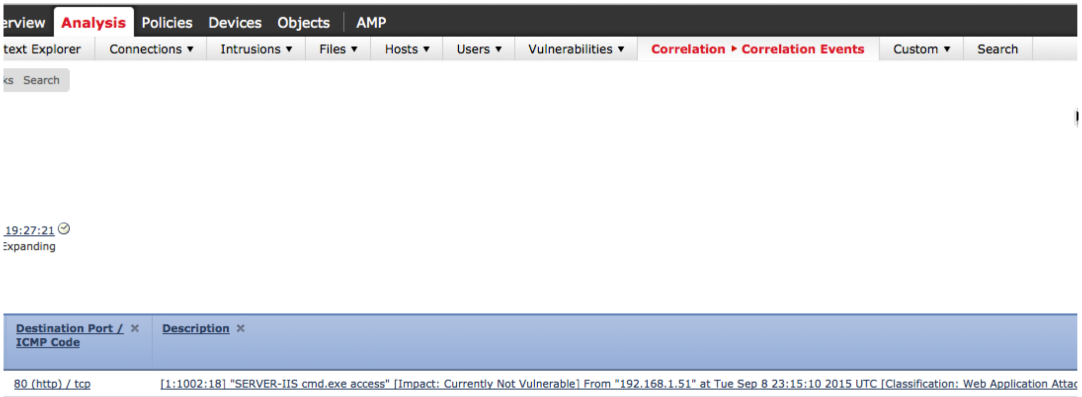
Correlation Events

2015-09-08 17:02:58 - 2015-09-08 1

No Search Constraints (Edit Search)

	Time	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Security Intelligence Category	Source User	Destination User	Source Port / ICMP Type
☐	2015-09-08 19:15:05	3		192.168.1.7		98.139.183.24	USA		John Eppich (jeppich, LDAP)		53245 / tcp

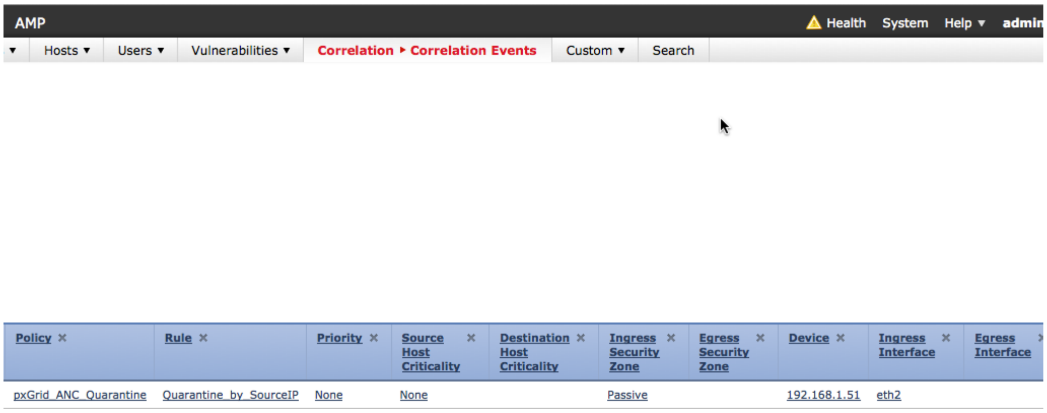
第 4 步： 随着我们继续处理同一事件
请注意目标端口和 pxGrid_Intrusion_Policy 规则中包含的规则违规。



19:27:21
Expanding

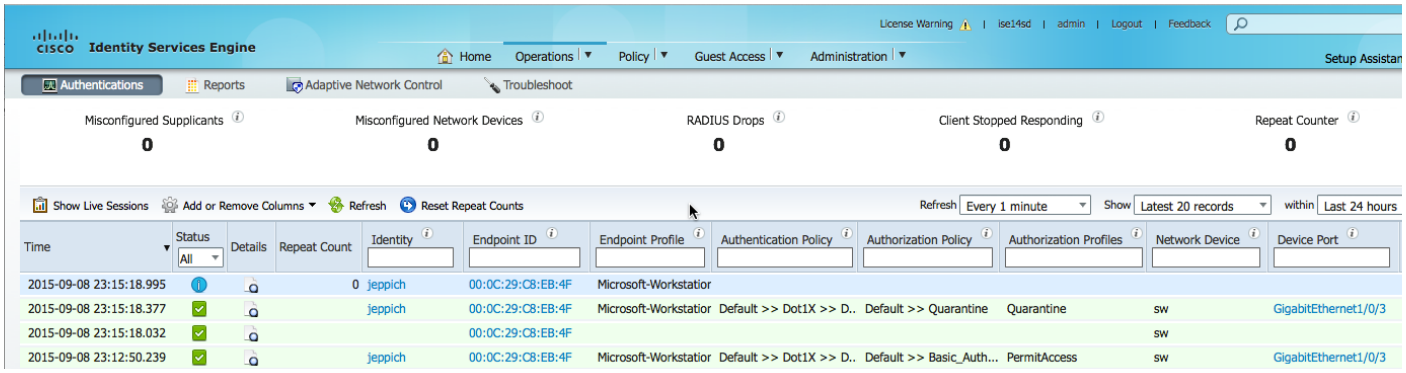
Destination Port / ICMP Code	Description
80 (http) / tcp	[1:1002:18] "SERVER-IIS cmd.exe access" [Impact: Currently Not Vulnerable] From "192.168.1.51" at Tue Sep 8 23:15:10 2015 UTC [Classification: Web Application Attac

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



Policy	Rule	Priority	Source Host Criticality	Destination Host Criticality	Ingress Security Zone	Egress Security Zone	Device	Ingress Interface	Egress Interface
pxGrid_ANC_Quarantine	Quarantine_by_SourceIP	None	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)



Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 0 | Client Stopped Responding 0 | Repeat Counter 0

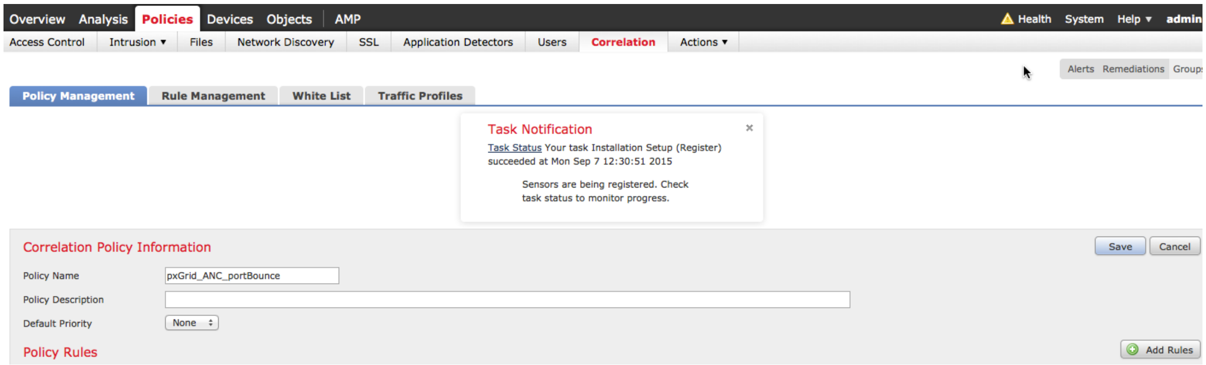
Refresh Every 1 minute | Show Latest 20 records | within Last 24 hours

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port
2015-09-08 23:15:18.995	ⓘ		0	jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior					
2015-09-08 23:15:18.377	✓			jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior	Default >> Dot1X >> D..	Default >> Quarantine	Quarantine	sw	GigabitEthernet1/0/3
2015-09-08 23:15:18.032	✓				00:0C:29:C8:EB:4F					sw	
2015-09-08 23:12:50.239	✓			jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior	Default >> Dot1X >> D..	Default >> Basic_Auth...	PermitAccess	sw	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)**



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

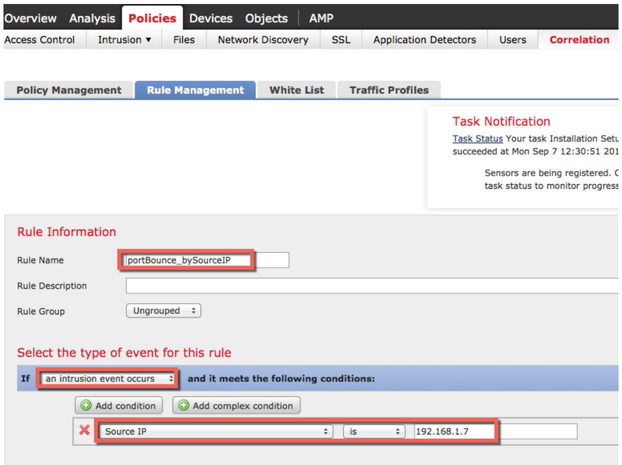
Policy Name: pxGrid_ANC_portBounce

Policy Description:

Default Priority: None

Policy 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)**



Task Notification

Task Status Your task Installation Setu
succeeded at Mon Sep 7 12:30:51 201

Sensors are being registered. C
task status to monitor progress

Rule Information

Rule Name: portBounce_bySourceIP

Rule Description:

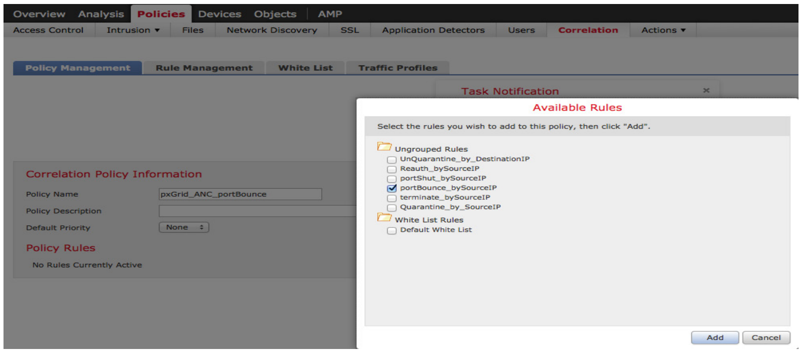
Rule Group: Ungrouped

Select the type of event for this rule

If an intrusion event occurs and it meets the following conditions:

Source IP is 192.168.1.7

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



Correlation Policy Information

Policy Name: pxGrid_ANC_portBounce

Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

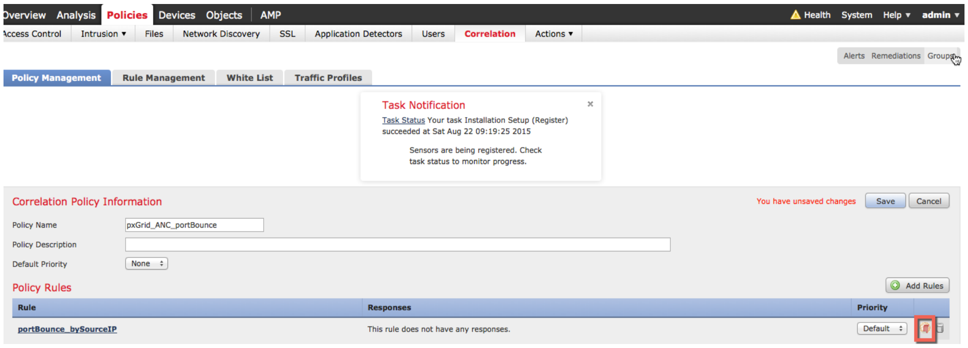
Available Rules

Select the rules you wish to add to this policy, then click "Add".

Ungrouped Rules
- □ UnQuarantine_by_DestinationIP
- □ Reauth_bySourceIP
- □ portShut_bySourceIP
- ☑ portBounce_bySourceIP
- □ terminate_bySourceIP
- □ Quarantine_by_SourceIP

White List Rules
- □ Default White List

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



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Sat Aug 22 09:19:25 2015

Sensors are being registered. Check task status to monitor progress.

Correlation Policy Information

You have unsaved changes

Policy Name: pxGrid_ANC_portBounce

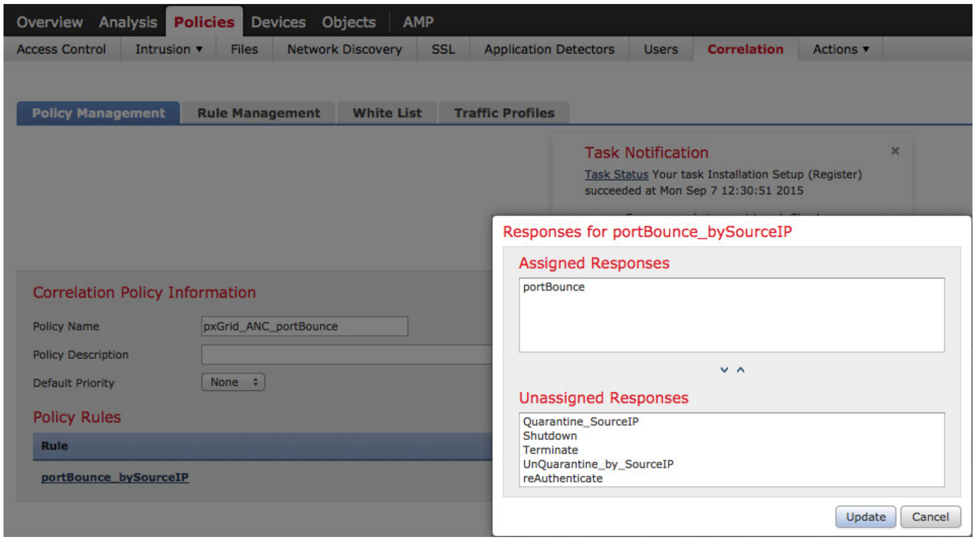
Policy Description:

Default Priority: None

Policy 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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

Correlation Policy Information

Policy Name: pxGrid_ANC_portBounce

Policy Description:

Default Priority: None

Policy Rules

Rule

portBounce_bySourceIP

Responses for portBounce_bySourceIP

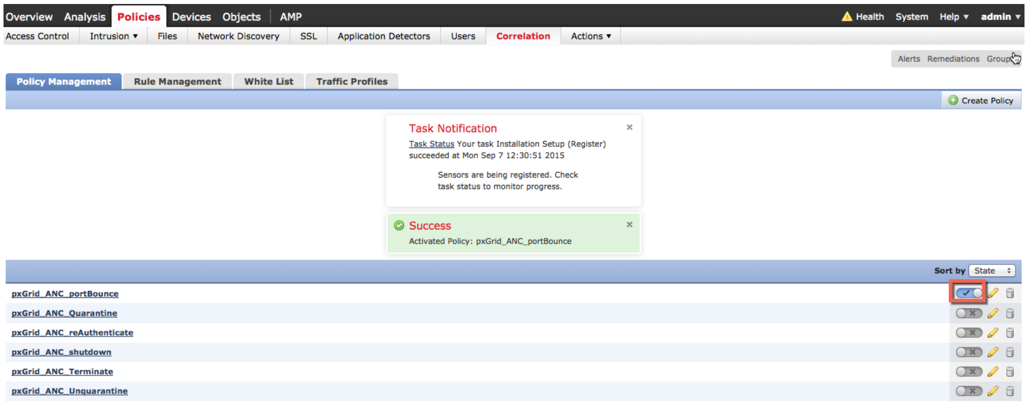
Assigned Responses

portBounce

Unassigned Responses

Quarantine_SourceIP
Shutdown
Terminate
UnQuarantine_by_SourceIP
reAuthenticate

第 6 步： 激活终止政策，点击将会打开该策略的以下**按钮**



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

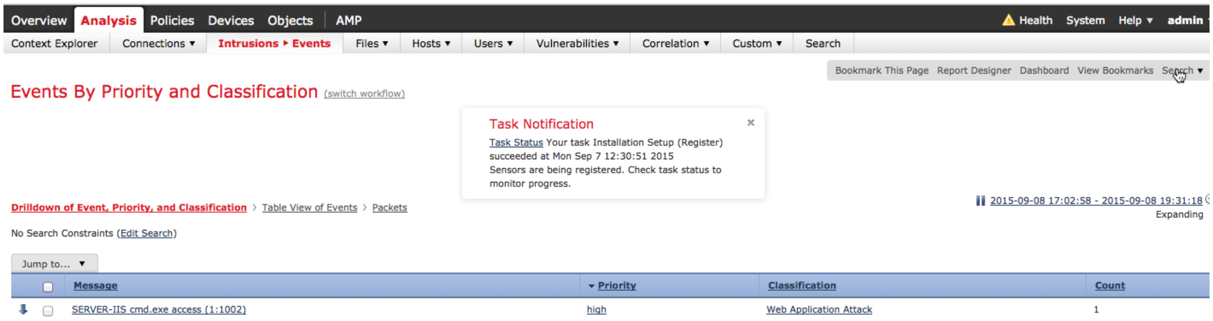
Activated Policy: pxGrid_ANC_portBounce

pxGrid_ANC_portBounce
pxGrid_ANC_Quarantine
pxGrid_ANC_reAuthenticate
pxGrid_ANC_shutdown
pxGrid_ANC_Terminate
pxGrid_ANC_Unquarantine

测试

最终用户将在其浏览器窗口中键入 www.yahoo.com/cmd.exe，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 www.yahoo.com/cmd.exe
第 2 步： 这将触发“Web 应用攻击”(Web Application Attack) 入侵事件



Events By Priority and Classification (switch workflow)

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.

Drilldown of Event, Priority, and Classification › Table View of Events › Packets

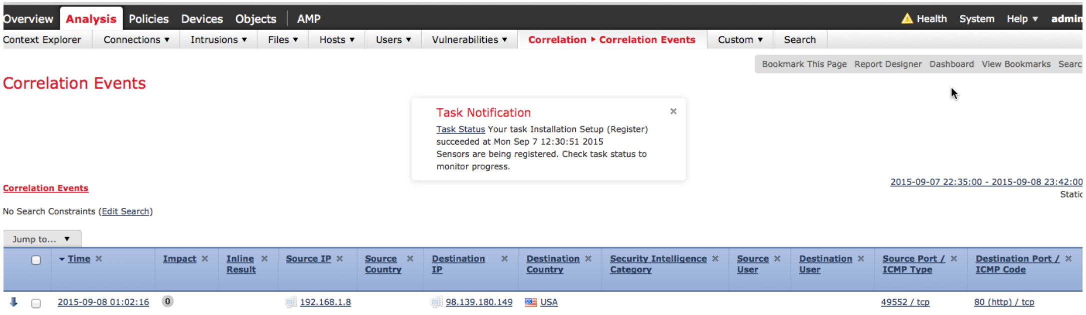
2015-09-08 17:02:58 - 2015-09-08 19:31:18
Expanding

No Search Constraints (Edit Search)

	□	Message	▾ Priority	Classification	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。

<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。



Correlation Events

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.

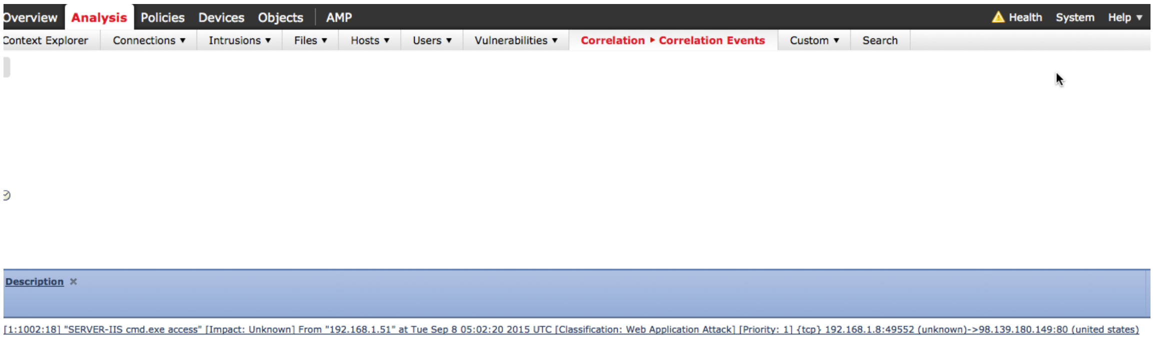
Correlation Events

2015-09-07 22:35:00 - 2015-09-08 23:42:00
Static

No Search Constraints (Edit Search)

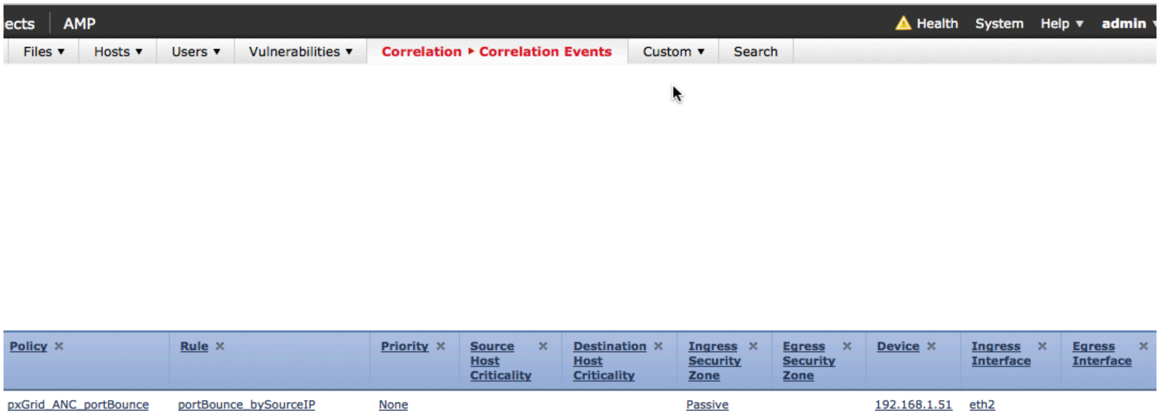
	□	▾ Time	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Security Intelligence Category	Source User	Destination User	Source Port / ICMP Type	Destination Port / ICMP Code
⬇	□	2015-09-08 01:02:16	0		192.168.1.8		98.139.180.149	USA				49552 / tcp	80 (http) / tcp

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。



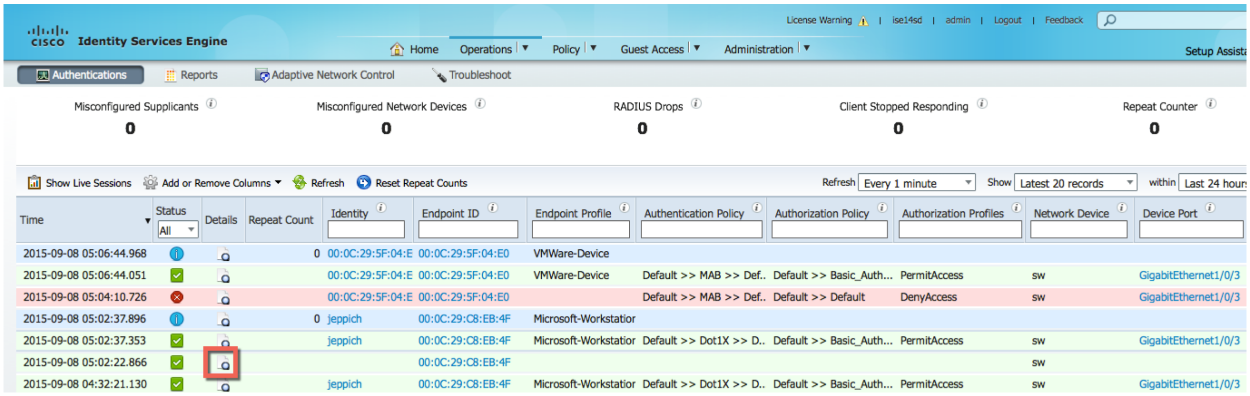
Description
[1:1002:18] "SERVER-IIS cmd.exe access" [Impact: Unknown] From "192.168.1.51" at Tue Sep 8 05:02:20 2015 UTC [Classification: Web Application Attack] [Priority: 1] {tcp} 192.168.1.8:49552 (unknown)->98.139.180.149:80 (united states)

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



Policy	Rule	Priority	Source Host Criticality	Destination Host Criticality	Ingress Security Zone	Egress Security Zone	Device	Ingress Interface	Egress Interface
pxGrid_ANC_portBounce	portBounce_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)**

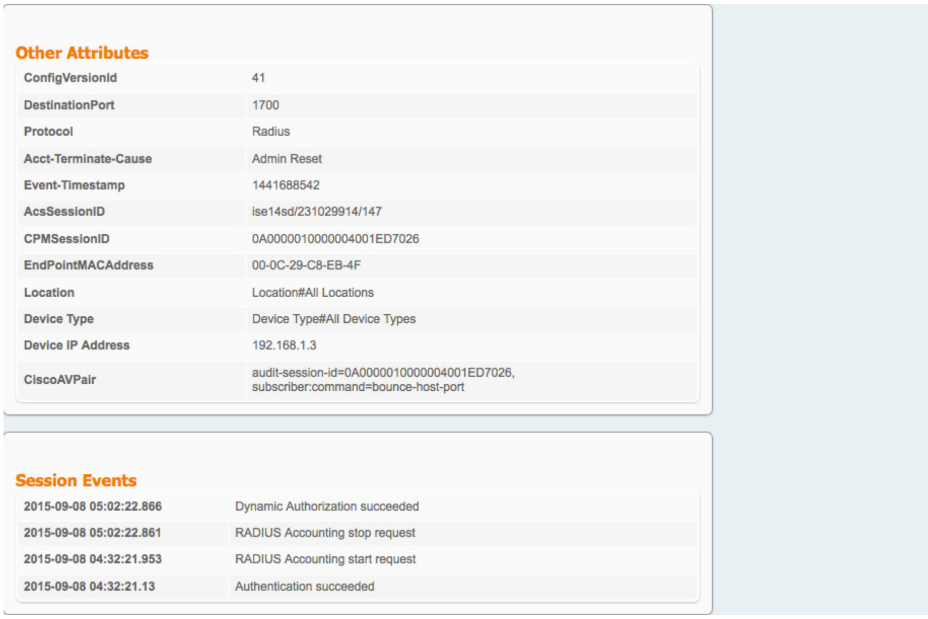


Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 0 | Client Stopped Responding 0 | Repeat Counter 0

Refresh: Every 1 minute | Show: Latest 20 records | within: Last 24 hours

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port
2015-09-08 05:06:44.968	ⓘ		0	00:0C:29:5F:04:E	00:0C:29:5F:04:E0	VMWare-Device					
2015-09-08 05:06:44.051	✓			00:0C:29:5F:04:E	00:0C:29:5F:04:E0	VMWare-Device	Default >> MAB >> Def..	Default >> Basic_Auth...	PermitAccess	sw	GigabitEthernet1/0/3
2015-09-08 05:04:10.726	☒			00:0C:29:5F:04:E	00:0C:29:5F:04:E0		Default >> MAB >> Def..	Default >> Default	DenyAccess	sw	GigabitEthernet1/0/3
2015-09-08 05:02:37.896	ⓘ		0	jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior					
2015-09-08 05:02:37.353	✓			jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior	Default >> Dot1X >> 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..	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



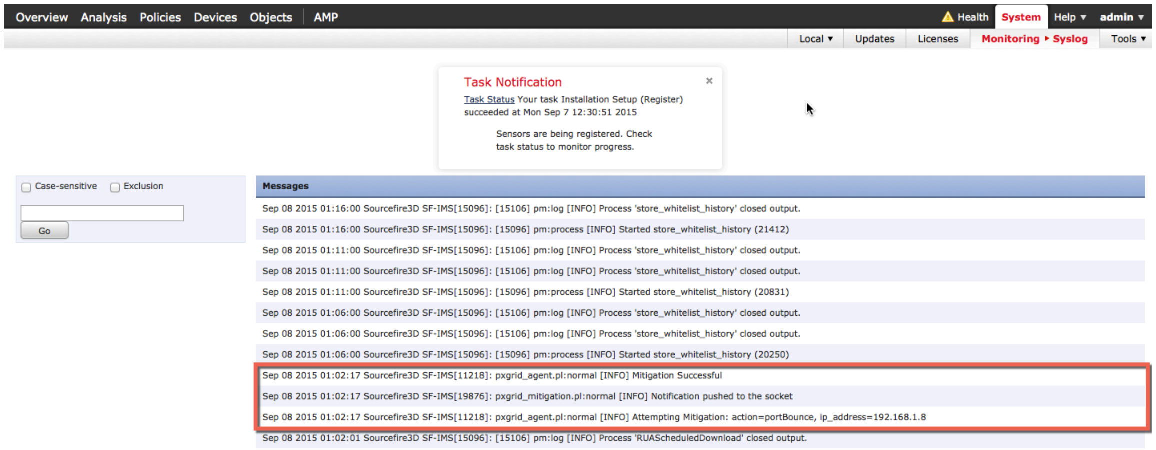
Other Attributes

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

Session 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
2015-09-08 04:32:21.13	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跳转缓解操作是否成功



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.

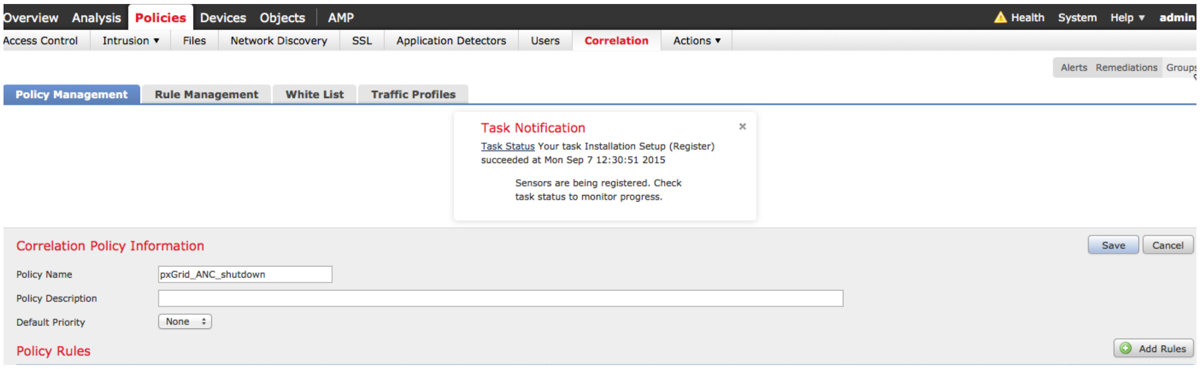
Messages

```
Sep 08 2015 01:16:00 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_history' closed output.
Sep 08 2015 01:16:00 Sourcefire3D SF-IMS[15096]: [15096] pm:process [INFO] Started store_whitelist_history (21412)
Sep 08 2015 01:11:00 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_history' closed output.
Sep 08 2015 01:11:00 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_history' closed output.
Sep 08 2015 01:11:00 Sourcefire3D SF-IMS[15096]: [15096] pm:process [INFO] Started store_whitelist_history (20831)
Sep 08 2015 01:06:00 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_history' closed output.
Sep 08 2015 01:06:00 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_history' closed output.
Sep 08 2015 01:06:00 Sourcefire3D SF-IMS[15096]: [15096] pm:process [INFO] Started store_whitelist_history (20250)
Sep 08 2015 01:02:17 Sourcefire3D SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Mitigation Successful
Sep 08 2015 01:02:17 Sourcefire3D SF-IMS[19876]: pxgrid_mitigation.pl:normal [INFO] Notification pushed to the socket
Sep 08 2015 01:02:17 Sourcefire3D SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Attempting Mitigation: action=portBounce, ip_address=192.168.1.8
Sep 08 2015 01:02:01 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'RUAScheduledDownload' 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)**



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

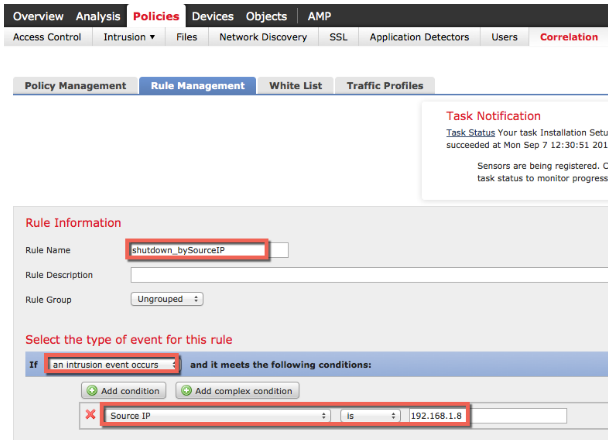
Policy Name: pxGrid_ANC_shutdown

Policy Description:

Default Priority: None

Policy 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)**



Task Notification

Task Status Your task Installation Setu succeeded at Mon Sep 7 12:30:51 201

Sensors are being registered. C task status to monitor progress

Rule Information

Rule Name: shutdown_bySourceIP

Rule Description:

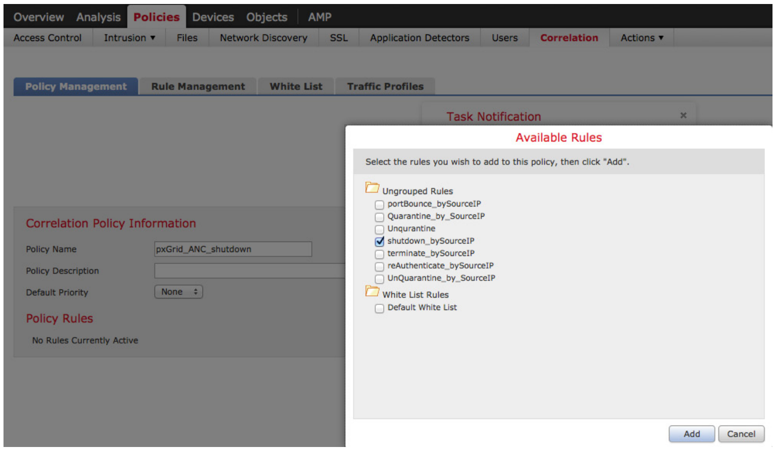
Rule Group: Ungrouped

Select the type of event for this rule

If an intrusion event occurs and it meets the following conditions:

Source IP is 192.168.1.8

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**



Correlation Policy Information

Policy Name: pxGrid_ANC_shutdown

Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

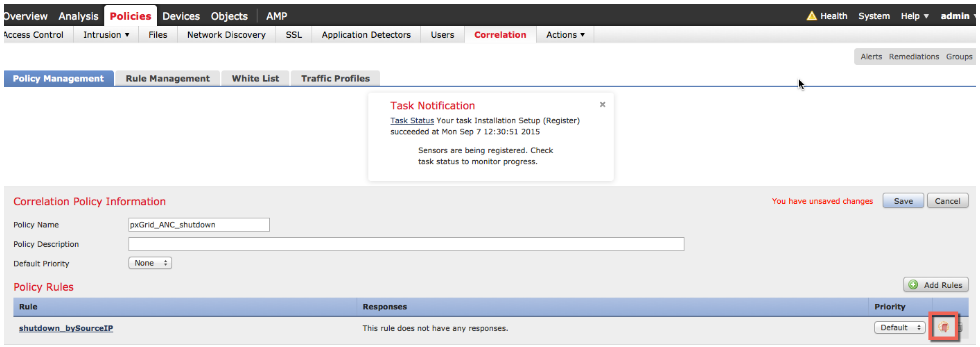
Available Rules

Select the rules you wish to add to this policy, then click "Add".

Ungrouped Rules
- ☐ portBounce_bySourceIP
- ☐ Quarantine_by_SourceIP
- ☐ Unquarantine
- ☑ shutdown_bySourceIP
- ☐ terminate_bySourceIP
- ☐ reAuthenticate_bySourceIP
- ☐ UnQuarantine_by_SourceIP

White List Rules
- ☐ Default White List

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



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

Policy Name: pxGrid_ANC_shutdown

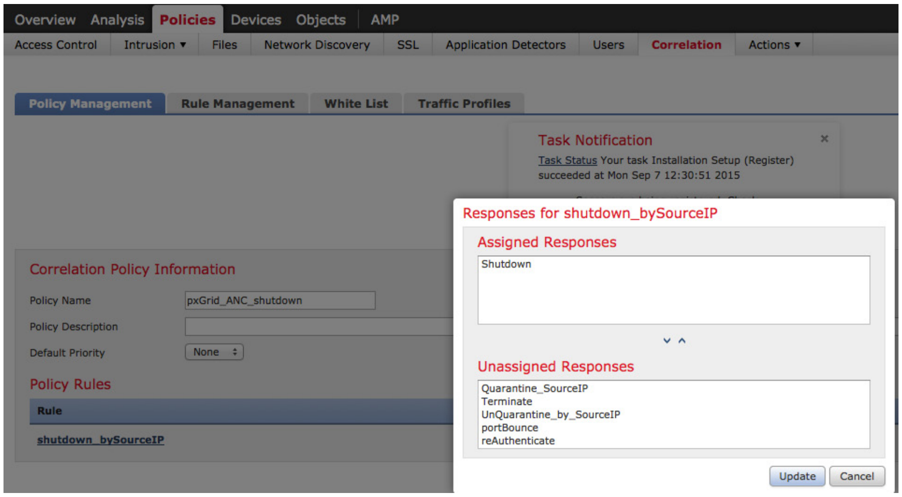
Policy Description:

Default Priority: None

Policy Rules

Rule	Responses	Priority
shutdown_bySourceIP	This rule does not have any responses.	Default

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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

Responses for shutdown_bySourceIP

Assigned Responses

Shutdown

Unassigned Responses

Quarantine_SourceIP
Terminate
UnQuarantine_by_SourceIP
portBounce
reAuthenticate

Correlation Policy Information

Policy Name: pxGrid_ANC_shutdown

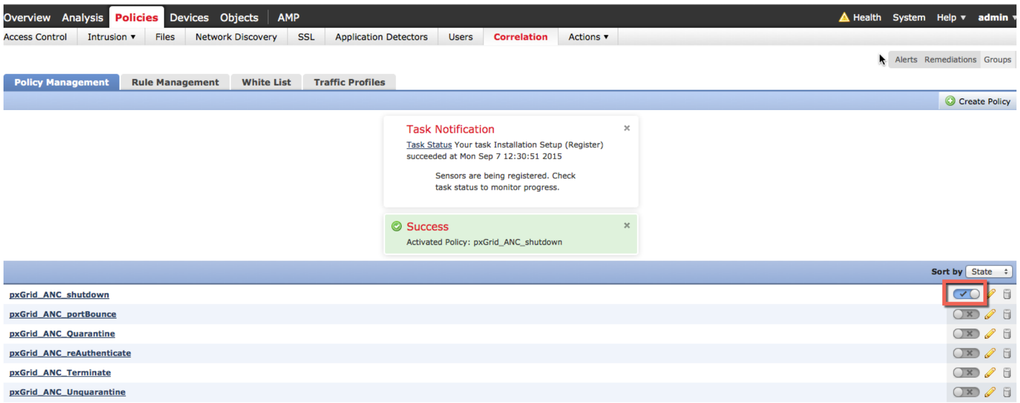
Policy Description:

Default Priority: None

Policy Rules

Rule
shutdown_bySourceIP

第 6 步： 激活终止政策，点击将会打开该策略的以下**按钮**



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_shutdown

Sort by State

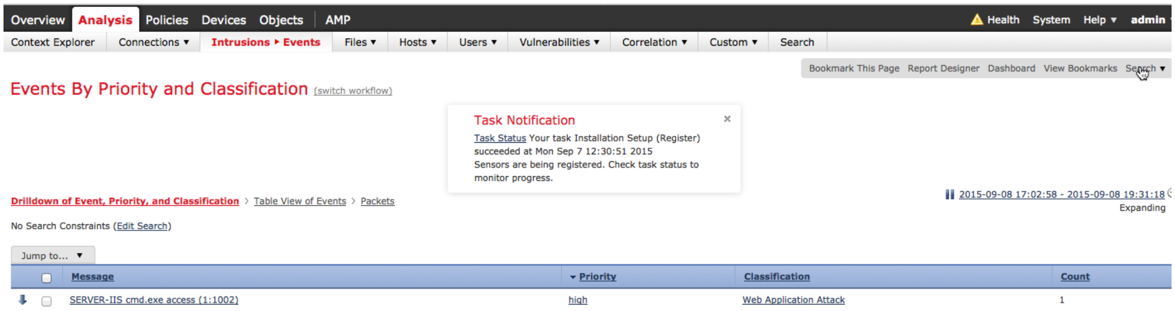
pxGrid_ANC_shutdown ✓
pxGrid_ANC_portBounce ✕
pxGrid_ANC_Quarantine ✕
pxGrid_ANC_reAuthenticate ✕
pxGrid_ANC_Terminate ✕
pxGrid_ANC_Unquarantine ✕

测试

最终用户将在其浏览器窗口中键入 www.yahoo.com/cmd.exe，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 www.yahoo.com/cmd.exe

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



Events By Priority and Classification (switch workflow)

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.

Drilldown of Event, Priority, and Classification › Table View of Events › Packets

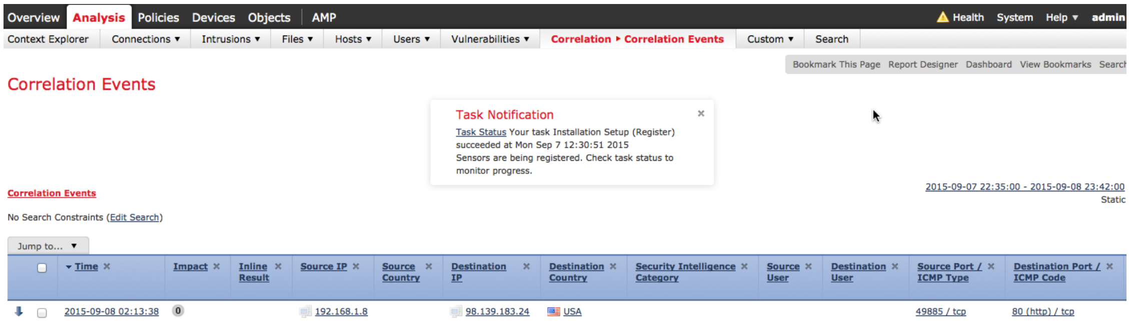
2015-09-08 17:02:58 - 2015-09-08 19:31:18
Expanding

No Search Constraints (Edit Search)

	☐	Message	▾ Priority	Classification	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。



Correlation Events

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.

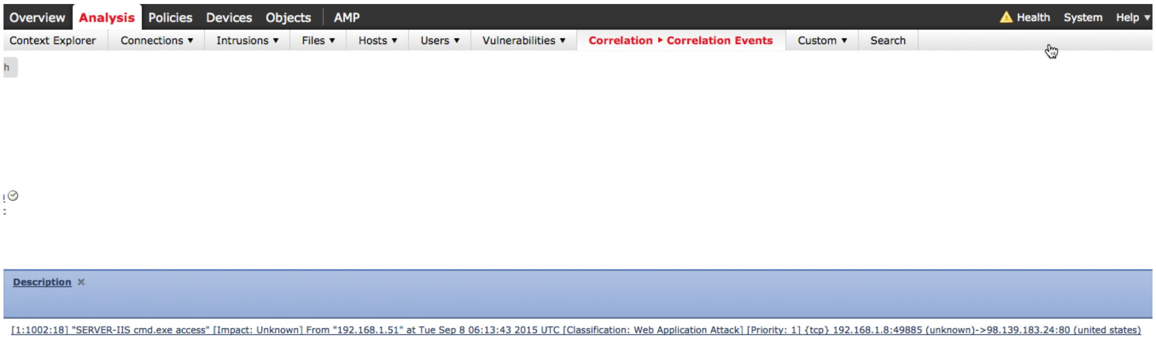
Correlation Events

2015-09-07 22:35:00 - 2015-09-08 23:42:00
Static

No Search Constraints (Edit Search)

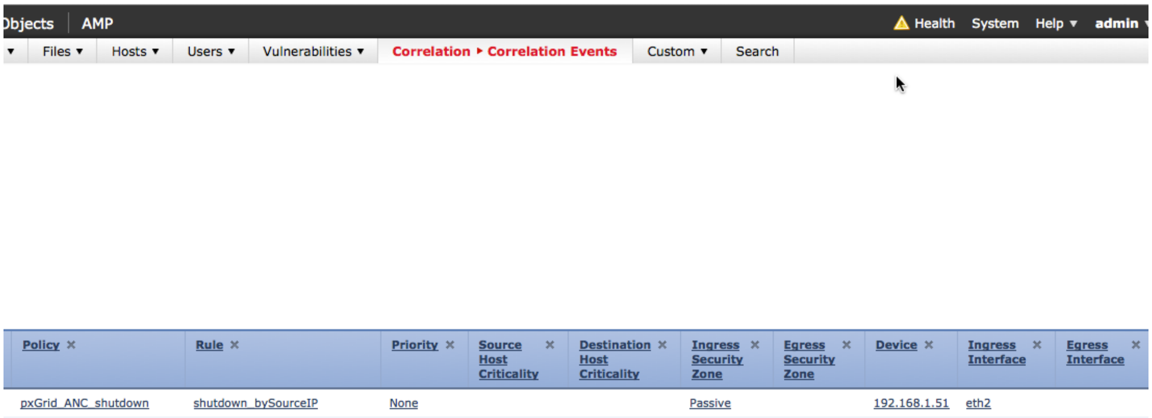
	☐	▾ Time ×	Impact ×	Inline Result ×	Source IP ×	Source Country ×	Destination IP ×	Destination Country ×	Security Intelligence Category ×	Source User ×	Destination User ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×
⬇	☐	2015-09-08 02:13:38	0		192.168.1.8		98.139.183.24	USA				49885 / tcp	80 (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。



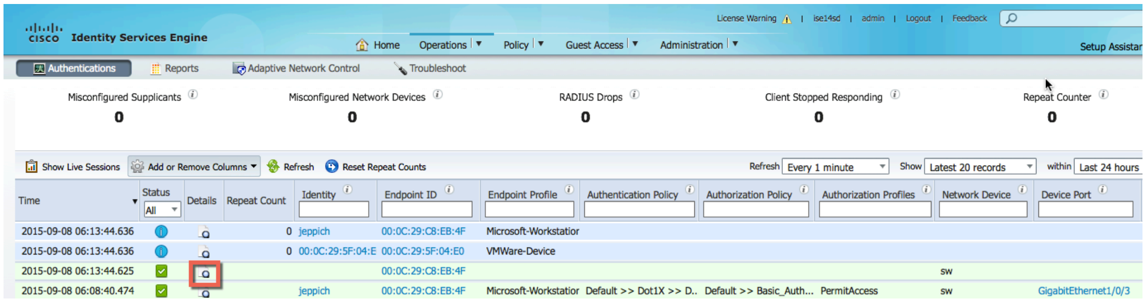
Description ×
[1:1002:18] "SERVER-IIS cmd.exe access" [Impact: Unknown] From "192.168.1.51" at Tue Sep 8 06:13:43 2015 UTC [Classification: Web Application Attack] [Priority: 1] {tcp} 192.168.1.8:49885 (unknown)->98.139.183.24:80 (united states)

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



Policy ✕	Rule ✕	Priority ✕	Source Host Criticality ✕	Destination Host Criticality ✕	Ingress Security Zone ✕	Egress Security Zone ✕	Device ✕	Ingress Interface ✕	Egress Interface ✕
pxGrid_ANC_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)**

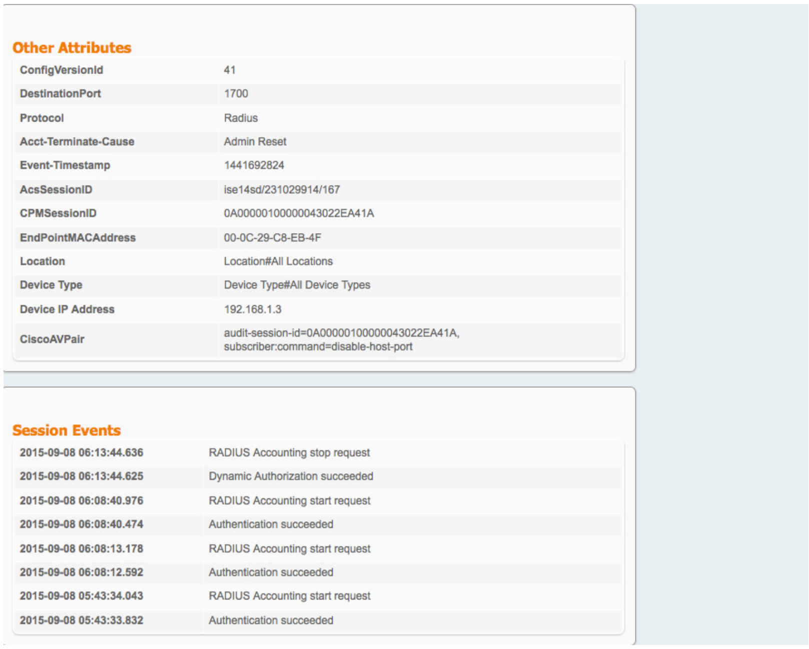


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Every 1 minute Show Latest 20 records within Last 24 hours

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	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



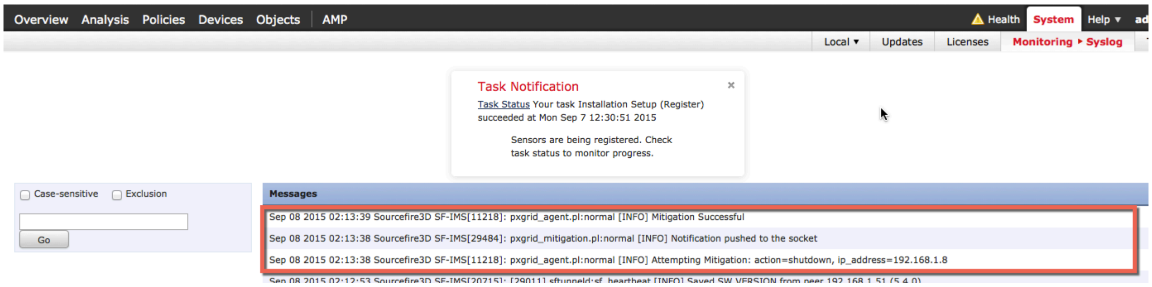
Other Attributes

ConfigVersionId	41
DestinationPort	1700
Protocol	Radius
Acct-Terminate-Cause	Admin Reset
Event-Timestamp	1441692824
AcsSessionID	ise14sd/231029914/167
CPMSessionID	0A00000100000043022EA41A
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=0A00000100000043022EA41A, subscriber:command=disable-host-port

Session Events

2015-09-08 06:13:44.636	RADIUS Accounting stop request
2015-09-08 06:13:44.625	Dynamic Authorization succeeded
2015-09-08 06:08:40.976	RADIUS Accounting start request
2015-09-08 06:08:40.474	Authentication succeeded
2015-09-08 06:08:13.178	RADIUS Accounting start request
2015-09-08 06:08:12.592	Authentication succeeded
2015-09-08 05:43:34.043	RADIUS Accounting start request
2015-09-08 05:43:33.832	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



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.

```
Sep 08 2015 02:13:39 Sourcefire3D SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Mitigation Successful
Sep 08 2015 02:13:38 Sourcefire3D SF-IMS[29484]: pxgrid_mitigation.pl:normal [INFO] Notification pushed to the socket
Sep 08 2015 02:13:38 Sourcefire3D SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Attempting Mitigation: action=shutdown, ip_address=192.168.1.8
Sep 08 2015 02:12:53 Sourcefire3D SF-IMS[20715]: [29011] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer 192.168.1.51 (5.4.0)
```

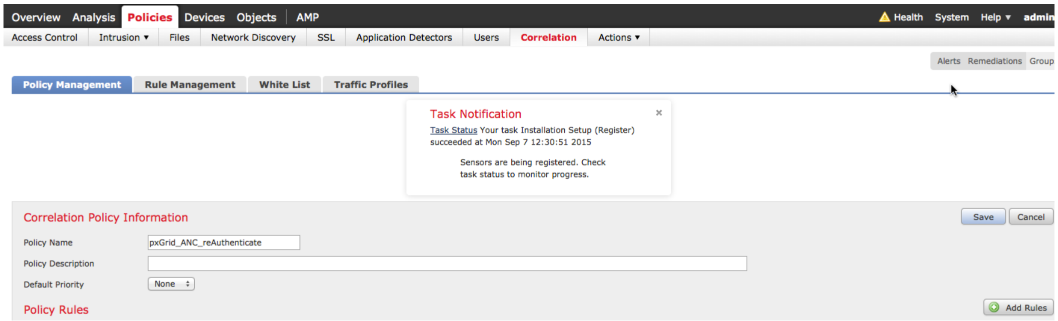
第 9 步： 此外，在交换机上，您将在端口上看到“shutdown”

```
interface GigabitEthernet1/0/3
 description internal LAN
 switchport mode access
 shutdown
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication fallback mab
 mab
```

重新身份验证

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)



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

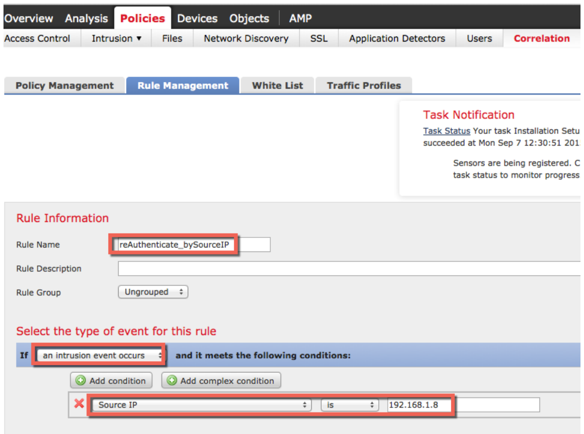
Policy Name: pxGrid_ANC_reAuthenticate

Policy Description:

Default Priority: None

Policy 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 AMP
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation
Policy Management Rule Management White List Traffic Profiles

Task Notification
Task Status Your task Installation Setu
succeeded at Mon Sep 7 12:30:51 201
Sensors are being registered. C
task status to monitor progress

Rule Information

Rule Name: reAuthenticate_bySourceIP

Rule Description:

Rule Group: Ungrouped

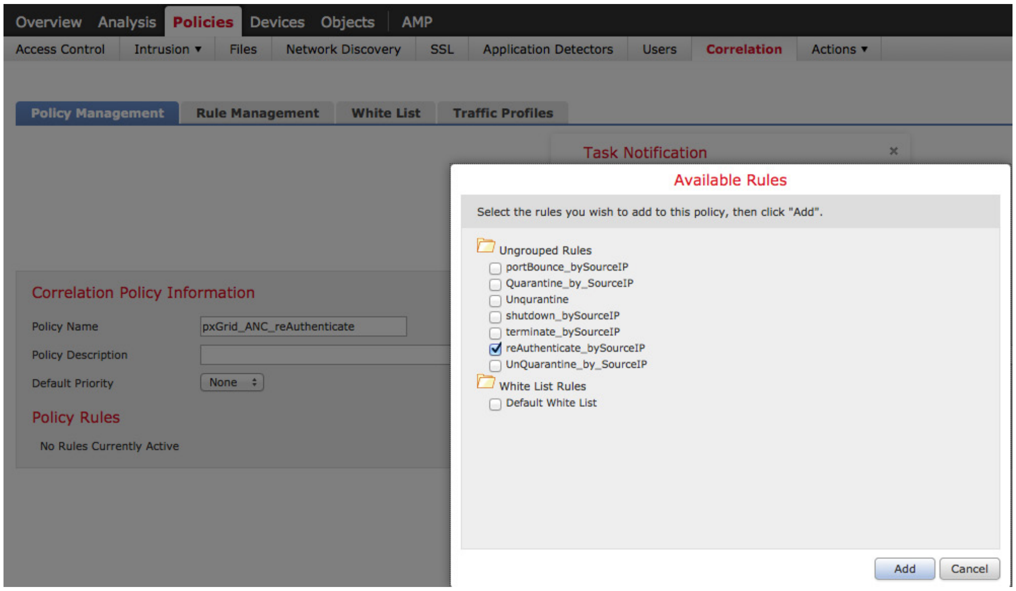
Select the type of event for this rule

If an intrusion event occurs and it meets the following 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


Overview Analysis Policies Devices Objects AMP
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▾
Policy Management Rule Management White List Traffic Profiles
Task Notification ×

Correlation Policy Information

Policy Name: pxGrid_ANC_reAuthenticate

Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

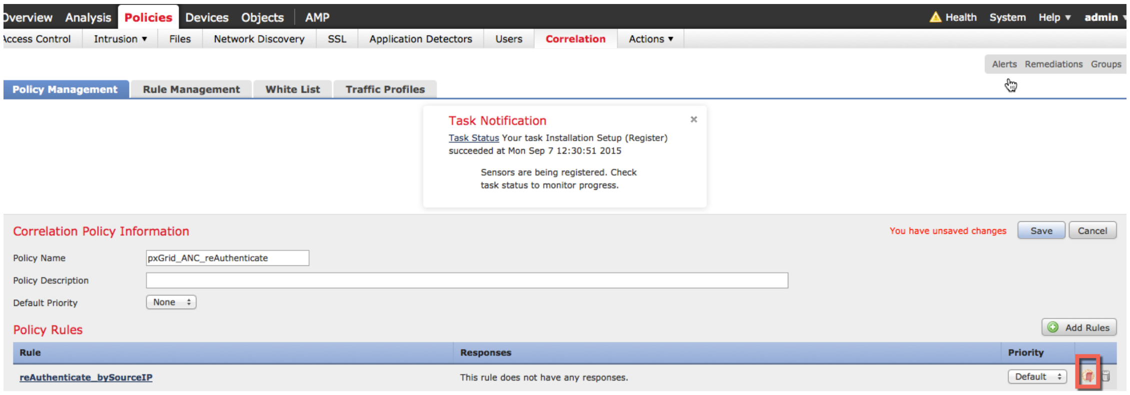
Available Rules

Select the rules you wish to add to this policy, then click "Add".

Ungrouped Rules
- ☐ portBounce_bySourceIP
- ☐ Quarantine_by_SourceIP
- ☐ Unqurantine
- ☐ shutdown_bySourceIP
- ☐ terminate_bySourceIP
- ☑ reAuthenticate_bySourceIP
- ☐ UnQuarantine_by_SourceIP

White List Rules
- ☐ Default White List

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
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

Policy Name: pxGrid_ANC_reAuthenticate

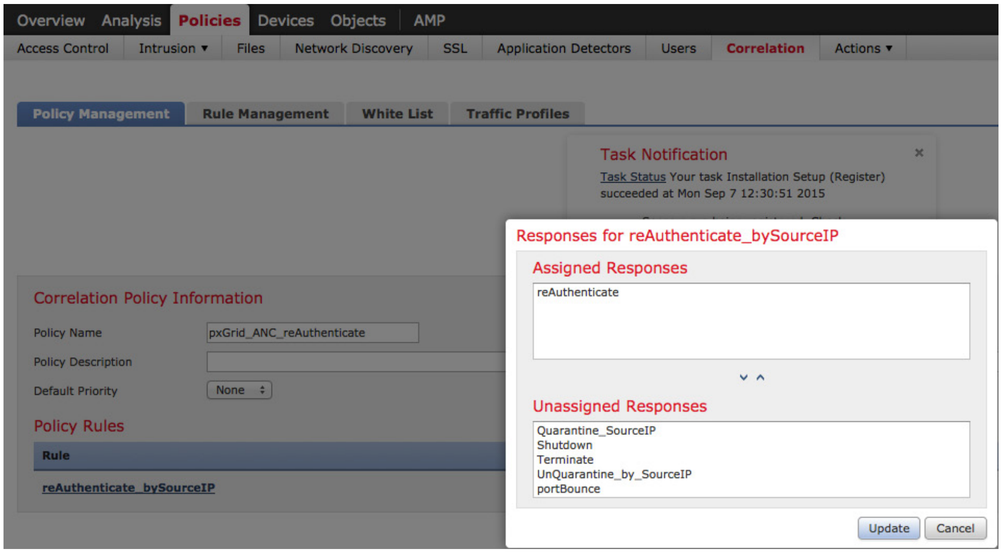
Policy Description:

Default Priority: None

Policy 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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

Correlation Policy Information

Policy Name: pxGrid_ANC_reAuthenticate

Policy Description:

Default Priority: None

Policy Rules

Rule

reAuthenticate_bySourceIP

Responses for reAuthenticate_bySourceIP

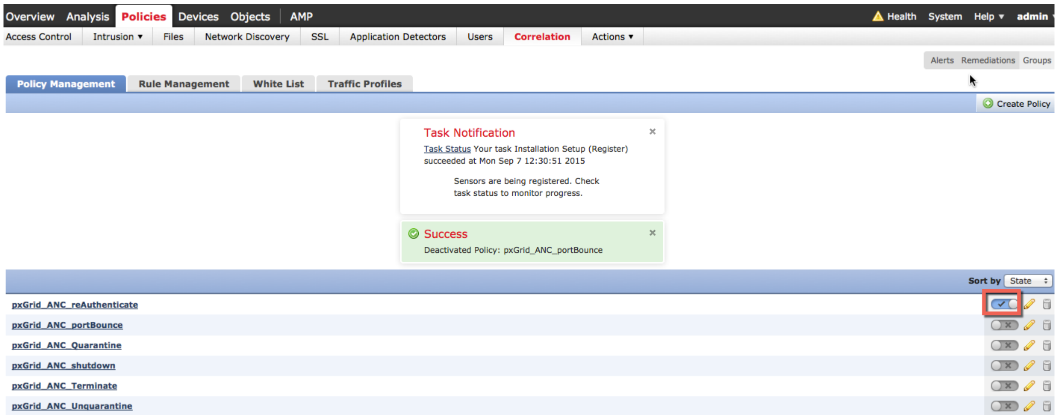
Assigned Responses

reAuthenticate

Unassigned Responses

Quarantine_SourceIP
Shutdown
Terminate
UnQuarantine_by_SourceIP
portBounce

第 6 步： 激活终止政策，点击将会打开该策略的以下**按钮**



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

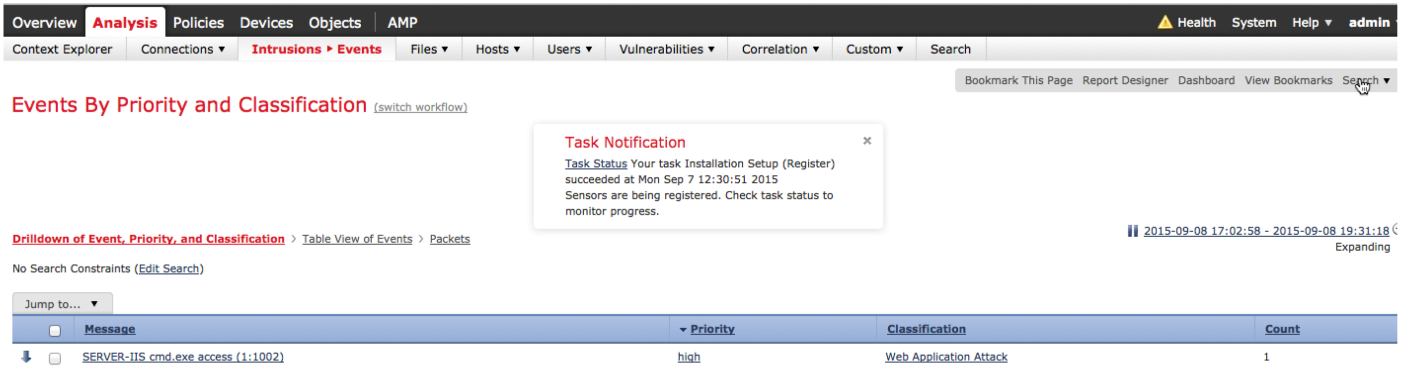
Deactivated Policy: pxGrid_ANC_portBounce

pxGrid_ANC_reAuthenticate
pxGrid_ANC_portBounce
pxGrid_ANC_Quarantine
pxGrid_ANC_shutdown
pxGrid_ANC_Terminate
pxGrid_ANC_Unquarantine

测试

最终用户将在其浏览器窗口中键入 www.yahoo.com/cmd.exe，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 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 Analysis Policies Devices Objects AMP
Health System Help ▾ admin
Context Explorer Connections ▾ Intrusions ▸ Events Files ▾ Hosts ▾ Users ▾ Vulnerabilities ▾ Correlation ▾ Custom ▾ Search
Bookmark This Page Report Designer Dashboard View Bookmarks Search ▾

Events By Priority and Classification (switch workflow)

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.

Drilldown of Event, Priority, and Classification › Table View of Events › Packets

2015-09-08 17:02:58 - 2015-09-08 19:31:18
Expanding

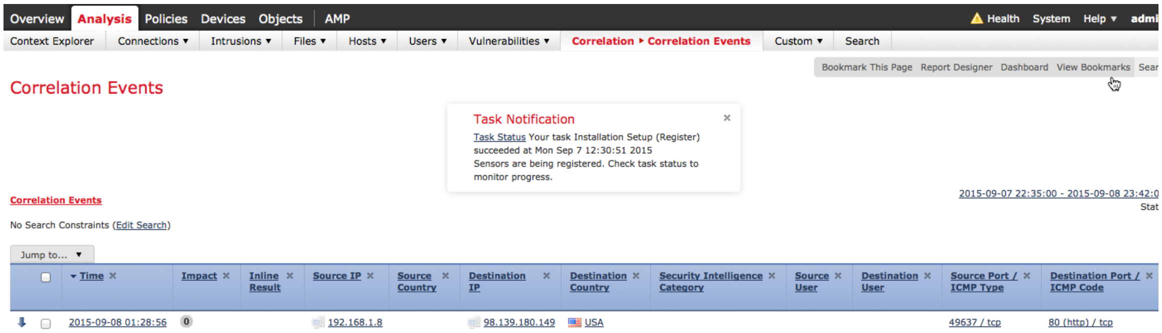
No Search Constraints (Edit Search)

Jump to... ▾

		Message	▾ Priority	Classification	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 地址的最终用户将重新进行身份验证。

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 Policies Devices Objects AMP
Health System Help ▾ admi
Context Explorer Connections ▾ Intrusions ▾ Files ▾ Hosts ▾ Users ▾ Vulnerabilities ▾ Correlation ▸ Correlation Events Custom ▾ Search
Bookmark This Page Report Designer Dashboard View Bookmarks Sear

Correlation Events

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 Events

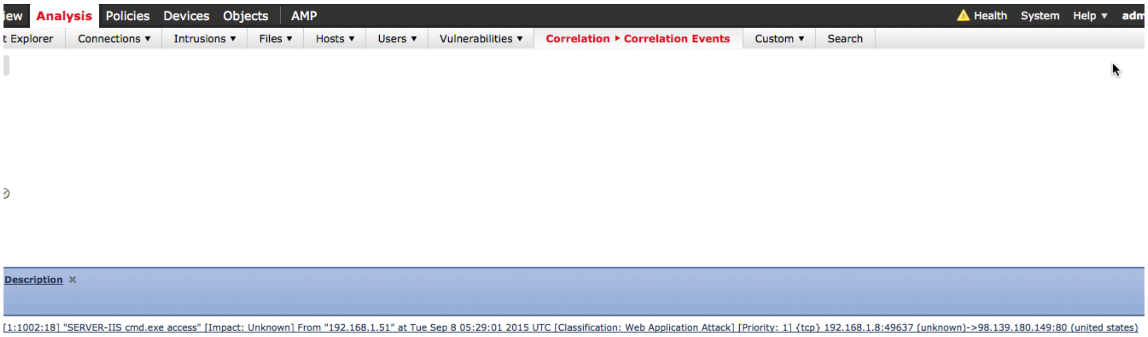
2015-09-07 22:35:00 - 2015-09-08 23:42:0
Stat

No Search Constraints (Edit Search)

Jump to... ▾

		▾ Time ×	Impact ×	Inline Result ×	Source IP ×	Source Country ×	Destination IP ×	Destination Country ×	Security Intelligence Category ×	Source User ×	Destination User ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×
⬇	□	2015-09-08 01:28:56	0		192.168.1.8		98.139.180.149	USA				49637 / tcp	80 (http) / tcp

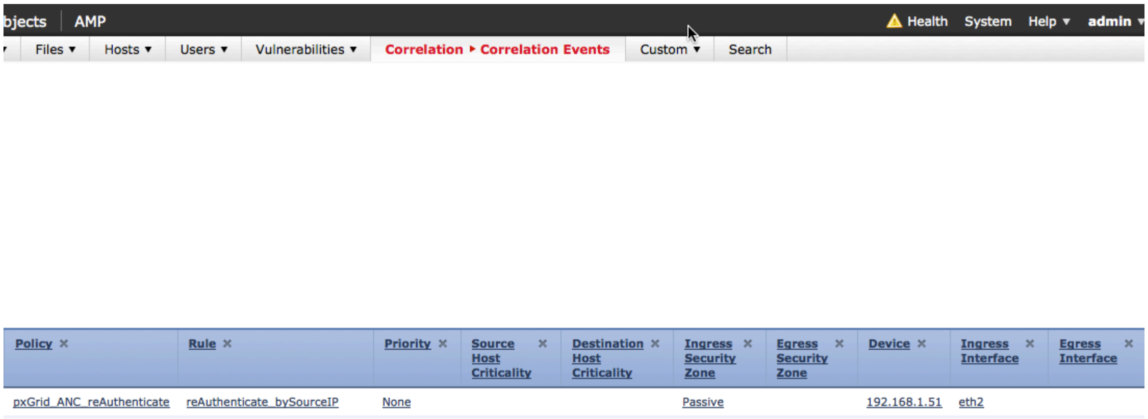
第 4 步： 随着我们继续处理同一事件
请注意 pxGrid_Intrusion_Policy 规则中包含的规则违规。


iew Analysis Policies Devices Objects AMP
Health System Help ▾ adm
t Explorer Connections ▾ Intrusions ▾ Files ▾ Hosts ▾ Users ▾ Vulnerabilities ▾ Correlation ▸ Correlation Events Custom ▾ Search

Description ×

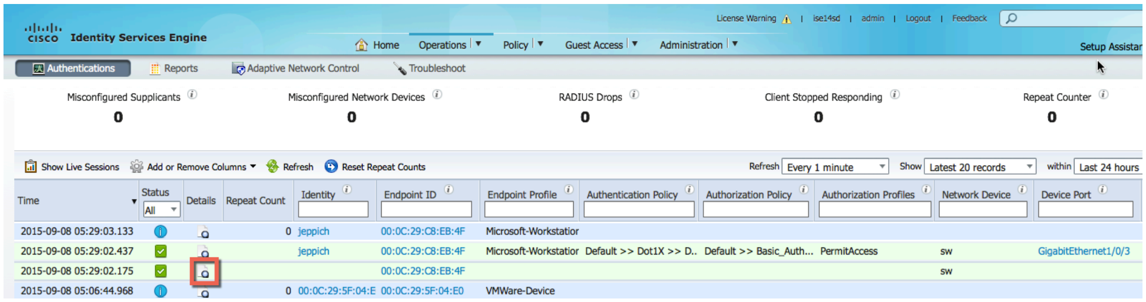
[1:1002:18] "SERVER-IIS cmd.exe access" [Impact: Unknown] From "192.168.1.51" at Tue Sep 8 05:29:01 2015 UTC [Classification: Web Application Attack] [Priority: 1] {tcp} 192.168.1.8:49637 (unknown)->98.139.180.149:80 (united states)

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重新身份验证缓解响应的关联策略和关联规则



Policy	Rule	Priority	Source Host Criticality	Destination Host Criticality	Ingress Security Zone	Egress Security Zone	Device	Ingress Interface	Egress Interface
pxGrid_ANC_reAuthenticate	reAuthenticate_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)**

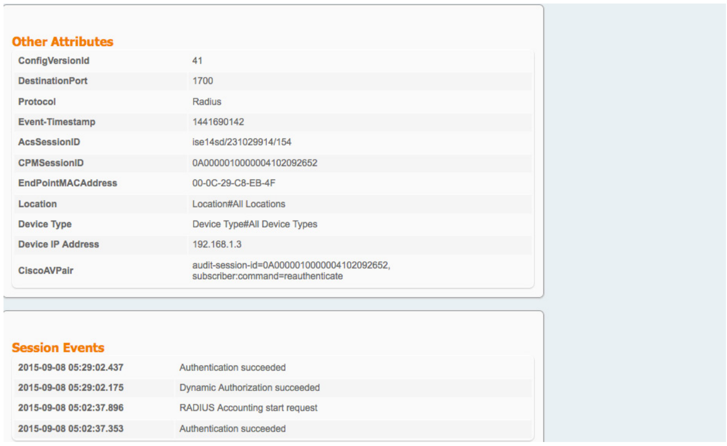


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Every 1 minute　Show: Latest 20 records　within: Last 24 hours

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	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					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



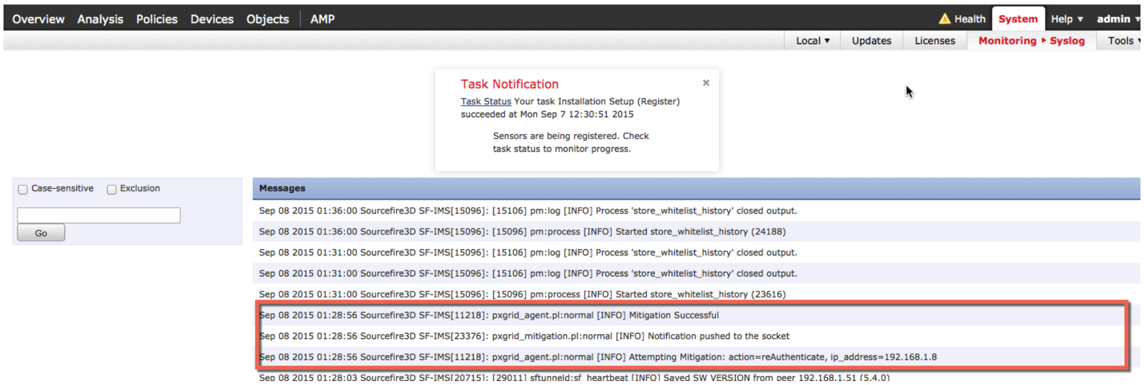
Other Attributes

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
Health System Help ▾ admin ▾
Local ▾ Updates Licenses Monitoring ▸ Syslog Tools ▾
□ Case-sensitive □ Exclusion
Go

Task Notification

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

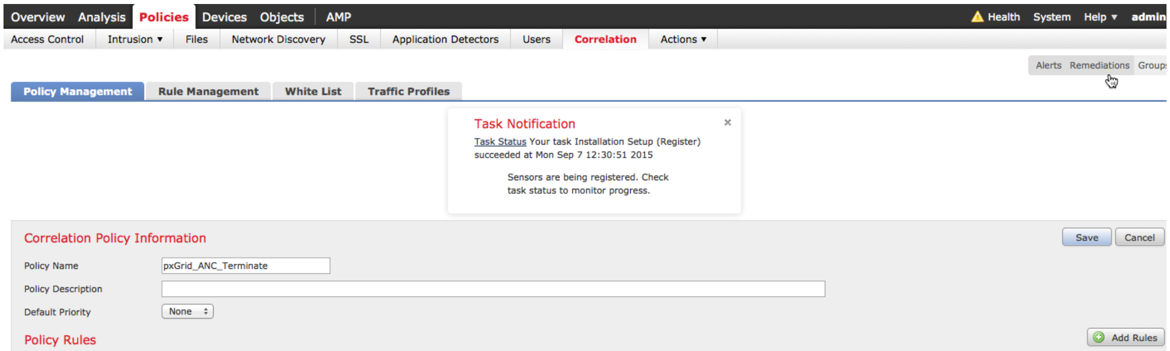
Sensors are being registered. Check task status to monitor progress.

```
Messages
Sep 08 2015 01:36:00 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_history' closed output.
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_history' closed output.
Sep 08 2015 01:31:00 Sourcefire3D SF-IMS[15096]: [15106] pm:log [INFO] Process 'store_whitelist_history' 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
Sep 08 2015 01:28:56 Sourcefire3D SF-IMS[23376]: pxgrid_mitigation.pl:normal [INFO] Notification pushed to the socket
Sep 08 2015 01:28:56 Sourcefire3D SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Attempting Mitigation: action=reAuthenticate, ip_address=192.168.1.8
Sep 08 2015 01:28:03 Sourcefire3D SF-IMS[20715]: [29011] sftunneld:sf_heartbeat [INFO] Saved SW VERSION 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 Detectors Users Correlation Actions ▾
Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles
Save Cancel
Add Rules

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

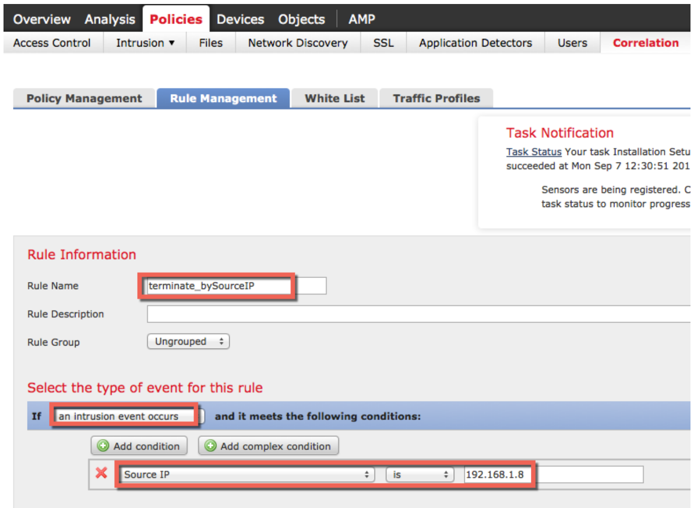
Policy Name: pxGrid_ANC_Terminate

Policy Description:

Default Priority: None

Policy 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)


Overview Analysis Policies Devices Objects AMP
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation
Policy Management Rule Management White List Traffic Profiles
Add condition
Add complex condition

Task Notification

Task Status Your task Installation Setu succeeded at Mon Sep 7 12:30:51 201

Sensors are being registered. C task status to monitor progress

Rule Information

Rule Name: terminate_bySourceIP

Rule Description:

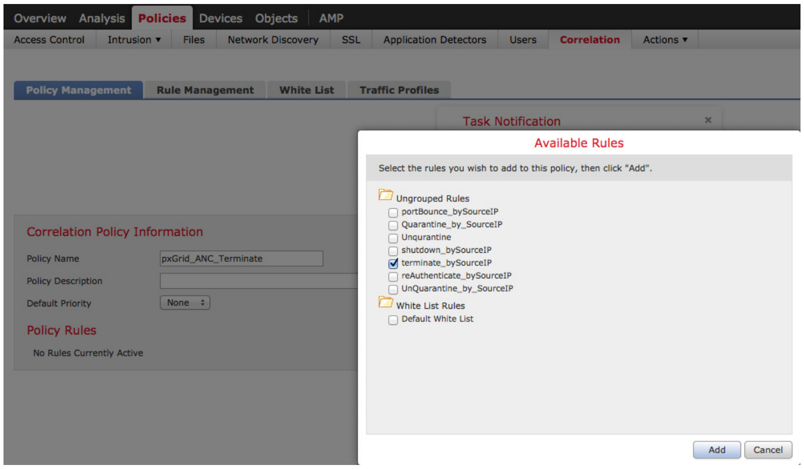
Rule Group: Ungrouped

Select the type of event for this rule

If an intrusion event occurs and it meets the following conditions:

Source IP is 192.168.1.8

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



Available Rules

Select the rules you wish to add to this policy, then click "Add".

Ungrouped Rules
- □ portBounce_bySourceIP
- □ Quarantine_by_SourceIP
- □ Unquarantine
- □ shutdown_bySourceIP
- ☑ terminate_bySourceIP
- □ reAuthenticate_bySourceIP
- □ UnQuarantine_by_SourceIP

White List Rules
- □ Default White List

Correlation Policy Information

Policy Name: pxGrid_ANC_Terminate

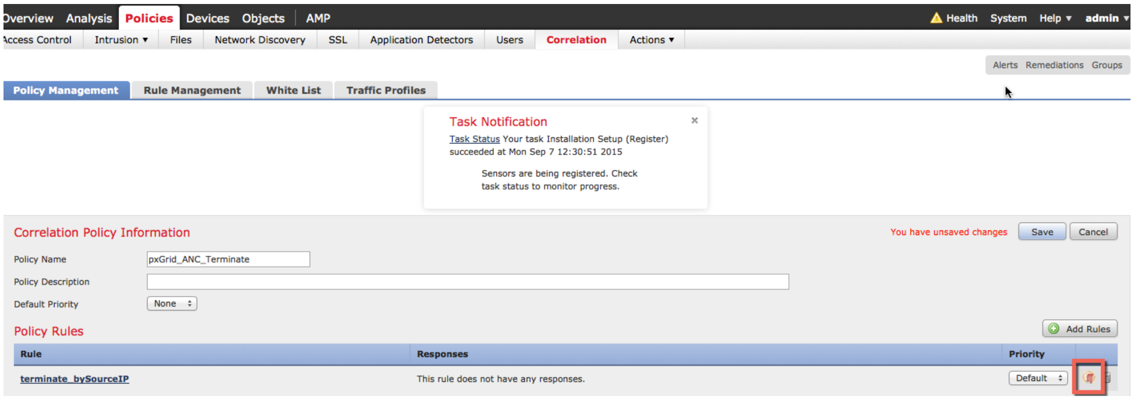
Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

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



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

Policy Name: pxGrid_ANC_Terminate

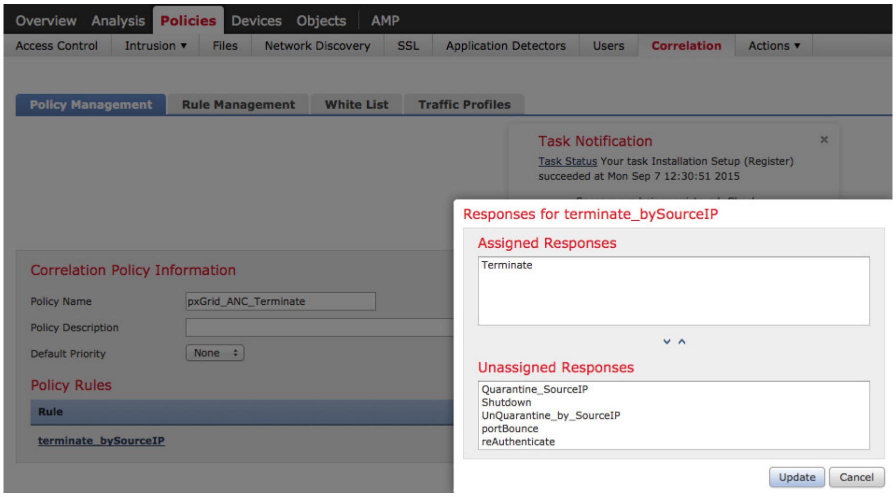
Policy Description:

Default Priority: None

Policy 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)



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

Responses for terminate_bySourceIP

Assigned Responses

Terminate

Unassigned Responses

Quarantine_SourceIP
Shutdown
UnQuarantine_by_SourceIP
portBounce
reAuthenticate

Correlation Policy Information

Policy Name: pxGrid_ANC_Terminate

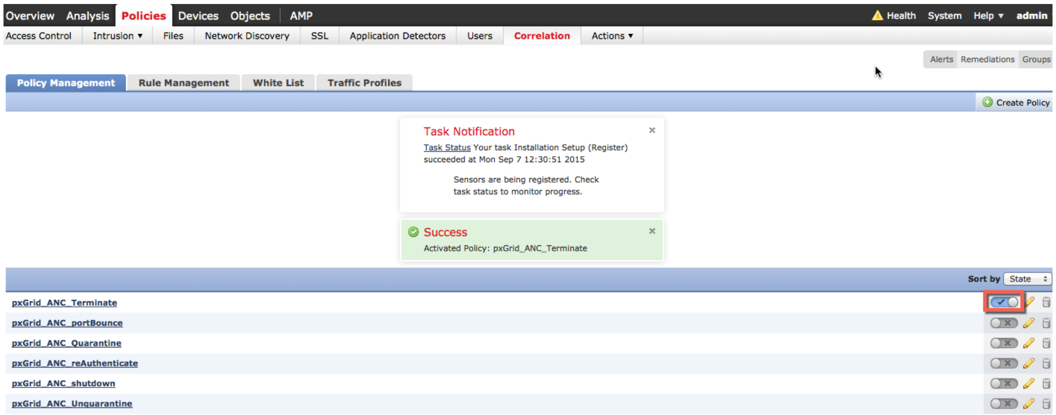
Policy Description:

Default Priority: None

Policy Rules

Rule
terminate_bySourceIP

第 6 步： 激活终止政策，点击将会打开该策略的以下**按钮**



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_Terminate

pxGrid_ANC_Terminate

pxGrid_ANC_portBounce

pxGrid_ANC_Quarantine

pxGrid_ANC_reAuthenticate

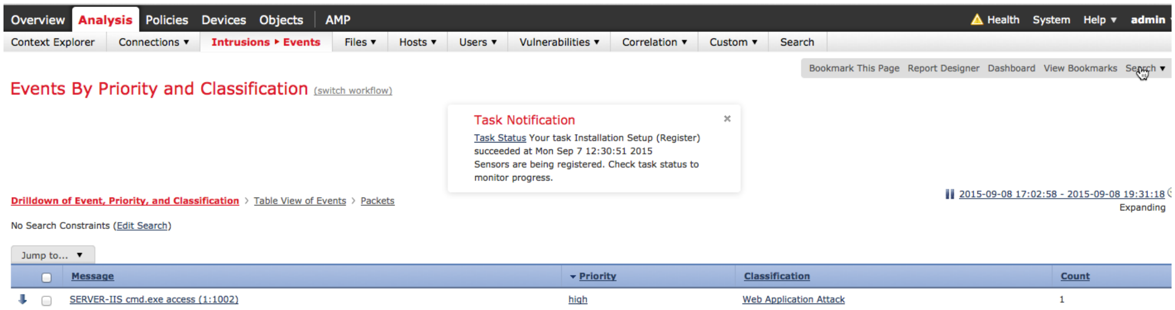
pxGrid_ANC_shutdown

pxGrid_ANC_Unquarantine

测试

最终用户将在其浏览器窗口中键入 www.yahoo.com/cmd.exe，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 www.yahoo.com/cmd.exe
第 2 步： 这将触发“Web 应用攻击”(Web Application Attack) 入侵事件



Events By Priority and Classification (switch workflow)

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.

Drilldown of Event, Priority, and Classification > Table View of Events > Packets

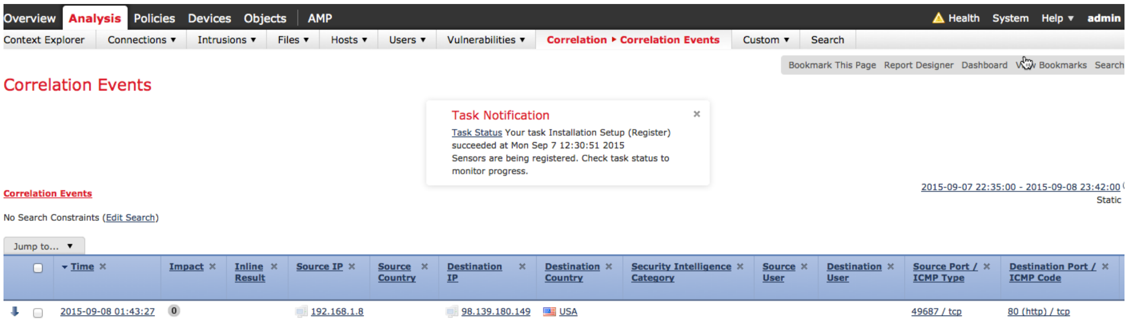
2015-09-08 17:02:58 - 2015-09-08 19:31:18
Expanding

No Search Constraints (Edit Search)

Message	Priority	Classification	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

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。



Correlation Events

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.

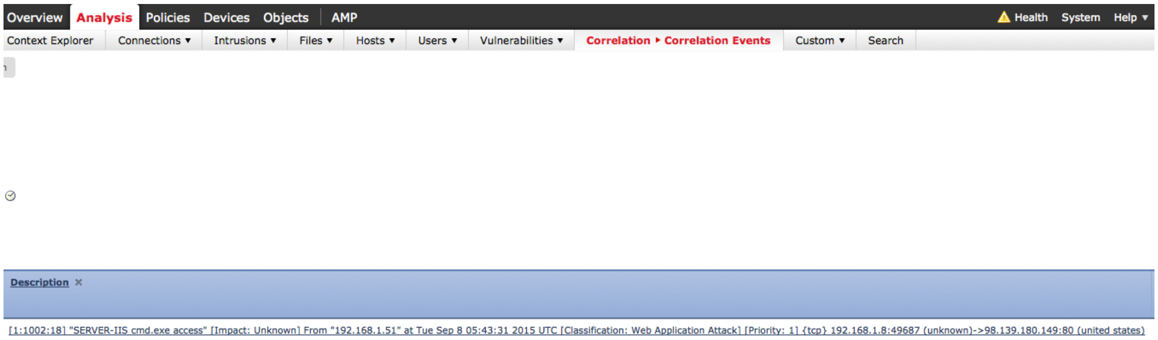
Correlation Events

2015-09-07 22:35:00 - 2015-09-08 23:42:00
Static

No Search Constraints (Edit Search)

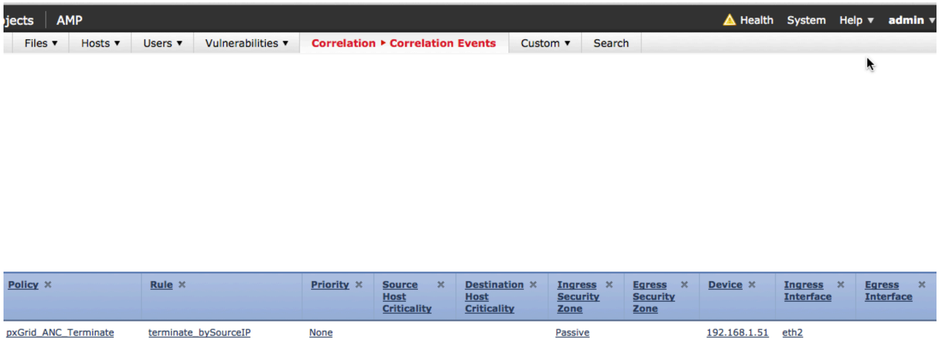
Time	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Security Intelligence Category	Source User	Destination User	Source Port / ICMP Type	Destination Port / ICMP Code
2015-09-08 01:43:27	0		192.168.1.8		98.139.180.149	USA				49687 / tcp	80 (http) / tcp

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。



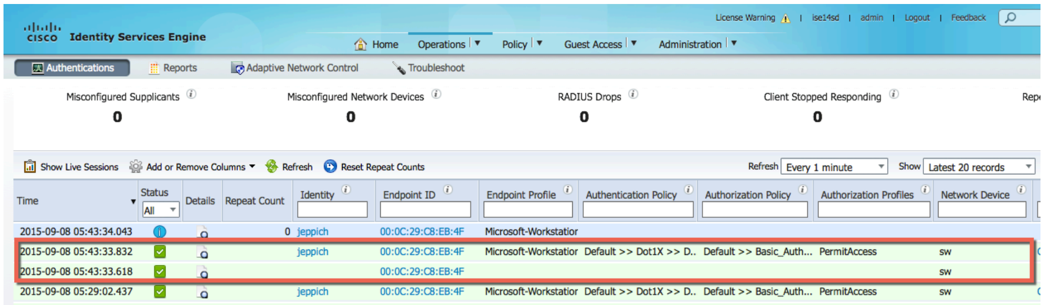
Description
[1:1002:18] "SERVER-IIS cmd.exe access" [Impact: Unknown] From "192.168.1.51" at Tue Sep 8 05:43:31 2015 UTC [Classification: Web Application Attack] [Priority: 1] {tcp} 192.168.1.8:49687 (unknown)->98.139.180.149:80 (united states)

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终止缓解响应的关联策略和关联规则



Policy	Rule	Priority	Source Host Criticality	Destination Host Criticality	Ingress Security Zone	Egress 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)

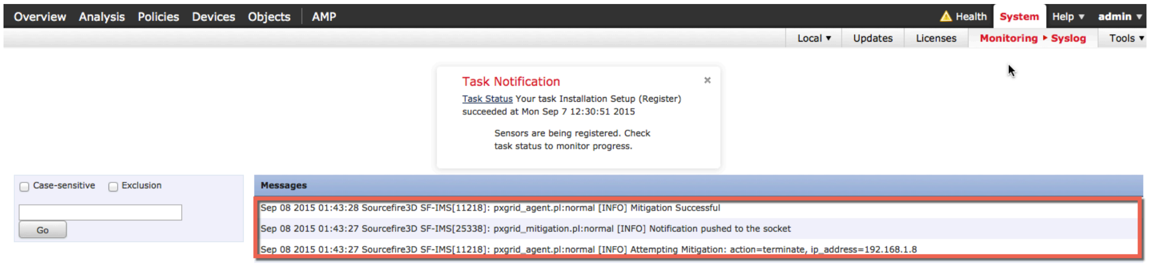


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Rep
0	0	0	0	

Refresh: Every 1 minute　Show: Latest 20 records

Time	Status (All)	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2015-09-08 05:43:34.043	ⓘ		0	jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior				
2015-09-08 05:43:33.832	☑			jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior	Default >> Dot1X >> D..	Default >> Basic_Auth...	PermitAccess	sw
2015-09-08 05:43:33.618	☑				00:0C:29:C8:EB:4F					sw
2015-09-08 05:29:02.437	☑			jeppich	00:0C:29:C8:EB:4F	Microsoft-Workstatior	Default >> Dot1X >> D..	Default >> Basic_Auth...	PermitAccess	sw

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



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.

Messages

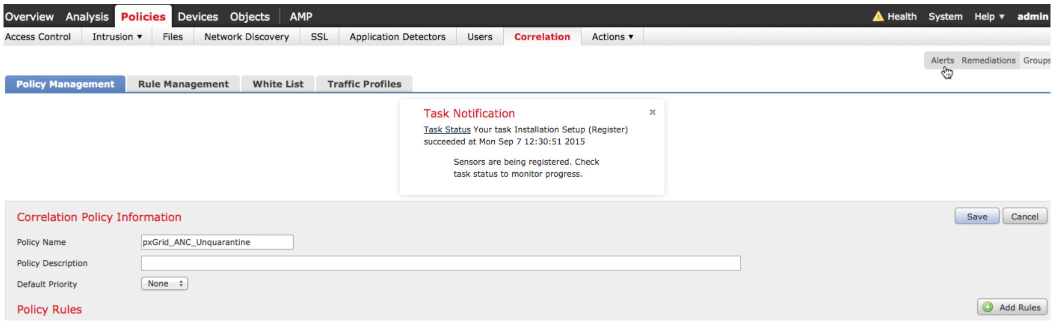
```
Sep 08 2015 01:43:28 Sourcefire3D SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Mitigation Successful
Sep 08 2015 01:43:27 Sourcefire3D SF-IMS[25338]: pxgrid_mitigation.pl:normal [INFO] Notification pushed to the socket
Sep 08 2015 01:43:27 Sourcefire3D SF-IMS[11218]: pxgrid_agent.pl:normal [INFO] Attempting Mitigation: action=terminate, ip_address=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)**



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

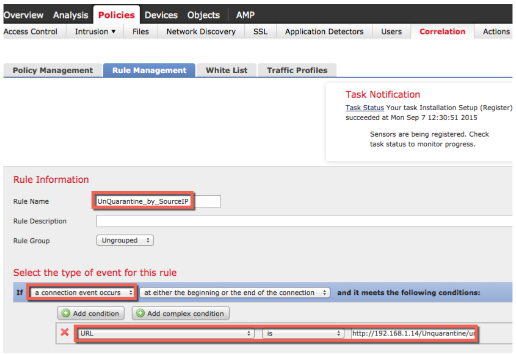
Policy Name: pxGrid_ANC_Unquarantine

Policy Description:

Default Priority: None

Policy 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)**



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.

Rule Information

Rule Name: UnQuarantine_by_SourceIP

Rule Description:

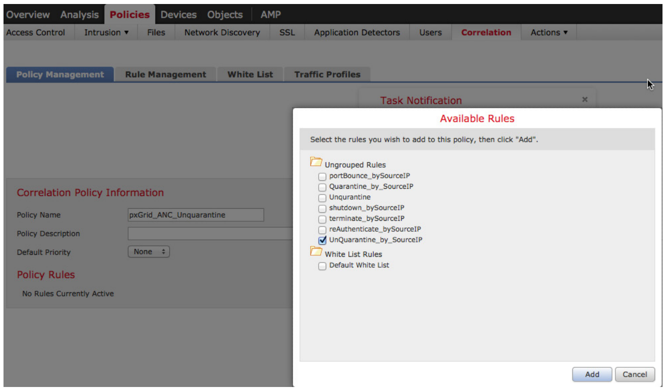
Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at either the beginning or the end of the connection and it meets the following conditions:

✕ URL is http://192.168.1.14/Unquarantine/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



Task Notification

Available Rules

Select the rules you wish to add to this policy, then click "Add".

Ungrouped Rules
- □ portBounce_bySourceIP
- □ Quarantine_by_SourceIP
- □ Unqurantine
- □ shutdown_bySourceIP
- □ terminate_bySourceIP
- □ reAuthenticate_bySourceIP
- ☑ UnQuarantine_by_SourceIP

White List Rules
- □ Default White List

Correlation Policy Information

Policy Name: pxGrid_ANC_Unquarantine

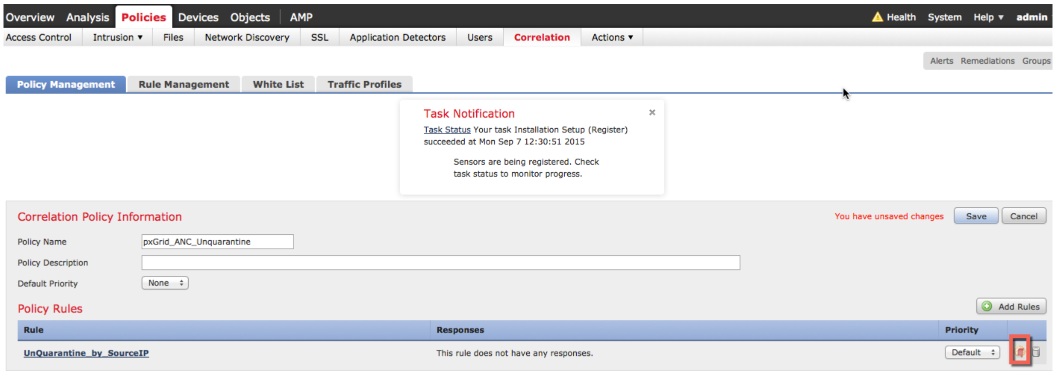
Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

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



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

Policy Name: pxGrid_ANC_Unquarantine

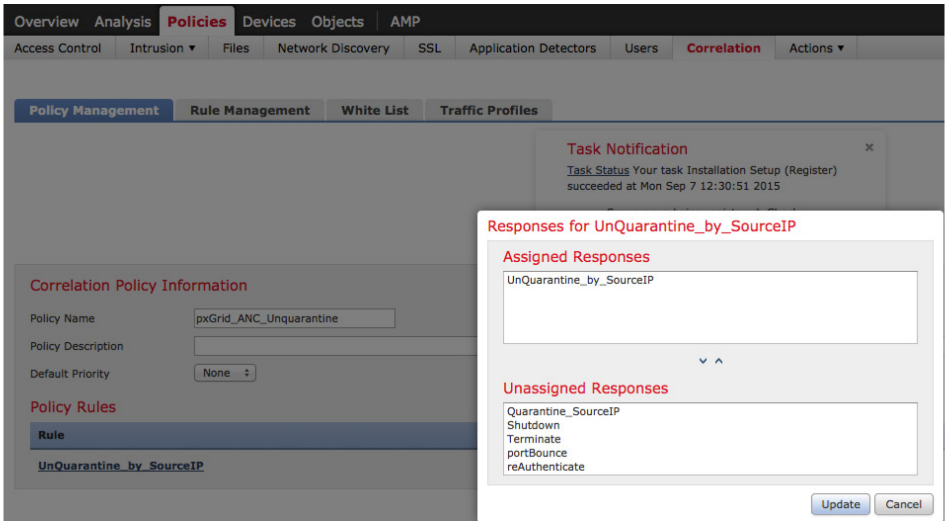
Policy Description:

Default Priority: None

Policy 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)**



Task Notification

Task Status Your task Installation Setup (Register) succeeded at Mon Sep 7 12:30:51 2015

Responses for UnQuarantine_by_SourceIP

Assigned Responses

UnQuarantine_by_SourceIP

Unassigned Responses

Quarantine_SourceIP
Shutdown
Terminate
portBounce
reAuthenticate

Correlation Policy Information

Policy Name: pxGrid_ANC_Unquarantine

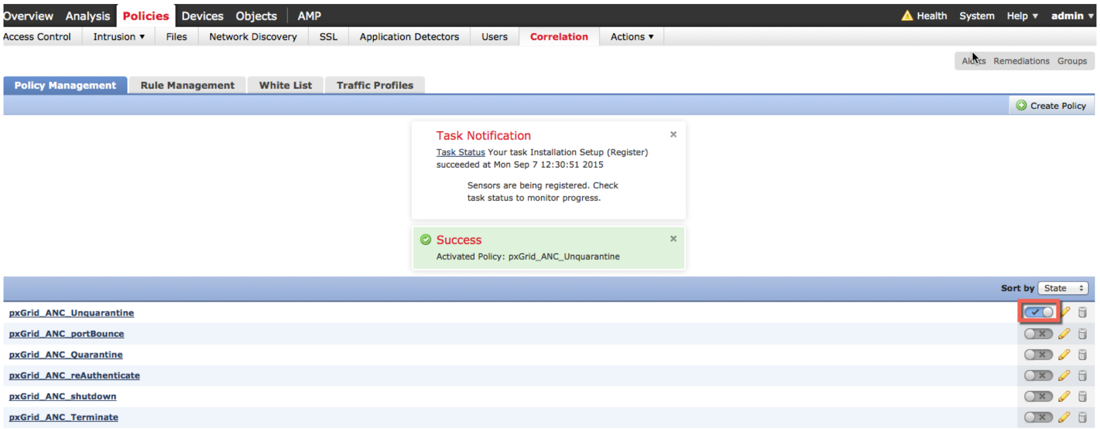
Policy Description:

Default Priority: None

Policy Rules

Rule
UnQuarantine_by_SourceIP

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

Alerts Remediations Groups

Policy Management | Rule Management | White List | Traffic Profiles

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_Unquarantine

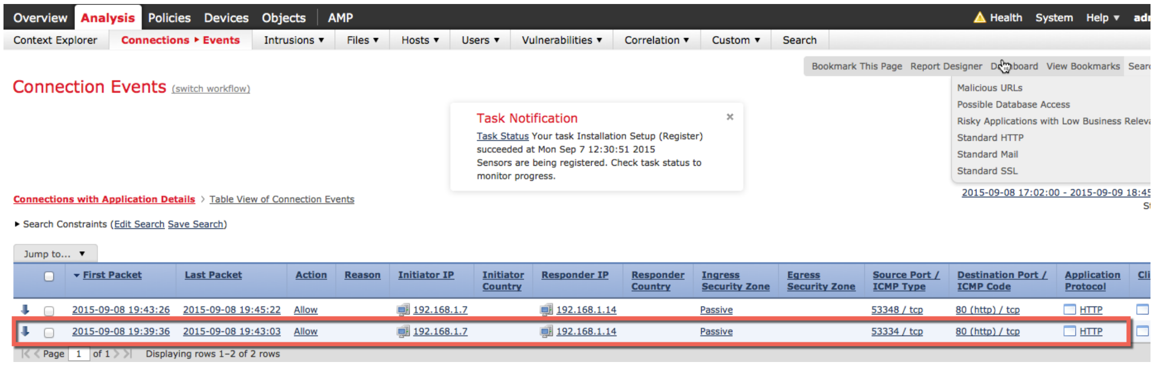
Sort by State

pxGrid_ANC_Unquarantine	✓
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 www.yahoo.com/cmd.exe，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



Overview Analysis Policies Devices Objects AMP | Health System Help adı

Context Explorer Connections ▸ Events Intrusions Files Hosts Users Vulnerabilities Correlation Custom Search

Bookmark This Page Report Designer Dashboard View Bookmarks Sear

Malicious URLs
Possible Database Access
Risky Applications with Low Business Releva
Standard HTTP
Standard Mail
Standard SSL

Connection Events (switch workflow)

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.

2015-09-08 17:02:00 - 2015-09-09 18:45

Connections with Application Details > Table View of Connection Events

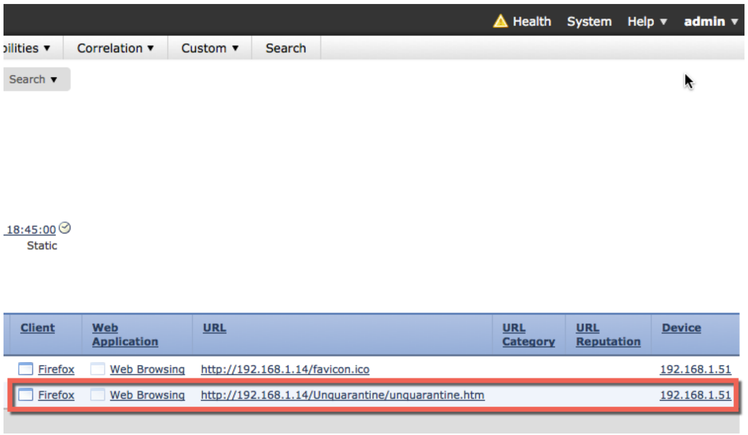
▸ Search Constraints (Edit Search Save Search)

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Cli
□	2015-09-08 19:43:26	2015-09-08 19:45:22	Allow		192.168.1.7		192.168.1.14		Passive		53348 / tcp	80 (http) / tcp	HTTP	
□	2015-09-08 19:39:36	2015-09-08 19:43:03	Allow		192.168.1.7		192.168.1.14		Passive		53334 / tcp	80 (http) / tcp	HTTP	

Page 1 of 1 Displaying rows 1–2 of 2 rows

第 3 步： 此处是连接事件的持续



Health System Help admin

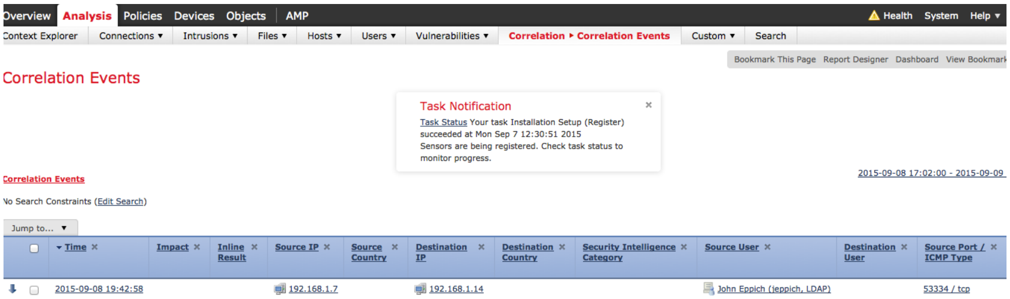
ilities Correlation Custom Search

Search

18:45:00
Static

Client	Web Application	URL	URL Category	URL Reputation	Device
Firefox	Web Browsing	http://192.168.1.14/favicon.ico			192.168.1.51
Firefox	Web Browsing	http://192.168.1.14/Unquarantine/unquarantine.htm			192.168.1.51

第 4 步： 这还会触发“关联事件”
请注意，源 IP 地址将取消隔离。



Correlation Events

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.

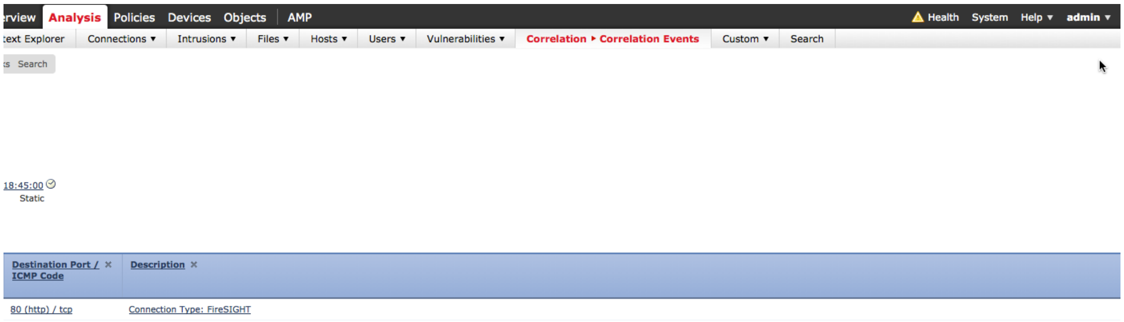
Correlation Events

2015-09-08 17:02:00 - 2015-09-09

No Search Constraints (Edit Search)

	▾ Time	Impact	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			192.168.1.7		192.168.1.14			John Eppich (jeppich, LDAP)		53334 / tcp

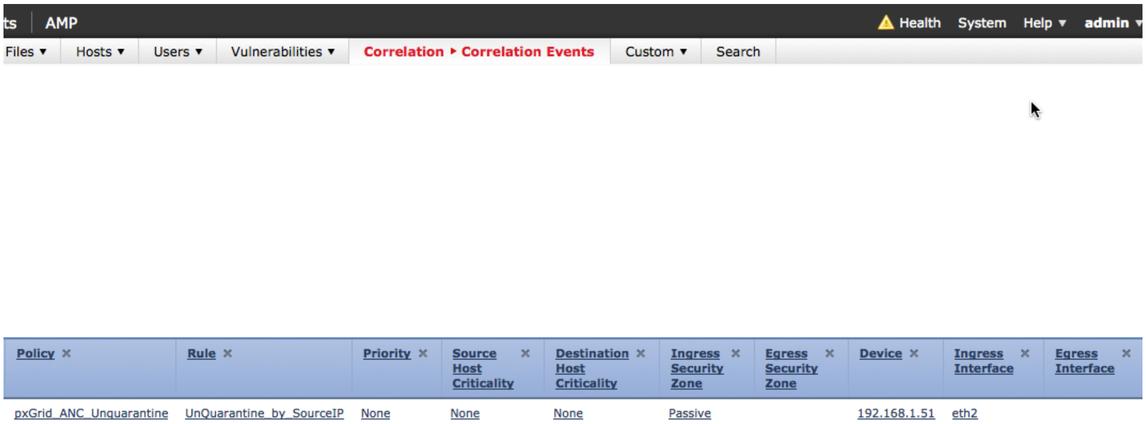
第 5 步： 随着我们继续处理同一事件
请注意连接事件。



18:45:00
Static

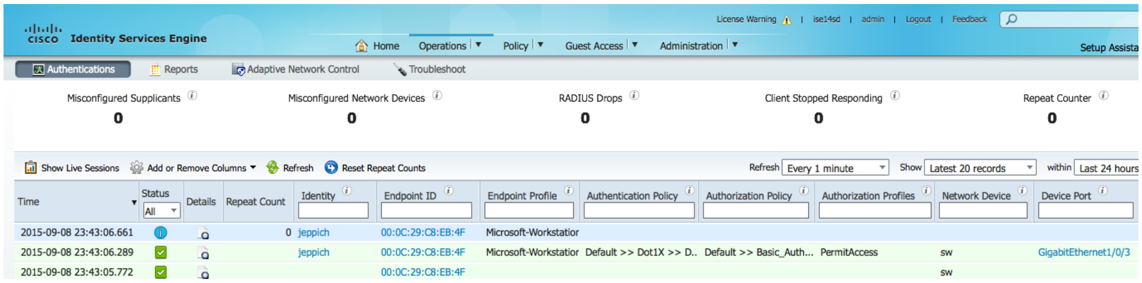
Destination Port / ICMP Code	Description
80 (http) / tcp	Connection Type: FireSIGHT

第 6 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



Policy	Rule	Priority	Source Host Criticality	Destination Host Criticality	Ingress Security Zone	Egress Security Zone	Device	Ingress Interface	Egress Interface
pxGrid_ANC_Unquarantine	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)**

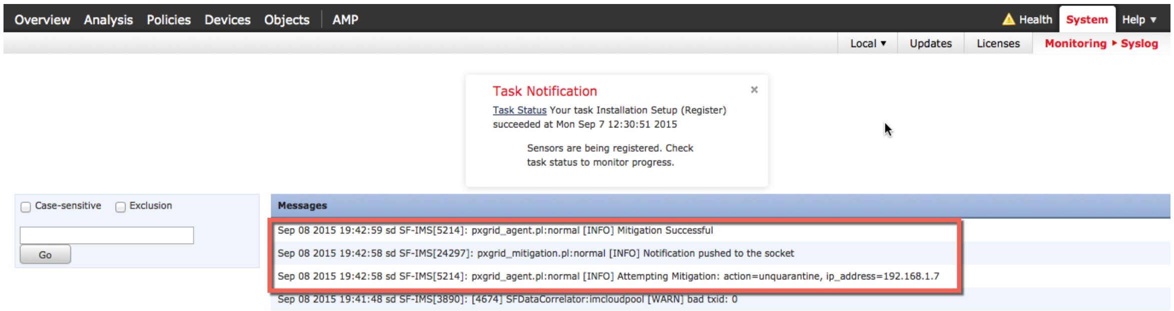


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Every 1 minute　Show Latest 20 records　within Last 24 hours

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port
	All										
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



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.

Messages

```
Sep 08 2015 19:42:59 sd SF-IMS[5214]: pxgrid_agent.pl:normal [INFO] Mitigation Successful
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=192.168.1.7
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 ise14lab.pem
```

pem 文件应包含证书

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:19:bf:90:00:00:00:00:ab:b7:4f:a0:57:21:a0:03
    Signature Algorithm: sha1WithRSAEncryption
        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:
                    0d: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:
```

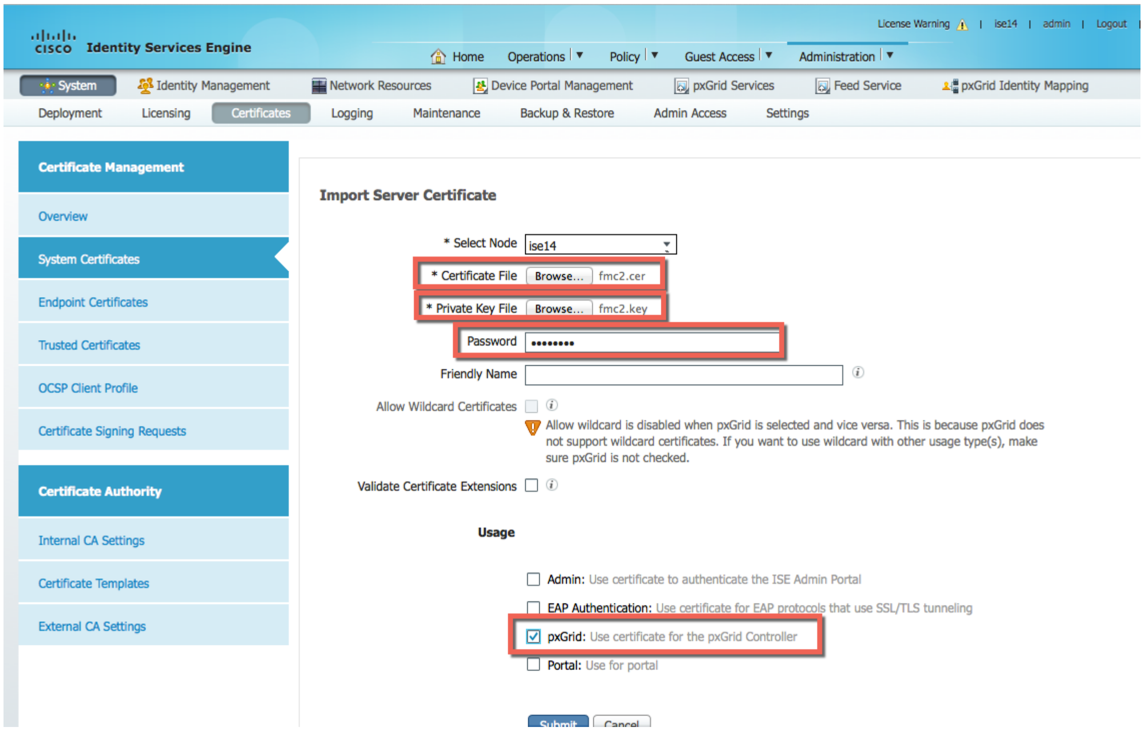
```
        3d:53:8b:77:ed:e7:8a:5a:38:b6:3b:0e:c0:93:63:c1:f6:2e:
        a3:ce:33:a4:0a:82:d4:f7:8f:0f:c2:99:9e:96:36:c5:89:a2:
        9f:f3:66:01:12:da:13:53:d4:92:ef:17:9e:2b:26:4b:3c:7d:
        1f:6f:a3:b4
```

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



Import Server Certificate

* Select Node: ise14

* Certificate File: Browse... fmc2.cer

* Private Key File: Browse... fmc2.key

Password: ••••••••

Friendly Name:

Allow Wildcard Certificates □

Allow wildcard is disabled when pxGrid is selected and vice versa. This is because pxGrid does not support wildcard certificates. If you want to use wildcard with other usage type(s), make sure pxGrid is not checked.

Validate Certificate Extensions □

Usage

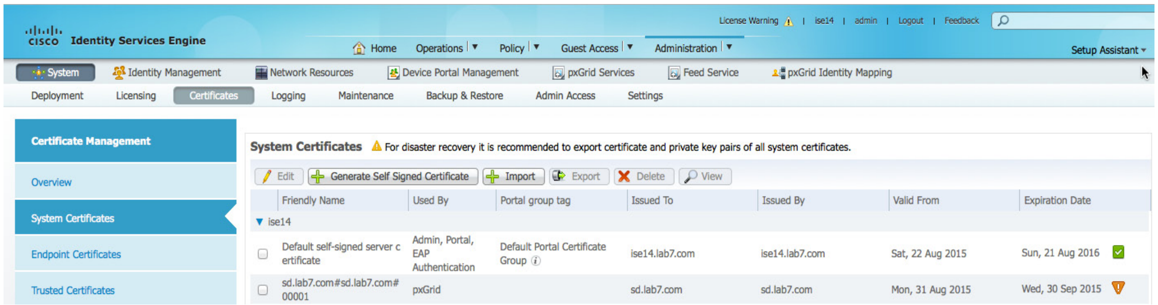
□ Admin: Use certificate to authenticate the ISE Admin Portal

□ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

☑ pxGrid: Use certificate for the pxGrid Controller

□ Portal: Use for portal

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：



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise14								
□	Default self-signed server certificate	Admin, Portal, EAP Authentication	Default Portal Certificate Group ⓘ	ise14.lab7.com	ise14.lab7.com	Sat, 22 Aug 2015	Sun, 21 Aug 2016	✓
□	sd.lab7.com#sd.lab7.com#00001	pxGrid		sd.lab7.com	sd.lab7.com	Mon, 31 Aug 2015	Wed, 30 Sep 2015	!

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

提交的缺陷：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

说明：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：http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

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：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-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：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf