

Integração do pxGrid da versão 1.3 ISE com aplicativo do pxLog IPS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama da rede e fluxo de tráfego](#)

[pxLog](#)

[Arquitetura](#)

[Instalação](#)

[Snort](#)

[ISE](#)

[Configuração](#)

[Personalidade e certificado](#)

[Serviço de proteção do valor-limite \(EP\)](#)

[Regras da autorização](#)

[Troubleshooting](#)

[Teste](#)

[Step1. Registro para o pxGrid](#)

[Step2. o pxLog ordena a configuração](#)

[Step3. Primeira sessão do dot1x](#)

[Step4. Microsoft Windows PC envia o pacote que provoca o alarme](#)

[Step5. pxLog](#)

[Step6. Quarentena ISE](#)

[Step7. pxLog Unquarantine](#)

[Step8. ISE Unquarantine](#)

[funcionalidade do pxLog](#)

[requisitos de protocolo do pxGrid](#)

[Grupos](#)

[Certificados e Javas KeyStore](#)

[Hostname](#)

[Note para colaboradores](#)

[Syslog](#)

[Snort](#)

[Inspeção adaptável da ferramenta de segurança de Cisco \(ASA\)](#)

[Sistemas da prevenção de intrusão da próxima geração de Cisco Sourcefire \(NGIPS\)](#)

[NetScreen do zimbra](#)

[Zimbra JunOS](#)

[Iptables de Linux](#)

[FreeBSD IPFirewall \(IPFW\)](#)

[Prontidão VPN e manipulação CoA](#)

[Parceiros e soluções do pxGrid](#)

[ISE API: RESTO contra EREST contra o pxGrid](#)

[Downloads](#)

[Informações Relacionadas](#)

Introdução

A versão 1.3 do Identity Services Engine (ISE) apoia um pxGrid chamado API novo. Estes protocolo que apoia a autenticação, criptografia, e privilégios modernos e flexíveis (grupos) permitem a fácil integração com outras soluções da Segurança. Este documento descreve o uso do aplicativo do pxLog que foi escrito como um teste de conceito. o pxLog pode receber mensagens do syslog do Intrusion Prevention System (IPS) e enviar mensagens do pxGrid ao ISE a fim quarantine o atacante. Em consequência, o ISE usa a mudança do RAIO da autorização (CoA) a fim mudar o estado de autorização do valor-limite que limita o acesso de rede. Toda a esta acontece transparentemente ao utilizador final.

Para este exemplo, o Snort foi usado como o IPS, mas toda a outra solução poderia ser usada. Realmente não tem que ser um IPS. Tudo que é exigido é enviar o mensagem do syslog ao pxLog com o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante. Isto cria uma possibilidade para a integração de um grande número soluções.

Este documento igualmente apresenta como pesquisar defeitos e testar soluções do pxGrid, com os problemas típicos e as limitações.

Ressalva: O aplicativo do pxLog não é apoiado por Cisco. Este artigo foi escrito como um teste de conceito. O propósito principal era usá-la durante betatesting da aplicação do pxGrid no ISE.

Pré-requisitos

Requisitos

Cisco recomenda que você tem a experiência com configuração de Cisco ISE e conhecimento básico destes assuntos:

- Disposições e configuração de autorização ISE
- Configuração de CLI do Switches do Cisco catalyst

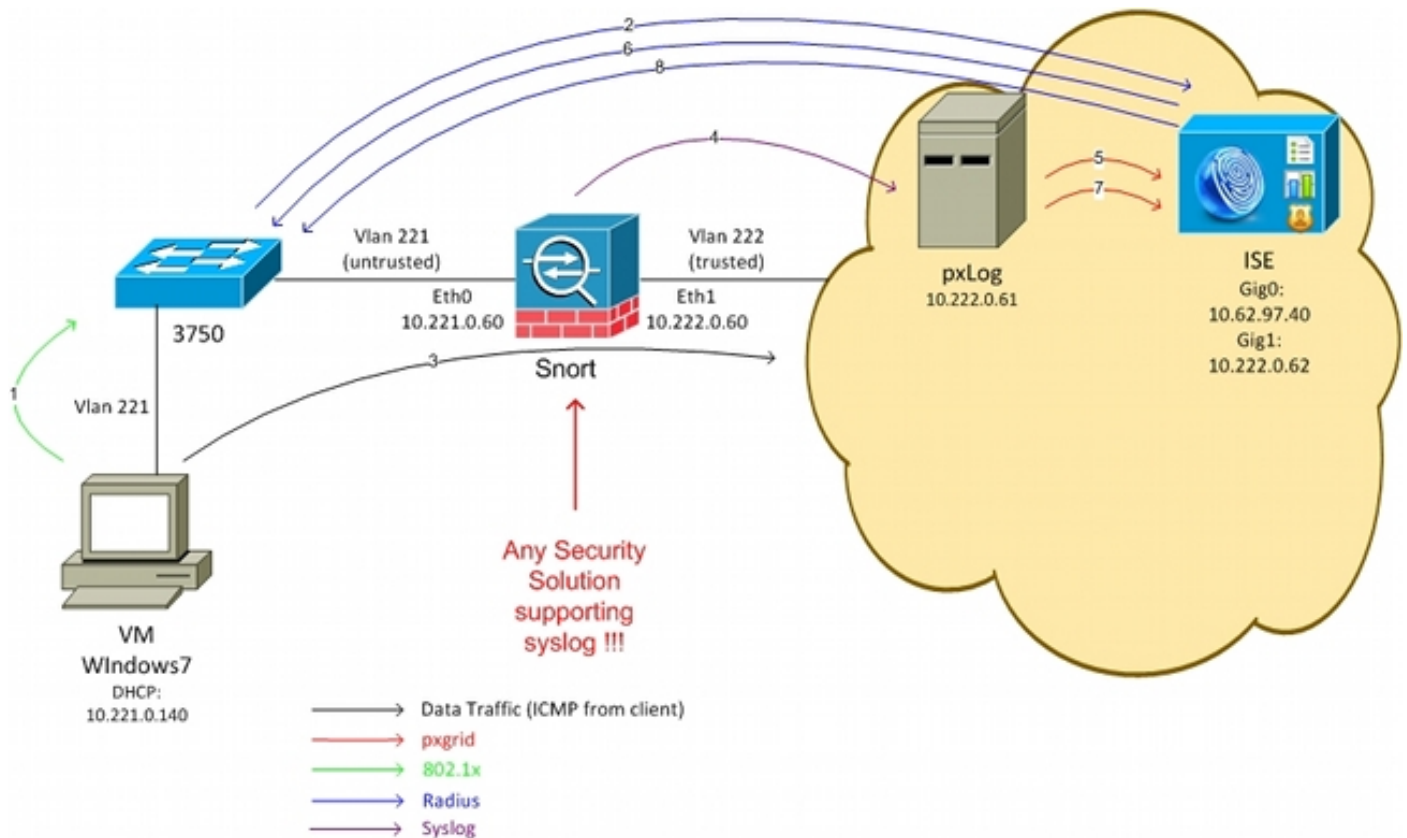
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Software do Cisco Catalyst 3750X Series Switch, versões 15.0 e mais recente
- Software de Cisco ISE, versões 1.3 e mais recente

- Mobile Security de Cisco AnyConnect com gerente do acesso de rede (NAM), versão 3.1 e mais recente
- Versão 2.9.6 do Snort com por aquisição de dados (DAQ)
- aplicativo do pxLog instalado em Tomcat 7 com versão 5 de MySQL

Diagrama da rede e fluxo de tráfego



Está aqui o fluxo de tráfego, como ilustrado no diagrama da rede:

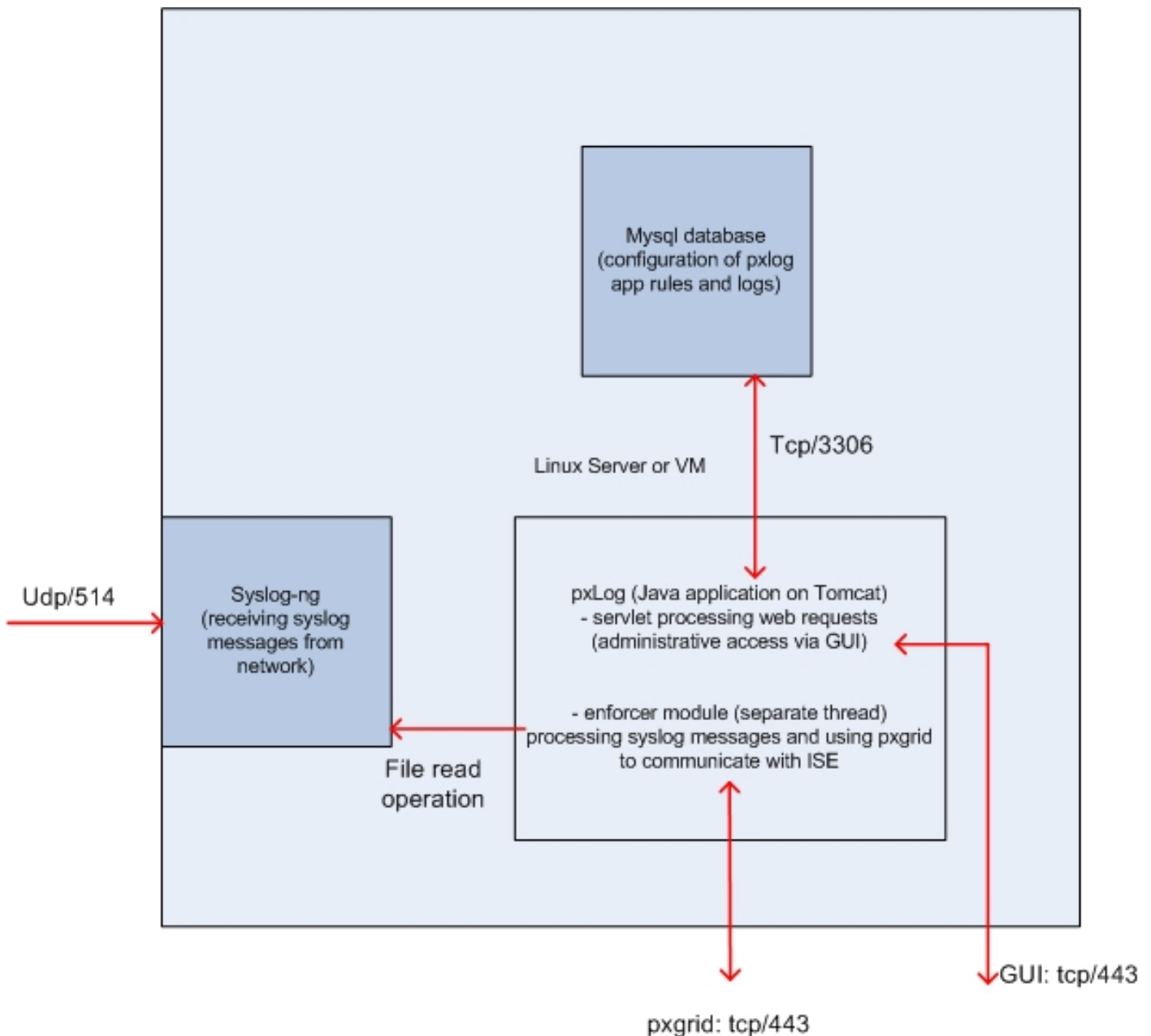
1. Um usuário de Microsoft Windows 7 conecta ao interruptor e executa a autenticação do 802.1x.
2. O interruptor usa o ISE como o server do Authentication, Authorization, and Accounting (AAA). A regra da autorização do **acesso direto do dot1x** é combinada e o acesso de rede completo é concedido (DACL: PERMIT_ALL).
3. O usuário tenta conectar com a rede confiável e viola a regra do Snort.
4. Em consequência, o Snort envia um alerta ao aplicativo do pxLog (através do Syslog).
5. O aplicativo do pxLog executa a verificação contra seu base de dados local. É configurado a fim travar os mensagens do syslog enviados pelo Snort e extrair o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante. Então usa o pxGrid para enviar um pedido para o ISE a fim quarantine o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante (o ISE é um controlador do pxGrid).
6. O ISE reavalia sua política da autorização. Porque o valor-limite quarantined, a **sessão: A**

condição da **quarentena dos IGUAIS de EPSStatus** é estada conforme e um perfil diferente da autorização é combinado (**quarentena do dot1x**). O ISE envia um CoA termina ao interruptor a fim terminar a sessão. Isto provoca a reautenticação e um ACL baixável novo (DACL) (PERMIT_ICMP) é aplicado, que fornece o acesso de rede limitado ao utilizador final.

7. Nesta fase, o administrador pôde decidir ao unquarantine o valor-limite. Isto pode ser conseguido através do GUI do pxLog. Além disso, a mensagem do pxGrid para o ISE é enviada.
8. O ISE executa uma operação similar como na etapa 6. Esta vez, o valor-limite já não quarantined e o acesso direto é fornecido.

pxLog

Arquitetura



A solução é instalar um grupo de aplicativos em uma máquina de Linux:

1. O aplicativo do pxLog escrito nas Javas e distribuído no server de Tomcat. Esse aplicativo consiste:

Servlet que processa pedidos da Web - Isto é usado a fim alcançar o painel administrativo através do navegador da Web.

Módulo do impulsionador - Rosqueie que é começado junto com o servlet. O impulsionador lê mensagens do syslog do arquivo (aperfeiçoado), processa aquelas mensagens conforme as regras configuradas, e executa ações (como a quarentena através do pxGrid).

2. O base de dados de MySQL que contém a configuração para o pxLog (regras e logs).
3. O servidor de SYSLOG que recebe mensagens do syslog dos sistemas externos e os

escreve a um arquivo.

Instalação

O aplicativo do pxLog usa estas bibliotecas:

- jQuery (para o apoio de AJAX)
- A biblioteca padrão da etiqueta das páginas de JavaServer (JSTL) (o modelo modelo do controlador da vista (MVC), dados é separada da lógica: O código da página de JavaServer (JSP) é usado para render somente, nenhum código HTML nas classes java)
- Log4j como um subsistema de registro
- Conector de MySQL
- displaytag para tabelas da rendição/de classificação
- pxGrid API por Cisco (atualmente alfa 147 da versão)

Todas aquelas bibliotecas não estão já no diretório do liberal do projeto tão lá são nenhuma necessidade de transferir any more arquivos do Java Archive (FRASCO).

A fim instalar o aplicativo:

1. Desembale o diretório inteiro ao diretório de Tomcat Webapp.
2. Edite o **arquivo WEB-INF/web.xml**. A única alteração requerida é a serveripvariable, que devem apontar ao ISE. Igualmente as Javas Certificate KeyStores (um para confiado e um para a identidade) puderam ser geradas (em vez do padrão). Isto é usado pelo pxGrid API que usa a sessão do secure sockets layer (SSL) com ambos os Certificados de cliente e servidor. Ambos os lados da necessidade de comunicação de apresentar com o certificado e de precisar de confiar-se. Refira a seção dos requisitos de protocolo do pxGrid para mais informação.
3. Certifique-se que o hostname ISE está resolvido corretamente no pxLog (refira o registro no Domain Name Server (DNS) ou na **entrada de /etc/hosts**). Refira a seção dos requisitos de protocolo do pxGrid para mais informação.
4. Configurar o base de dados de MySQL com o **script mysql/init.sql**. As credenciais podem ser mudadas mas devem ser refletidas no **arquivo WEB-INF/web.xml**.

Snort

Este artigo não se centra sobre nenhum IPS específico, que é porque somente uma explicação resumida é fornecida.

O Snort é configurado como inline com apoio DAQ. O tráfego é reorientado com iptables:

```
iptables -I FORWARD -j ACCEPT
iptables -I FORWARD -j NFQUEUE --queue-num 1
```

Então, após a inspeção, é injetado e enviado conforme regras iptable do padrão.

Algumas regras feitas sob encomenda do Snort foram configuradas (o arquivo de

`/etc/snort/rules/test.rules` é incluído na configuração global).

```
alert icmp any any -> any any (itype:8; dsize:666<>686; sid:100122)
alert icmp any any -> any any (itype:8; ttl: 6; sid:100124)
```

O Snort envia um mensagem do syslog quando o Time to Live (TTL) do pacote é igual a 6 ou o tamanho do payload está entre 666 e 686. O tráfego não é obstruído pelo Snort.

Igualmente os pontos iniciais devem estabelecer-se para certificar-se que os alertas não estão provocados demasiado frequentemente (`/etc/snort/threshold.conf`):

```
event_filter gen_id 1, sig_id 100122, type limit, track by_src, count 1, seconds 60
event_filter gen_id 1, sig_id 100124, type limit, track by_src, count 1, seconds 60
```

Então o servidor de SYSLOG aponta à máquina do pxLog (`/etc/snort/snort.conf`):

```
output alert_syslog: host=10.222.0.61:514, LOG_AUTH LOG_ALERT
```

Para algumas versões do Snort, há uns erros relativos à configuração do Syslog, e então as configurações padrão poderiam ser usadas que apontam ao host local e o Syslog-NG poderia ser configurado a fim encaminhar mensagens específicas ao host do pxLog.

ISE

Configuração

Personalidade e certificado

1. Permita o papel do pxGrid, que é desabilitado no ISE à revelia, sob a **administração > o desenvolvimento**:

Edit Node

General Settings

Profiling Configuration

Hostname **lise**
FQDN **lise.example.com**
IP Address **10.62.97.40**
Node Type **Identity Services Engine (ISE)**

Personas

- Administration Role **STANDALONE**

- Monitoring Role Other Monitoring Node

- Policy Service
 - Enable Session Services ⓘ
 Include Node in Node Group ⓘ

 - Enable Profiling Service

- pxGrid ⓘ

2. Verifique se os Certificados são usados para o pxGrid sob a **administração > Certificados > Certificados do sistema**:

Certificate Management

- Overview
- System Certificates**
- Endpoint Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests

Certificate Authority

- Internal CA Settings
- Certificate Templates
- External CA Settings

Edit System Certificate

Issuer

* Friendly Name:

Description:

Subject: CN=lise.example.com

Issuer: win2012

Valid From: Tue, 26 Aug 2014 12:32:56 CEST

Valid To (Expiration): Thu, 25 Aug 2016 12:32:56 CEST

Serial Number: 7B 00 00 00 3D 4C D6 27 D1 7D BB DF A6 00 00 00 00 3D

Signature Algorithm: SHA1WITHRSA

Key Length: 2048

Usage

- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- Admin: Use certificate to authenticate the ISE Admin Portal
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

Serviço de proteção do valor-limite (EP)

Os EP devem ser permitidos (desabilitado à revelia) da **administração > dos ajustes:**

Settings

- Client Provisioning
- Endpoint Protection Service**
- FIPS Mode
- Alarm Settings

Endpoint Protection Service ⓘ

Service Status: Enabled ▾

Isto permite que você use a funcionalidade da quarentena/unquarantine.

Regras da autorização

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 (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Dot1x Quarantine	if (DEVICE:Device Type EQUALS All Device Types#switch AND Session:EPSSStatus EQUALS Quarantine)	then Permit_ICMP
✓	Dot1x Full Access	if DEVICE:Device Type EQUALS All Device Types#switch	then Permit_ALL

A primeira regra é encontrada somente quando o valor-limite quarantined. O acesso então limitado é reforçado dinamicamente pelo CoA do RAIO. O interruptor igualmente deve ser adicionado aos dispositivos de rede com o segredo compartilhado correto.

Troubleshooting

O estado do pxGrid pode ser verificado com o CLI:

```
lise/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	6717
Database Server	running	51 PROCESSES
Application Server	running	9486
Profiler Database	running	7804
AD Connector	running	10058
M&T Session Database	running	7718
M&T Log Collector	running	9752
M&T Log Processor	running	9712
Certificate Authority Service	running	9663
pxGrid Infrastructure Service	running	14979
pxGrid Publisher Subscriber Service	running	15281
pxGrid Connection Manager	running	15248
pxGrid Controller	running	15089
Identity Mapping Service	running	9962

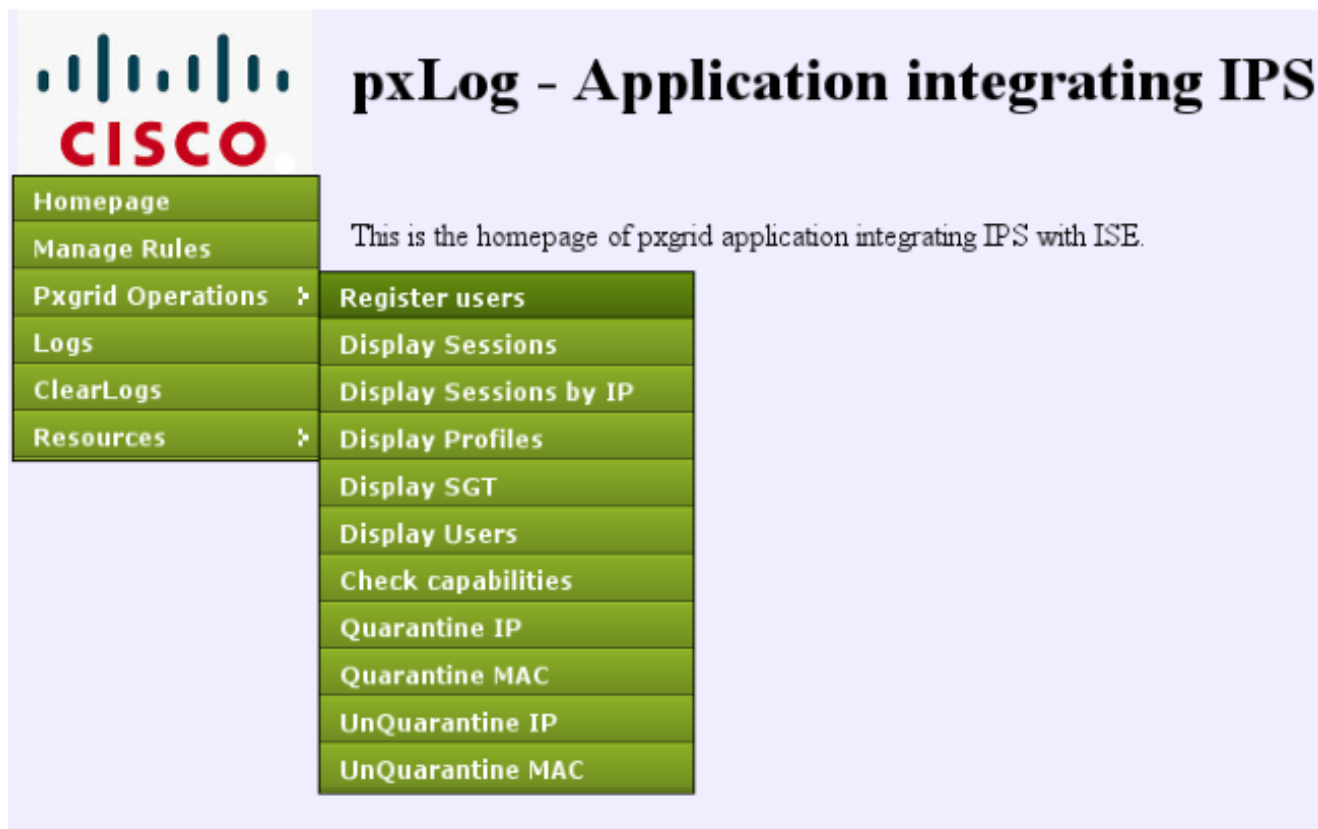
Há igualmente separado debuga para o pxGrid (a **administração > registrando > debuga a configuração > o pxGrid do log**). Debugar arquivos são armazenados no diretório do pxGrid. Os dados os mais importantes estão no **pxgrid/pxgrid-jabberd.log** e no **pxgrid/pxgrid-controller.log**.

Teste

Step1. Registro para o pxGrid


O aplicativo do pxLog é distribuído automaticamente quando Tomcat começa.

1. A fim usar o pxGrid, registrar dois usuários no ISE (um com acesso da sessão, e um com quarentena). Isto pode ser terminado dos **usuários das operações > do registro de Pxgrid**:



The screenshot shows the pxLog application interface. At the top left is the Cisco logo. The main heading is "pxLog - Application integrating IPS". Below the heading is a navigation menu with the following items: Homepage, Manage Rules, Pxgrid Operations, Logs, ClearLogs, and Resources. The "Pxgrid Operations" menu is expanded, showing a list of options: Register users, Display Sessions, Display Sessions by IP, Display Profiles, Display SGT, Display Users, Check capabilities, Quarantine IP, Quarantine MAC, UnQuarantine IP, and UnQuarantine MAC. The main content area displays the text: "This is the homepage of pxgrid application integrating IPS with ISE."

O registro começa automaticamente:



The screenshot shows the pxLog application interface during the registration process. The main heading is "pxLog - Application integrating IPS with Cisco ISE". The navigation menu is the same as in the previous screenshot. The main content area displays the following text: "Registration", "The Registration process has started", "Two pxgrid clients are being registered on ISE", "One client with Session privileges (to browse session data) and other with EPS privileges (to execute quarantine)", "Please login to ISE and approve registration by clicking 'Approve'", "Content of the page will be updated automatically every 5 seconds to notify if the users are approved on ISE", "Waiting for the status to be updated...", and "Waiting for the status to be updated..."

2. Nesta fase, é necessário aprovar usuários registrados no ISE (a auto aprovação é desabilitada à revelia):

Client Name	Client Description	Capabilities	Status	Client Group
ise-admin-lise		Capabilities(3 Pub, 1 Sub)	Online	Administrator
ise-mnt-lise		Capabilities(1 Pub, 0 Sub)	Online	Administrator
pxclient_session	test	Capabilities(0 Pub, 0 Sub)	Pending	Session
pxclient_eps	test	Capabilities(0 Pub, 0 Sub)	Pending	EPS

Após a aprovação, o pxLog notifica automaticamente o administrador (através de um atendimento de AJAX):

```
Session user: pxclient_session registered and approved successfully
EPS user: pxclient_eps registered and approved successfully
```

O ISE mostra o estado para aqueles dois usuários como em linha ou off line (não durante anymore).

Step2. o pxLog ordena a configuração

o pxLog deve processar mensagens do syslog e executar as ações baseadas nele. A fim adicionar uma regra nova, seleta **controle regras**:

pxLog - Application integrating

Rules for the Enforcer module.
 IPS sending syslog messages, Enforcer receiving and processing.
 When the match against configured rules is found
 Enforcer is automatically executing quarantine via pxgrid

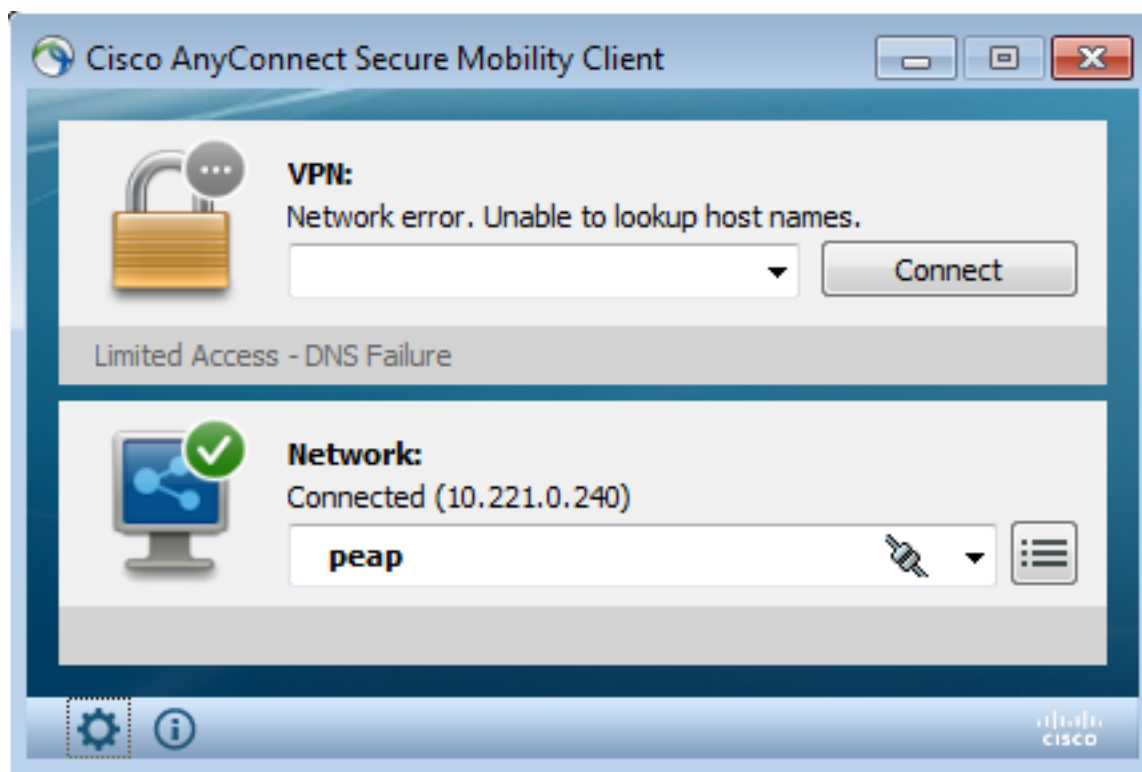
Rule Id	Rule string	Action
19	snort[Remove
New Rule	<input type="text"/>	Add New Rule

Agora o módulo do impulsador procura esta expressão regular (regexp) no mensagem do syslog: "snort [". Se encontrado, procura todos os endereços IP de Um ou Mais Servidores Cisco ICM NT e seleciona esse antes do último. Isto combina a maioria de soluções da Segurança.

Refira a seção do Syslog para mais informação. Esse endereço IP de Um ou Mais Servidores Cisco ICM NT (atacante) quarantined através do pxGrid. Igualmente uma regra mais granulada pôde ser usada (por exemplo, pôde incluir o número da assinatura).

Step3. Primeira sessão do dot1x

A estação de Microsoft Windows 7 inicia uma sessão prendida do dot1x. Cisco Anyconnect NAM foi usado como um suplicante. O método Protocolo-protégido autenticação extensível EAP (EAP-PEAP) é configurado.



O perfil da autorização do **acesso direto do dot1x ISE** é selecionado. O interruptor transfere a lista de acessos a fim conceder o acesso direto:

```
3750#show authentication sessions interface g0/17
  Interface: GigabitEthernet0/17
  MAC Address: 0050.b611.ed31
  IP Address: 10.221.0.240
  User-Name: cisco
    Status: Authz Success
    Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: N/A
    ACS ACL: xACSACLx-IP-PERMIT_ALL-53fc9dbe
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A01000C000037E6BAB267CF
  Acct Session ID: 0x00003A70
  Handle: 0xA100080E
```

```
Runnable methods list:
  Method   State
  dot1x    Authc Success
```

```
3750#show ip access-lists interface g0/17
  permit ip any any
```

Step4. Microsoft Windows PC envia o pacote que provoca o alarme

Isto mostra o que acontece se você envia de um pacote de Microsoft Windows com TTL = 7:

```
3750#show authentication sessions interface g0/17
  Interface: GigabitEthernet0/17
  MAC Address: 0050.b611.ed31
  IP Address: 10.221.0.240
  User-Name: cisco
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: N/A
  ACS ACL: xACSACLx-IP-PERMIT_ALL-53fc9dbe
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A01000C000037E6BAB267CF
  Acct Session ID: 0x00003A70
  Handle: 0xA100080E
```

```
Runnable methods list:
  Method   State
  dot1x    Authc Success
```

```
3750#show ip access-lists interface g0/17
  permit ip any any
```

Que o valor está decrescido no Snort na corrente da transmissão e em um alarme é aumentado. Em consequência, um mensagem do syslog para o pxLog é enviado:

```
Sep  6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 ->
10.222.0.61
```

Step5. pxLog

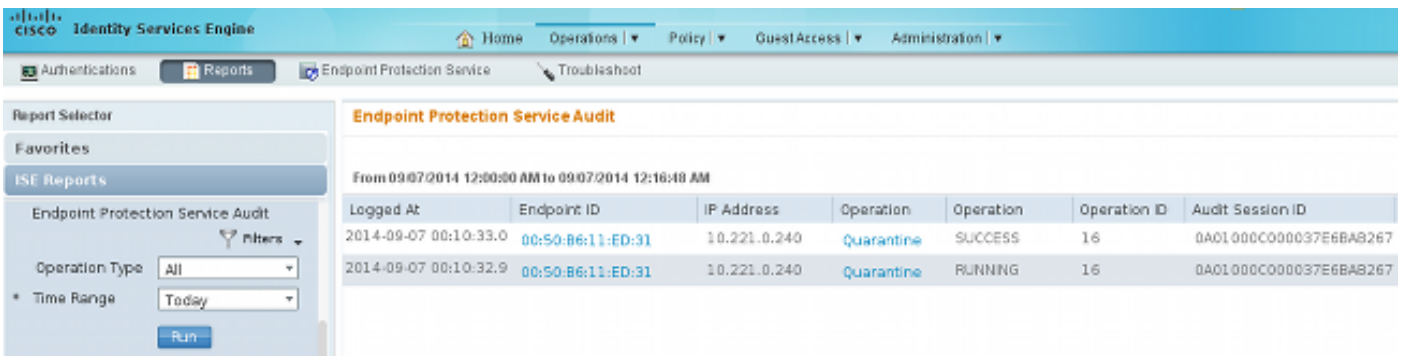
O pxLog recebe o mensagem do syslog, processa-o, e pede-o para quarantine esse endereço IP de Um ou Mais Servidores Cisco ICM NT. Isto pode ser confirmado se você verifica os logs:

Logs from the actions executed by the Enforcer module

Id	Type	Action	Syslog message	IP
66	SYSLOG	QUARANTINE	Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61	10.221.0.240

Step6. Quarentena ISE

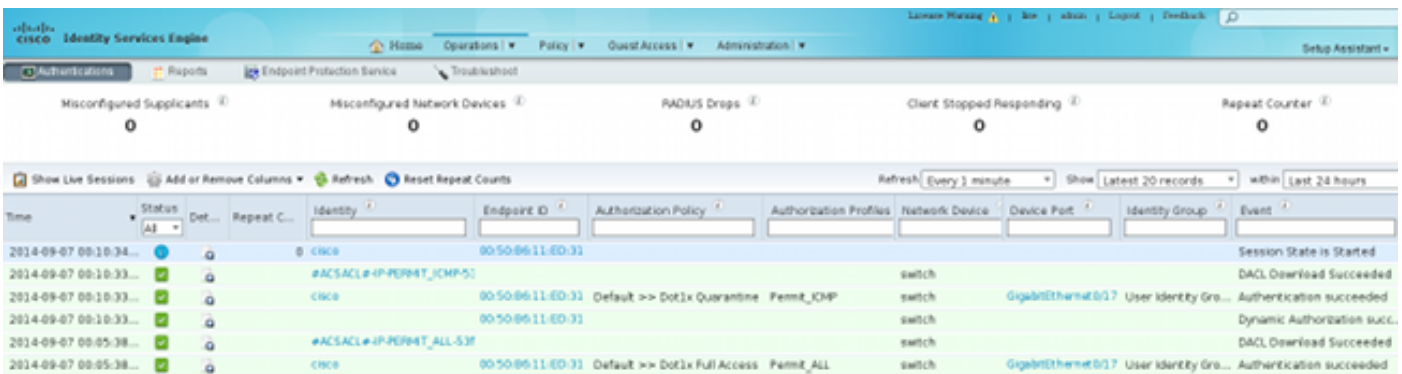
O ISE relata que o endereço IP de Um ou Mais Servidores Cisco ICM NT quarantined:



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The main content area displays the 'Endpoint Protection Service Audit' report for the period from 09/07/2014 12:00:00 AM to 09/07/2014 12:16:48 AM. The report includes a table with the following columns: Logged At, Endpoint ID, IP Address, Operation, Operation, Operation ID, and Audit Session ID. Two entries are visible, both showing a 'Quarantine' operation with a 'SUCCESS' status.

Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session ID
2014-09-07 00:10:33.0	00:50:B6:11:ED:31	10.221.0.240	Quarantine	SUCCESS	16	0A01000C000037E6B8267
2014-09-07 00:10:32.9	00:50:B6:11:ED:31	10.221.0.240	Quarantine	RUNNING	16	0A01000C000037E6B8267

Em consequência, revê a política da autorização, escolhe a quarentena, e envia o CoA do RAI0 a fim atualizar o estado de autorização no interruptor para esse valor-limite específico.



The screenshot shows the Cisco Identity Services Engine (ISE) interface displaying the 'Live Sessions' table. The table includes columns for Time, Status, Det., Repeat C., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, Network Device, Device Port, Identity Group, and Event. The table shows several sessions, including one with a 'Session State is Started' event and another with a 'CoA' event.

Time	Status	Det.	Repeat C.	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Event
2014-09-07 00:10:34...	0	cisco	00:50:B6:11:ED:31						Session State is Started
2014-09-07 00:10:33...	#ACSACL#IP-PEPH4T_ICMP50	00:50:B6:11:ED:31	Default >> Dot1x Quarantine Permit_ICMP		switch			DACL Download Succeeded
2014-09-07 00:10:33...	cisco	00:50:B6:11:ED:31	Default >> Dot1x Quarantine Permit_ICMP		switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded
2014-09-07 00:10:33...	#ACSACL#IP-PEPH4T_ALL_53F	00:50:B6:11:ED:31			switch			Dynamic Authorization succ.
2014-09-07 00:05:38...	cisco	00:50:B6:11:ED:31	Default >> Dot1x Full Access Permit_ALL		switch	GigabitEthernet0/17	User Identity Gro...	DACL Download Succeeded
2014-09-07 00:05:38...	cisco	00:50:B6:11:ED:31	Default >> Dot1x Full Access Permit_ALL		switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded

Aquele é o CoA termina a mensagem que força o suplicante para iniciar uma sessão nova e para obter acesso limitado (Permit_ICMP):

No.	Source	Destination	Protocol	Length	Info
580	10.62.71.140	10.62.97.40	RADIUS	326	Accounting-Request(4) (id=157, l=284)
581	10.62.97.40	10.62.71.140	RADIUS	238	Access-Accept(2) (id=113, l=196)
582	10.62.97.40	10.62.71.140	RADIUS	62	Accounting-Response(5) (id=157, l=20)
2536	10.62.97.40	10.62.71.140	RADIUS	176	Disconnect-Request(40) (id=3, l=134)
2537	10.62.71.140	10.62.97.40	RADIUS	62	Disconnect-ACK(41) (id=3, l=20)
2538	10.62.71.140	10.62.97.40	RADIUS	394	Accounting-Request(4) (id=158, l=352)
2541	10.62.97.40	10.62.71.140	RADIUS	62	Accounting-Response(5) (id=158, l=20)
2545	10.62.71.140	10.62.97.40	RADIUS	272	Access-Request(1) (id=114, l=230)
2546	10.62.97.40	10.62.71.140	RADIUS	160	Access-Challenge(11) (id=114, l=118)

```

> Internet Protocol Version 4, Src: 10.62.97.40 (10.62.97.40), Dst: 10.62.71.140 (10.62.71.140)
> User Datagram Protocol, Src Port: 45006 (45006), Dst Port: mps-raft (1700)
< RADIUS Protocol
  Code: Disconnect-Request (40)
  Packet identifier: 0x3 (3)
  Length: 134
  Authenticator: 21ed5cda0eacbf87659a5e1dce9d0598
  \[The response to this request is in frame 2537\]
  Attribute Value Pairs
    > AVP: l=6 t=NAS-IP-Address(4): 10.62.71.140
    > AVP: l=19 t=Calling-Station-Id(31): 00:50:B6:11:ED:31
    > AVP: l=10 t=Acct-Session-Id(44): 00003A6B
    > AVP: l=6 t=Acct-Terminate-Cause(49): Admin-Reset(6)
    > AVP: l=6 t=Event-Timestamp(55): Sep 7, 2014 00:00:00.000000000 CEST
    > AVP: l=18 t=Message-Authenticator(80): 587cfbaf54769d84f092ffd233b96427
    > AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)

```

O resultado pode ser confirmado no interruptor (acesso limitado para o valor-limite):

```

3750#show authentication sessions interface g0/17
  Interface: GigabitEthernet0/17
  MAC Address: 0050.b611.ed31
  IP Address: 10.221.0.240
  User-Name: cisco
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: N/A
  ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A01000C000037E7BAB7D68C
  Acct Session ID: 0x00003A71
  Handle: 0xE000080F

Runnable methods list:
  Method  State
  dot1x   Authc Success

```

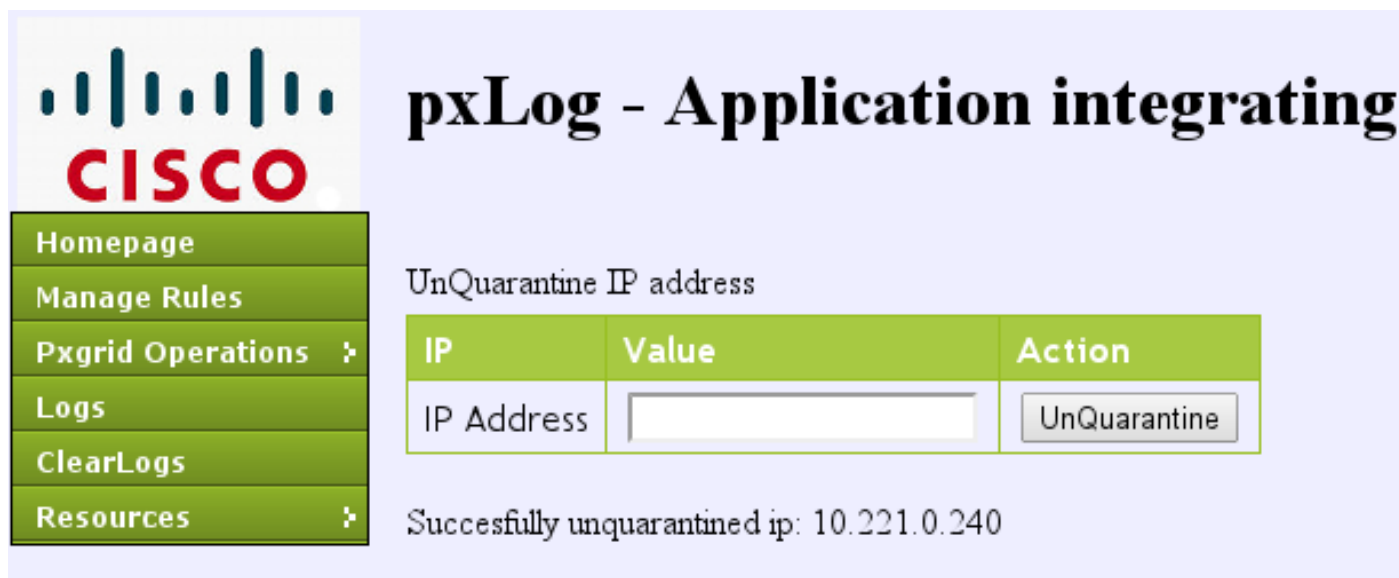
```

3750#show ip access-lists interface g0/17
  permit icmp any any

```

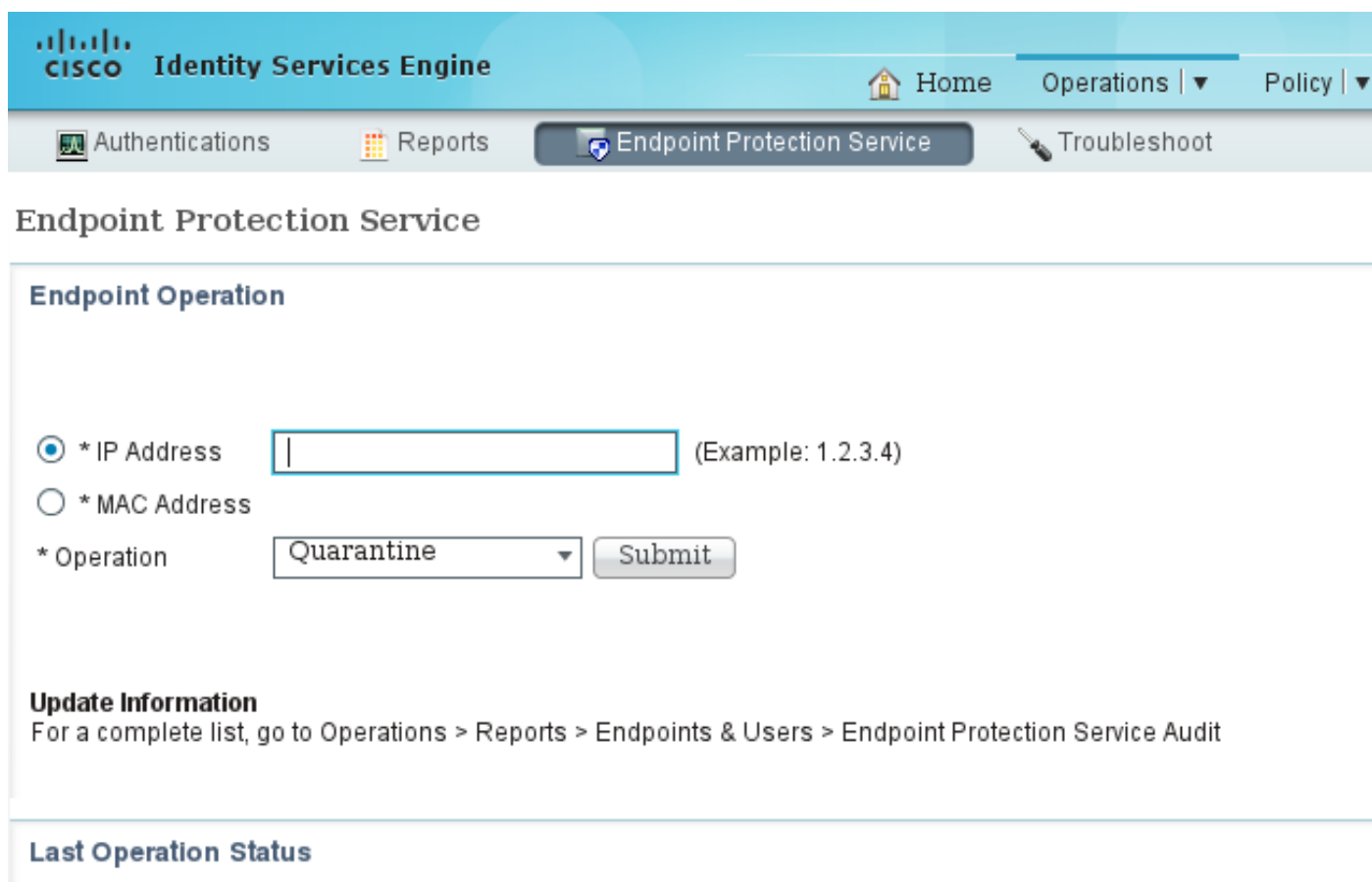
Step7. pxLog Unquarantine

Nesta fase, o administrador decide ao unquarantine que valor-limite:



The screenshot shows the Cisco pxLog interface. On the left is a navigation menu with items: Homepage, Manage Rules, Pxgrid Operations, Logs, ClearLogs, and Resources. The main content area is titled "pxLog - Application integrating" and contains a form for "UnQuarantine IP address". The form has a table with columns "IP", "Value", and "Action". The "IP" column contains "IP Address", the "Value" column has an empty text input field, and the "Action" column has a button labeled "UnQuarantine". Below the form, a message states "Succesfully unquarantined ip: 10.221.0.240".

A mesma operação pode ser executada diretamente do ISE:



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes "Cisco Identity Services Engine" and links for Home, Operations, and Policy. Below this is a secondary navigation bar with "Authentications", "Reports", "Endpoint Protection Service" (highlighted), and "Troubleshoot". The main content area is titled "Endpoint Protection Service" and contains a section for "Endpoint Operation". This section has two radio buttons: "* IP Address" (selected) and "* MAC Address". The "* IP Address" option has a text input field and the text "(Example: 1.2.3.4)". Below the radio buttons is a dropdown menu for "* Operation" set to "Quarantine" and a "Submit" button. At the bottom of the section is "Update Information" with the text: "For a complete list, go to Operations > Reports > Endpoints & Users > Endpoint Protection Service Audit".

Step8. ISE Unquarantine

O ISE outra vez revê as regras e atualiza o estado de autorização no interruptor (o acesso de rede completo é concedido):

Time	Status	Del...	A	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Event
2014-09-07 00:21:11...	●			osco	00:50:86:11:ED:31						Session State is Started
2014-09-07 00:21:10...	●			#ACSACL#-IP/PERMIT_ALL-1				switch			DACL Download Succeeded
2014-09-07 00:21:10...	●			osco	00:50:86:11:ED:31	Default => Dat1= Full Access	Permit_ALL	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded
2014-09-07 00:21:10...	●			#ACSACL#-IP/PERMIT_ALL-1				switch			Dynamic Authorization succeeded
2014-09-07 00:10:33...	●			#ACSACL#-IP/PERMIT_CHMP				switch			DACL Download Succeeded
2014-09-07 00:10:33...	●			osco	00:50:86:11:ED:31	Default => Dat1= Quarantine	Permit_CHMP	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded
2014-09-07 00:10:33...	●			#ACSACL#-IP/PERMIT_ALL-1				switch			Dynamic Authorization succeeded
2014-09-07 00:05:38...	●			#ACSACL#-IP/PERMIT_ALL-1				switch			DACL Download Succeeded
2014-09-07 00:05:38...	●			osco	00:50:86:11:ED:31	Default => Dat1= Full Access	Permit_ALL	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded

O relatório confirma:

Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session ID
2014-09-07 00:21:10.342	00:50:86:11:ED:31	10.221.0.240	Unquarantine	SUCCESS	17	0A01000C000037E7B8B7D68C
2014-09-07 00:21:10.309	00:50:86:11:ED:31	10.221.0.240	Unquarantine	RUNNING	17	0A01000C000037E7B8B7D68C
2014-09-07 00:10:33.095	00:50:86:11:ED:31	10.221.0.240	Quarantine	SUCCESS	16	0A01000C000037E68AB267CF
2014-09-07 00:10:32.973	00:50:86:11:ED:31	10.221.0.240	Quarantine	RUNNING	16	0A01000C000037E68AB267CF

funcionalidade do pxLog

O aplicativo do pxLog foi escrito a fim demonstrar a funcionalidade do pxGrid API. Permite-o a:

- Registrar a sessão e os usuários EP no ISE
- Transfira a informação sobre todas as sessões ativas no ISE
- Transfira a informação sobre uma sessão ativa específica no ISE (pelo endereço IP de Um ou Mais Servidores Cisco ICM NT)
- Transfira a informação sobre um usuário ativo específico no ISE (pelo username)
- Indique a informação sobre todos os perfis (o perfilador)
- Indique a informação sobre as etiquetas do grupo de segurança de TrustSec (SGTs) definida no ISE
- Verifique a versão (as capacidades de pxGrid)
- Quarantine baseado no IP ou no MAC address
- Unquarantine baseou no IP ou no MAC address

Mais funcionalidade é planejada no futuro.

Estão aqui alguns screenshots do exemplo do pxLog:



pxLog - Application integrating IPS with

Homepage

Manage Rules

Pxgrid Operations >

Logs

ClearLogs

Resources >

List of the users with active sessions downloaded from ISE via pxgrid

User	Groups
cisco	User Identity Groups:Employee,User Identity Groups:VPN,Unknown



pxLog - Application integrating IPS with Cisco ISE using pxgrid

Homepage

Manage Rules

Pxgrid Operations >

Logs

ClearLogs

List of active sessions on ISE

Id	User	Domain	MAC	State	ESPStatus	SGT	Profile	NAS IP	NAS Port	AVP
0	cisco		00:50:B6:11:ED:31	Started			Unknown	10.62.71.140	GigabitEthernet0/17	Acct-Session-Id 00003A72



pxLog - Application integrating IPS with Cisco ISE using pxgrid

Homepage

Manage Rules

Pxgrid Operations >

Logs

ClearLogs

Resources >

Display session by IP address

IP	Value	Action
IP Address	<input type="text" value="10.221.0.240"/>	<input type="button" value="Display"/>

List of the sessions found by IP

Id	User	Domain	MAC	State	ESPStatus	SGT	Profile	NAS IP	NAS Port	AVP
0	cisco		00:50:B6:11:ED:31	Started			Unknown	10.62.71.140	GigabitEthernet0/17	Acct-Session-Id 00003A72



pxLog - Application integrating IPS with Cisco ISE using pxgrid

Homepage

Manage Rules

Pxgrid Operations >

Logs

ClearLogs

Resources >

List of SGT tags downloaded from ISE via pxgrid

Id	SGT Name	SGT Description	SGT number
a14bc9f0-3597-11e4-81d2-0050569c3ff3	Marketing		3
0c2ca0f0-3598-11e4-81d2-0050569c3ff3	Quarantined	Users violating policies, limited access	2
9c903db0-3597-11e4-81d2-0050569c3ff3	IT		2
173025d0-3598-11e4-81d2-0050569c3ff3	Development		6
06ce9320-3598-11e4-81d2-0050569c3ff3	VPN	Anyconnect Ikev2 sessions	2
d006f0b0-2c02-11e4-907b-005056bf2f0a	ANY	Any Security Group	65535
cff3b6d0-2c02-11e4-907b-005056bf2f0a	Unknown	Unknown Security Group	0
1c6527d0-3598-11e4-81d2-0050569c3ff3	Finance	Only for audits	2



pxLog - Application integrating IPS with Cisco ISE using pxgrid

- Homepage
- Manage Rules
- Pxgrid Operations >
- Logs
- ClearLogs
- Resources >

List of the profile download from ISE via pxgrid

Profile Id	Profile Name	Full Profile Name
0e4d9640-2c02-11e4-907b-005056bf2f0a	Xerox-WorkCentre-5020-dn	Xerox-Device:Xerox-WorkCentre-5020-dn
1657b140-2c02-11e4-907b-005056bf2f0a	Cisco-AP-Aironet-1240	Cisco-Device:Cisco-Access-Point:Cisco-AP-Aironet-1240
0a3e9db0-2c02-11e4-907b-005056bf2f0a	Xerox-Phaser-6140dn	Xerox-Device:Xerox-Phaser-6140dn
1f4e0100-2c02-11e4-907b-005056bf2f0a	VMWare-Device	VMWare-Device
ff876410-2c01-11e4-907b-005056bf2f0a	Cisco-WLC	Cisco-Device:Cisco-WLC
0d40e130-2c02-11e4-907b-005056bf2f0a	Xerox-Phaser-8860mp	Xerox-Device:Xerox-Phaser-8860mp
0bd6a2d0-2c02-11e4-907b-005056bf2f0a	Xerox-Phaser-7500dx	Xerox-Device:Xerox-Phaser-7500dx
21e43c40-2c02-11e4-907b-005056bf2f0a	Philips-Intellivue	Philips-Device:Philips-Intellivue
15d7f9f0-2c02-11e4-907b-005056bf2f0a	DLINK-DAP-1522	DLINK-Device:DLINK-DAP-1522
0eb5f500-2c02-11e4-907b-005056bf2f0a	Xerox-WorkCentre-5225	Xerox-Device:Xerox-WorkCentre-5225

requisitos de protocolo do pxGrid

Grupos

O cliente (usuário) pode ser um membro de um grupo de cada vez. Os dois grupos os mais de uso geral são:

- Sessão - Usado a fim consultar/informação da transferência sobre sessões/perfis/SGTs
- EP - Usado a fim executar a quarentena

Certificados e Javas KeyStore

Como mencionado previamente, o controlador de ambos os aplicativos do cliente, de pxLog e de pxGrid (ISE), deve ter os Certificados configurados a fim comunicar-se. O aplicativo do pxLog mantém aqueles nos arquivos de KeyStore das Javas:

- **loja/client.jks** - Inclui o cliente e os Certificados do Certificate Authority (CA)
- **loja/root.jks** - Inclui a corrente ISE: Identidade do nó da monitoração e do Troubleshooting (MNT) e o certificado de CA

Os arquivos são protegidos pela senha (padrão: cisco123). O local de arquivo e as senhas podem ser mudados em **WEB-INF/web.xml**.

Estão aqui as etapas para gerar uma Java nova KeyStore:

1. A fim criar um keystore da raiz (confiada), importe o certificado de CA (**cert-ca.der** deve estar no formato DER):

```
3750#show authentication sessions interface g0/17
      Interface: GigabitEthernet0/17
      MAC Address: 0050.b611.ed31
      IP Address: 10.221.0.240
      User-Name: cisco
      Status: Authz Success
      Domain: DATA
      Security Policy: Should Secure
```

```
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A01000C000037E7BAB7D68C
Acct Session ID: 0x00003A71
Handle: 0xE000080F
```

Runnable methods list:

```
Method State
dot1x Authc Success
```

```
3750#show ip access-lists interface g0/17
permit icmp any any
```

2. Quando você cria um keystore novo, escolha uma senha, que seja usada mais tarde a fim alcançar o keystore.
3. Importe o certificado de identidade MNT ao keystore da raiz (**cert-mnt.der é o certificado de identidade tomado do ISE e deve estar no formato DER**):

```
3750#show authentication sessions interface g0/17
Interface: GigabitEthernet0/17
MAC Address: 0050.b611.ed31
IP Address: 10.221.0.240
User-Name: cisco
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A01000C000037E7BAB7D68C
Acct Session ID: 0x00003A71
Handle: 0xE000080F
```

Runnable methods list:

```
Method State
dot1x Authc Success
```

```
3750#show ip access-lists interface g0/17
permit icmp any any
```

4. A fim criar o keystore do cliente, importe o certificado de CA:

```
3750#show authentication sessions interface g0/17
```

```
Interface: GigabitEthernet0/17
MAC Address: 0050.b611.ed31
IP Address: 10.221.0.240
User-Name: cisco
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A01000C000037E7BAB7D68C
Acct Session ID: 0x00003A71
Handle: 0xE000080F
```

Runnable methods list:

```
Method State
dot1x Authc Success
```

```
3750#show ip access-lists interface g0/17
permit icmp any any
```

5. Crie uma chave privada no keystore do cliente:

```
3750#show authentication sessions interface g0/17
Interface: GigabitEthernet0/17
MAC Address: 0050.b611.ed31
IP Address: 10.221.0.240
User-Name: cisco
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A01000C000037E7BAB7D68C
Acct Session ID: 0x00003A71
Handle: 0xE000080F
```

Runnable methods list:

```
Method State
dot1x Authc Success
```

```
3750#show ip access-lists interface g0/17
permit icmp any any
```

6. Gerencia uma solicitação de assinatura de certificado (CSR) no keystore do cliente:

```
3750#show authentication sessions interface g0/17
  Interface: GigabitEthernet0/17
  MAC Address: 0050.b611.ed31
  IP Address: 10.221.0.240
  User-Name: cisco
    Status: Authz Success
    Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: N/A
    ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A01000C000037E7BAB7D68C
  Acct Session ID: 0x00003A71
  Handle: 0xE000080F
```

```
Runnable methods list:
  Method  State
  dot1x   Authc Success
```

```
3750#show ip access-lists interface g0/17
  permit icmp any any
```

7. Assine o **cert-client.csr** e importe o certificado de cliente assinado:

```
3750#show authentication sessions interface g0/17
  Interface: GigabitEthernet0/17
  MAC Address: 0050.b611.ed31
  IP Address: 10.221.0.240
  User-Name: cisco
    Status: Authz Success
    Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: N/A
    ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A01000C000037E7BAB7D68C
  Acct Session ID: 0x00003A71
  Handle: 0xE000080F
```

```
Runnable methods list:
  Method  State
  dot1x   Authc Success
```

```
3750#show ip access-lists interface g0/17
  permit icmp any any
```

8. Verifique que ambos os keystores contêm os Certificados corretos:

```

3750#show authentication sessions interface g0/17
    Interface: GigabitEthernet0/17
    MAC Address: 0050.b611.ed31
    IP Address: 10.221.0.240
    User-Name: cisco
    Status: Authz Success
    Domain: DATA
    Security Policy: Should Secure
    Security Status: Unsecure
    Oper host mode: single-host
    Oper control dir: both
    Authorized By: Authentication Server
    Vlan Policy: N/A
    ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
    Session timeout: N/A
    Idle timeout: N/A
    Common Session ID: 0A01000C000037E7BAB7D68C
    Acct Session ID: 0x00003A71
    Handle: 0xE000080F

Runnable methods list:
    Method    State
    dot1x     Authc Success

3750#show ip access-lists interface g0/17
    permit icmp any any

```

Caution: Quando o nó ISE 1.3 é promovido, há uma opção para manter o certificado de identidade, mas a assinatura de CA é removida. Em consequência, o ISE promovido usa um certificado novo mas nunca anexa o certificado de CA na mensagem SSL/ServerHello. Isto provoca a falha no cliente que espera (conforme o RFC) ver uma corrente completa.

Hostname

O pxGrid API para diversas funções (como a transferência da sessão) executa a validação adicional. O cliente contacta o ISE e recebe o hostname ISE, que é definido pelo comando hostname no CLI. Então, o cliente tenta executar a resolução de DNS para esse hostname e tenta contactar e buscar dados desse endereço IP de Um ou Mais Servidores Cisco ICM NT. Se a resolução de DNS para o hostname ISE falha, o cliente não tenta obter nenhuns dados.

Caution: Observe que somente o hostname está usado para esta definição, que é **lise** nesta encenação, não o nome de domínio totalmente qualificado (FQDN), que é **lise.example.com** nesta encenação.

Note para colaboradores

Cisco publica e apoia o pxGrid API. Há um pacote nomeado como este:

pxgrid-sdk-1.0.0-167

Dentro de há:

- arquivos jar do pxGrid com classes, que podem facilmente ser decodificadas aos arquivos das Javas para verificar o código
- Javas KeyStores da amostra com Certificados
- Scripts da amostra que usam os classess das Javas da amostra que usam o pxGrid

Syslog

Está aqui a lista de soluções da Segurança que enviam mensagens do syslog com o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante. Estes podem facilmente ser integrados com pxLog enquanto você usa a regra correta do regexp na configuração.

Snort

O Snort envia alertas do Syslog neste formato:

```
3750#show authentication sessions interface g0/17
    Interface: GigabitEthernet0/17
    MAC Address: 0050.b611.ed31
    IP Address: 10.221.0.240
    User-Name: cisco
    Status: Authz Success
    Domain: DATA
    Security Policy: Should Secure
    Security Status: Unsecure
    Oper host mode: single-host
    Oper control dir: both
    Authorized By: Authentication Server
    Vlan Policy: N/A
    ACS ACL: xACSACLx-IP-PERMIT_ICMP-53fc9dc5
    Session timeout: N/A
    Idle timeout: N/A
    Common Session ID: 0A01000C000037E7BAB7D68C
    Acct Session ID: 0x00003A71
    Handle: 0xE000080F

Runnable methods list:
    Method  State
    dot1x   Authc Success
```

```
3750#show ip access-lists interface g0/17
    permit icmp any any
```

Aqui está um exemplo:

```
snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61
```

O endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante é sempre o segundo antes do último (destino). É simples construir um regexp granulado para uma assinatura específica e extrair o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante. Está aqui um regexp do exemplo para a assinatura 100124 e o Internet Control Message Protocol (ICMP) da mensagem:

```
snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61
```

Inspeção adaptável da ferramenta de segurança de Cisco (ASA)

Quando o ASA está configurado para a inspeção HTTP (exemplo), o mensagem syslog correspondente olha como este:

```
Mar 12 2014 14:36:20: %ASA-5-415006: HTTP - matched Class 23:
MS13-025_class in policy-map MS_Mar_2013_policy, URI matched -
Dropping connection from inside:192.168.60.88/2135 to
outside:192.0.2.63/80
```

Outra vez um regexp granulado podia ser usado a fim filtrar aquelas mensagens e extrair o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante, o segundo antes do último.

Sistemas da prevenção de intrusão da próxima geração de Cisco Sourcefire (NGIPS)

Está aqui um mensagem de exemplo enviado pelo sensor de Sourcefire:

```
Jan 28 19:46:19 IDS01 SFIMS: [CA IDS][Policy1][119:15:1] http_inspect: OVERSIZE
REQUEST-URI DIRECTORY [Classification: Potentially Bad Traffic] [Priority: 2]
{TCP} 10.12.253.47:55504 -> 10.15.224.60:80
```

Tão outra vez, é simples extrair o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante porque a mesma lógica se aplica. Igualmente o nome da política e a assinatura são fornecidos, assim que a regra do pxLog pode ser granulada.

NetScreen do zimbros

Está aqui um mensagem de exemplo enviado pela intrusion detection do zimbros & pela prevenção mais velhas (IDP):

```
dayId="20061012" recordId="0" timeRecv="2006/10/12
21:52:21" timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0"
device_ip="10.209.83.4" cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN"
srcZn="NULL" srcIntf="NULL" srcAddr="192.168.170.20" srcPort="63396"
natSrcAddr="NULL" natSrcPort="0" dstZn="NULL" dstIntf="NULL"
dstAddr="192.168.170.10" dstPort="27374" natDstAddr="NULL" natDstPort="0"
protocol="TCP" ruleDomain="" ruleVer="5" policy="Policy2" rulebase="IDS"
ruleNo="4" action="NONE" severity="LOW" alert="no" elapsedTime="0" inbytes="0"
outbytes="0" totBytes="0" inPak="0" outPak="0" totPak="0" repCount="0"
packetData="no" varEnum="31" misc="<017>'interface=eth2" user="NULL"
app="NULL" uri="NULL"
```

O endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante pode ser extraído da mesma forma.

Zimbros JunOS

JunOS é similar:

```
Jul 16 10:09:39 JuniperJunOS: asp[8265]:  
ASP_IDS_TCP_SYN_ATTACK: asp 3: proto 6 (TCP),  
ge-0/0/1.0 10.60.0.123:2280 -> 192.168.1.12:80, TCP  
SYN flood attack
```

Iptables de Linux

Estão aqui alguns iptables de Linux do exemplo.

```
Jun 15 23:37:33 netfilter kernel: Inbound IN=lo OUT=  
MAC=00:13:d3:38:b6:e4:00:01:5c:22:9b:c2:08:00 src=10.0.0.1 DST=10.0.0.100 LEN=60  
TOS=0x10 PREC=0x00 TTL=64 ID=47312 DF PROTO=TCP SPT=40945 DPT=3003 WINDOW=32767  
RES=0x00 SYN URGP=0
```

Você pode enviar a informação de syslog para qualquer tipo de pacote com a funcionalidade avançada fornecida pelos módulos iptable como a conexão que segue, xtables, rfilters, correspondência de padrão, e assim por diante.

FreeBSD IPFirewall (IPFW)

Está aqui um mensagem de exemplo para IPFW que obstrui fragmentos:

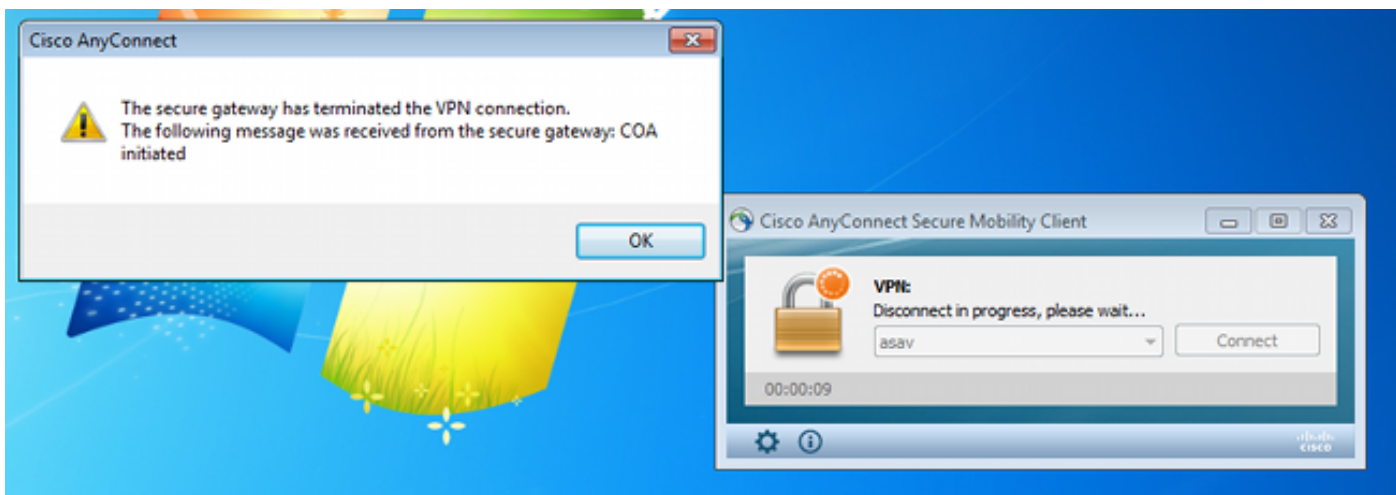
```
Sep 7 15:03:14 delta ipfw: 11400 Deny UDP 10.61.216.50 10.81.199.2 in via fxp0  
(frag 52639:519@1480)
```

Prontidão VPN e manipulação CoA

O ISE pode reconhecer o tipo de sessões em termos da manipulação CoA.

- Para um desvio prendido da autenticação 802.1x/MAC (MAB), o ISE envia o CoA reauthenticate, que provoca uma segunda autenticação.
- Para um Sem fio 802.1x/MAB, o ISE envia o CoA termina, que provoca uma segunda autenticação.
- Para um ASA VPN, o ISE envia um CoA com um DACL novo anexado (nenhuma segunda autenticação).

O módulo EP é simples. Quando executa uma quarentena, envia sempre um CoA termina o pacote. Para sessões prendidas/wireless, não é um problema (todos os suplicantes do 802.1x podem iniciar transparentemente uma segunda sessão EAP). Mas quando o ASA recebe o CoA termine, ele deixa cair a sessão de VPN e o utilizador final é apresentado com este:



Há duas soluções possíveis para forçar o AnyConnect VPN para reconectar automaticamente (configurado no perfil XML):

- Autoreconnect, que trabalha somente quando você perder a conexão com o gateway de VPN, não para a terminação administrativa
- Sempre-em, que trabalha e forças AnyConnect para restabelecer automaticamente a sessão. Mesmo quando a sessão nova é estabelecida, o ASA escolhe a auditoria-sessão-identificação nova. Do ponto de vista ISE, esta é uma sessão nova e não há nenhuma possibilidade encontrar a regra da quarentena. Igualmente para os VPN, não é possível usar o MAC address do valor-limite como a identidade, ao contrário dot1x prendido/wireless.

A solução é forçar os EP para comportar-se como o ISE e para enviar o tipo correto de CoA baseado na sessão. Esta funcionalidade será introduzida na versão 1.3.1 ISE.

Parceiros e soluções do pxGrid

Está aqui uma lista de Parceiros e de soluções do pxGrid:

- LogRhythm (informação de segurança e gerenciamento de evento (SIEM)) - Apoia transferência representacional do estado (RESTO) API
- Splunk (SIEM) - Apoia o RESTO API
- HP Arcsight (SIEM) - Apoia o RESTO API
- Sentinela NetIQ (SIEM) - Planos para apoiar o pxGrid
- Lancope StealthWatch (SIEM) - Planos para apoiar o pxGrid
- Cisco Sourcefire - Planos para apoiar o pxGrid 1HCY15
- Ferramenta de segurança da Web de Cisco (WSA) - Planos para apoiar o pxGrid em abril de 2014

Estão aqui outros Parceiros e soluções:

- Sustentável (avaliação da vulnerabilidade)
- Emulex (captura de pacote de informação e forense)
- Redes de Bayshore (prevenção de perda de dados (DLP) e Internet da política das coisas (IoT))
- Identidade do sibilo (sinal da identidade e do gerenciamento de acesso (eu estou) /Single

- sobre (SSO))
- Qradar (SIEM)
- LogLogic (SIEM)
- Symantec (Gerenciamento de dispositivo móvel do amd SIEM (MDM))

Refira o [catálogo das soluções do mercado](#) para a lista completa de soluções da Segurança.

ISE API: RESTO contra EREST contra o pxGrid

Há três tipos de API disponíveis na versão 1.3 ISE.

Está aqui uma comparação:

	RESTO	Repousante externo	pxGrid
Autenticação do cliente	username + senha (AUTH básico HTTP)	username + senha (AUTH básico HTTP)	certificado
Separação do privilégio	não	limitado (ERS Admin)	sim (grupos)
Acesso	MNT	MNT	MNT
Transporte	tcp/443 (HTTPS)	tcp/9060 (HTTPS)	tcp/5222 (XMPP)
Método HTTP	GET	GET/POST/PUT	GET/POST
Permitido à revelia	sim	não	não
Número de operações	poucos	muitos	poucos
O CoA termina	apoiado	não	apoiado
O CoA Reauthenticate	apoiado	não	apoiado *
Operações de usuário	não	sim	não
Operações do valor-limite	não	sim	não
Operações do grupo da identidade do valor-limite	não	sim	não
Quarentena (IP, MAC)	não	não	sim
UnQuarantine (IP, MAC)	não	não	sim
PortBounce/parada programada	não	não	sim
Operações de usuário convidado	não	sim	não
Operações do portal do convidado	não	sim	não
Operações do dispositivo de rede	não	sim	não
Operações do grupo de dispositivo de rede	não	sim	não

* Os usos da quarentena unificaram o apoio CoA da versão 1.3.1 ISE.

Downloads

o pxLog pode ser transferido de [Sourceforge](#).

O Software Development Kit (SDK) é já incluído. Para a documentação a mais atrasada SDK e API para o pxGrid, contacte seu sócio ou o Equipe de Conta da Cisco.

Informações Relacionadas

- [RESTO API de Cisco ISE 1.2](#)
- [Cisco ISE 1.2 API repousante externo](#)
- [Guia de administradores de Cisco ISE 1.3](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)