

# Configurar serviços da remediação com ISE e integração da potência de fogo

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Centro de gerenciamento de FireSight \(centro da defesa\)](#)

[Módulo da remediação ISE](#)

[Política da correlação](#)

[ASA](#)

[ISE](#)

[Configurar o dispositivo do acesso de rede \(o NAD\)](#)

[Permita o controle de rede adaptável](#)

[Quarantine DACL](#)

[Perfil da autorização para a quarentena](#)

[Regras da autorização](#)

[Verificar](#)

[AnyConnect inicia a sessão de VPN ASA](#)

[Batida da política da correlação de FireSight](#)

[O ISE executa a quarentena e envia o CoA](#)

[A sessão de VPN é desligada](#)

[Troubleshooting](#)

[FireSight \(centro da defesa\)](#)

[ISE](#)

[Erros](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como usar o módulo da remediação em um dispositivo de Cisco FireSight a fim detectar ataques e automaticamente remediate o atacante com o uso do motor do serviço da identidade de Cisco (ISE) como um servidor da política. O exemplo que é fornecido neste documento descreve-o o método que é usado para a remediação de um usuário remoto VPN que autentique através do ISE, mas pode igualmente ser usado para um 802.1x/MAB/WebAuth prendido ou o usuário Wireless.

Nota: O módulo da remediação que é provido neste documento não é apoiado oficialmente por Cisco. É compartilhado em um portal da comunidade e pode ser usado por qualquer um. Nas versões 5.4 e mais recente, há igualmente um módulo mais novo da remediação disponível que seja baseado no protocolo do *pxGrid*. Este módulo não é apoiado na versão 6.0 mas é planejado ser apoiado nas versões futuras.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN adaptável da ferramenta de segurança de Cisco (ASA)
- Configuração de Cliente de mobilidade Cisco AnyConnect Secure
- Configuração básica de Cisco FireSight
- Configuração básica da potência de fogo de Cisco
- Configuração de Cisco ISE

### Componentes Utilizados

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

- Microsoft Windows 7
- Versão ASA 9.3 de Cisco ou mais atrasado
- Versões de software 1.3 de Cisco ISE e mais atrasado
- Versões 3.0 e mais recente do Cliente de mobilidade Cisco AnyConnect Secure
- Versão 5.4 do centro de gerenciamento de Cisco FireSight
- Versão 5.4 da potência de fogo de Cisco (máquina virtual (VM))

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar

Use a informação que é fornecida nesta seção a fim configurar seu sistema.

Nota: Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

O exemplo que é descrito neste documento usa esta instalação de rede:

Está aqui o fluxo para esta instalação de rede:

1. O usuário inicia uma sessão de VPN remota com o ASA (através da versão 4.0 segura da mobilidade de Cisco AnyConnect).
2. O usuário tenta alcançar `http://172.16.32.1`. (O tráfego se move através da potência de fogo, que é instalada no VM e controlada por FireSight.)
3. A potência de fogo é configurada de modo que obstrua que (inline) o tráfego específico (políticas de acesso), mas ele igualmente tem uma política da correlação que seja provocada. Em consequência, inicia a remediação ISE através da interface de programação de aplicativo do RESTO (API) (o método de *QuarantineByIP*).
4. Uma vez que o ISE recebe o atendimento do RESTO API, olha acima para a sessão e envia uma mudança do RAIO da autorização (CoA) ao ASA, que termina essa sessão.
5. O ASA desliga o usuário VPN. Desde que AnyConnect é configurado com Sempre-em acesso VPN, uma sessão nova é estabelecida; contudo, esta vez uma regra diferente da autorização ISE é combinada (para anfitriões quarantined) e o acesso de rede limitado é fornecido. Nesta fase, não importa como o usuário conecta e autentica à rede; enquanto o ISE é usado para a authentication e autorização, o usuário limitou o acesso de rede devendo quarantine.

Como mencionado previamente, esta encenação trabalha para qualquer tipo da sessão autenticada (VPN, 802.1x/MAB/Webauth prendido, Sem fio 802.1x/MAB/Webauth) enquanto o ISE é usado para a autenticação e os suportes do dispositivo do acesso de rede o CoA do RAIO (todos os dispositivos Cisco modernos).

Dica: A fim mover o usuário fora da quarentena, você pode usar o ISE GUI. As versões futuras do módulo da remediação puderam apoiá-lo.

## Potência de fogo

Nota: Um dispositivo VM é usado para o exemplo que é descrito neste documento. Somente a configuração inicial é executada através do CLI. Todas as políticas são configuradas do centro da defesa de Cisco. Para mais detalhes, refira a [seção Informação Relacionada](#) deste documento.

O VM tem três relações, uma para o Gerenciamento e dois para a inspeção inline

(interno/externo).

Todo o tráfego dos usuários VPN move-se através da potência de fogo.

## Centro de gerenciamento de FireSight (centro da defesa)

### Política do controle de acesso

Depois que você instala as licenças corretas e adiciona o dispositivo da potência de fogo, navegue às **políticas > ao controle de acesso** e crie a política de acesso que é usada a fim deixar cair o tráfego de HTTP a 172.16.32.1:

Todo tráfego restante é aceitado.

### Módulo da remediação ISE

A versão atual do módulo ISE que é compartilhado no portal da comunidade é a *remediação beta 1.3.19 ISE 1.2*:

Navegue às **políticas > às ações > às remediações > aos módulos** e instale o arquivo:

O exemplo correto deve então ser criado. Navegue às **políticas > às ações > às remediações > aos exemplos** e forneça o endereço IP de Um ou Mais Servidores Cisco ICM NT do nó da administração de política (BANDEJA), junto com as credenciais administrativas ISE que são precisadas para o RESTO API (um usuário separado com o papel *ERS Admin* é recomendado):

O endereço IP de origem (atacante) deve igualmente ser usado para a remediação:

### Política da correlação

Você deve agora configurar uma regra específica da correlação. Esta regra é provocada no início da conexão que combina a regra previamente configurada do controle de acesso (*DropTCP80*). A fim configurar a regra, navegue às **políticas > ao Gerenciamento da correlação > da regra**:

Esta regra é usada na política da correlação. Navegue às **políticas > à correlação > ao Gerenciamento de políticas** a fim criar uma política nova, e adicionar então a regra configurada. Clique **Remediate** à direita e adicionar duas ações: **remediação para o sourceIP** (configurado mais cedo) e o **Syslog**:

Assegure-se de que você permita a política da correlação:

## ASA

Um ASA que atue como um gateway de VPN é configurado a fim usar o ISE para a autenticação. É igualmente necessário permitir a contabilidade e o CoA do RAIIO:

```
tunnel-group SSLVPN-FIRESIGHT general-attributes
address-pool POOL-VPN
authentication-server-group ISE
accounting-server-group ISE
default-group-policy POLICY

aaa-server ISE protocol radius
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
key *****

webvpn
enable outside
enable inside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable
error-recovery disable
```

## ISE

### Configurar o dispositivo do acesso de rede (o NAD)

Navegue à **administração > aos dispositivos de rede** e adicionar o ASA que atua como um cliente RADIUS.

### Permita o controle de rede adaptável

Navegue à **administração > ao sistema > aos ajustes > controle de rede adaptável** a fim permitir a quarentena API e a funcionalidade:

Nota: Nas versões 1.3 e anterior, esta característica é chamada *serviço de proteção de Valor-limite*.

### Quarentena DACL

A fim criar um Access Control List carregável (DACL) que é usado para os anfitriões quarantined, navegue à **política > aos resultados > à autorização > ACL baixável**.

### Perfil da autorização para a quarentena

Navegue à **política > aos resultados > à autorização > ao perfil da autorização** e crie um perfil da autorização com o DACL novo:

### Regras da autorização

Você deve criar duas regras da autorização. A primeira regra (ASA-VPN) fornece o acesso direto para todas as sessões de VPN que são terminadas no ASA. A regra *ASA-VPN\_quarantine* está batida para a sessão de VPN reauthenticated quando o host está já na quarentena (o acesso de rede limitado está fornecido).

A fim criar estas regras, navegue à **política > à autorização**:

## Verificar

Use a informação que é fornecida nesta seção a fim verificar que sua configuração trabalha corretamente.

### AnyConnect inicia a sessão de VPN ASA

O ASA cria a sessão sem nenhum DACL (acesso de rede completo):

```
asav# show vpn-sessiondb details anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : cisco                Index          : 37
Assigned IP   : 172.16.50.50         Public IP      : 192.168.10.21
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 18706                Bytes Rx       : 14619
Group Policy  : POLICY                Tunnel Group   : SSLVPN-FIRESIGHT
Login Time    : 03:03:17 UTC Wed May 20 2015
Duration      : 0h:01m:12s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                    VLAN           : none
Audt Sess ID  : ac10206400025000555bf975
Security Grp  : none
```

```
.....
```

```
DTLS-Tunnel:
```

```
<some output omitted for clarity>
```

### O usuário tenta o acesso

Uma vez que o usuário tenta alcançar <http://172.16.32.1>, a política de acesso está batida, o tráfego que corresponde é obstruído inline, e o mensagem do syslog é enviado do endereço IP de gerenciamento da potência de fogo:

```
May 24 09:38:05 172.16.31.205 SFIMS: [Primary Detection Engine
(cbe45720-f0bf-11e4-a9f6-bc538df1390b)][AccessPolicy] Connection Type: Start, User:
Unknown, Client: Unknown, Application Protocol: Unknown, Web App: Unknown,
Access Control Rule Name: DropTCP80, Access Control Rule Action: Block,
Access Control Rule Reasons: Unknown, URL Category: Unknown, URL Reputation:
Risk unknown, URL: Unknown, Interface Ingress: eth1, Interface Egress: eth2,
Security Zone Ingress: Internal, Security Zone Egress: External, Security
Intelligence Matching IP: None, Security Intelligence Category: None, Client Version:
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
```

NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes: 66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A, SSL Cipher Suite: N/A, SSL Certificate: 00000000000000000000000000000000, SSL Subject CN: N/A, SSL Subject Country: N/A, SSL Subject OU: N/A, SSL Subject Org: N/A, SSL Issuer CN: N/A, SSL Issuer Country: N/A, SSL Issuer OU: N/A, SSL Issuer Org: N/A, SSL Valid Start Date: N/A, SSL Valid End Date: N/A, SSL Version: N/A, SSL Server Certificate Status: N/A, SSL Actual Action: N/A, SSL Expected Action: N/A, SSL Server Name: (null), SSL URL Category: N/A, SSL Session ID: 00, SSL Ticket Id: 00, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80

## Batida da política da correlação de FireSight

A política da correlação do Gerenciamento de FireSight (centro da defesa) é batida, que é relatada pelo mensagem do syslog que é enviado do centro da defesa:

```
May 24 09:37:10 172.16.31.206 SFIMS: Correlation Event:
CorrelateTCP80Block/CorrelationPolicy at Sun May 24 09:37:10 2015 UTCTConnection Type:
FireSIGHT 172.16.50.50:49415 (unknown) -> 172.16.32.1:80 (unknown) (tcp)
```

Nesta fase, o centro da defesa usa o atendimento do RESTO API (quarentena) ao ISE, que é uma sessão HTTPS e pode ser decifrado em Wireshark (com o secure sockets layer (SSL) de encaixe e a chave privada do certificado administrativo da BANDEJA):

No GET o pedido para o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante é passado (172.16.50.50), e esse host quarantined pelo ISE.

Navegue à análise > à correlação > ao estado a fim confirmar a remediação bem sucedida:

## O ISE executa a quarentena e envia o CoA

Nesta fase, o ISE *prrt-management.log* notifica que o CoA deve ser enviado:

```
DEBUG [RMI TCP Connection(142)-127.0.0.1][] cisco.cpm.prrt.impl.PrRTLoggerImpl
-:::- send() - request instanceof DisconnectRequest
  clientInstanceIP = 172.16.31.202
  clientInterfaceIP = 172.16.50.50
  portOption = 0
  serverIP = 172.16.31.100
  port = 1700
  timeout = 5
  retries = 3
  attributes = cisco-av-pair=audit-session-id=ac10206400021000555b9d36
Calling-Station-ID=192.168.10.21
Acct-Terminate-Cause=Admin Reset
```

O tempo de execução (*prrt-server.log*) envia o *terminate* message CoA ao NAD, que termina a sessão (ASA):

```
DEBUG,0x7fad17847700,cntx=0000010786,CPMSessionID=2e8cdb62-bc0a-4d3d-a63e-f42ef8774893,
CallingStationID=08:00:27:DA:EF:AD, RADIUS PACKET: Code=40 (
DisconnectRequest) Identifier=9 Length=124
  [4] NAS-IP-Address - value: [172.16.31.100]
  [31] Calling-Station-ID - value: [08:00:27:DA:EF:AD]
  [49] Acct-Terminate-Cause - value: [Admin Reset]
  [55] Event-Timestamp - value: [1432457729]
  [80] Message-Authenticator - value:
[00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00]
  [26] cisco-av-pair - value: [audit-session-id=ac10206400021000555b9d36],
```

RadiusClientHandler.cpp:47

O ise.psc envia uma notificação similar a esta:

```
INFO [admin-http-pool51][ ] cisco.cpm.eps.prrt.PrrtManager -:~::~- PrrtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault
```

Quando você navega às operações > à autenticação, deve mostrar a *autorização dinâmica sucedida*.

## A sessão de VPN é desligada

O utilizador final envia uma notificação a fim indicar que a sessão está desligada (para 802.1x/MAB/guest prendido/Sem fio, este processo é transparente):

Detalhes da mostra dos logs de Cisco AnyConnect:

```
10:48:05 AM Establishing VPN...
10:48:05 AM Connected to 172.16.31.100.
10:48:20 AM Disconnect in progress, please wait...
10:51:20 AM The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: COA initiated
```

## Sessão de VPN com acesso limitado (quarentena)

Porque sempre-no VPN é configurado, a sessão nova é construída imediatamente. Esta vez, a regra ISE ASA-VPN\_quarantine é batida, que fornece o acesso de rede limitado:

Nota: O DACL é transferido em uma requisição RADIUS separada.

Uma sessão com acesso limitado pode ser verificada no ASA com o comando CLI do anyconnect do detalhe da mostra VPN-sessiondb:

```
asav# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : cisco                               Index      : 39
Assigned IP   : 172.16.50.50                       Public IP   : 192.168.10.21
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 11436                               Bytes Rx    : 4084
Pkts Tx       : 8                                   Pkts Rx     : 36
Pkts Tx Drop  : 0                                   Pkts Rx Drop : 0
Group Policy  : POLICY                               Tunnel Group : SSLVPN-FIRESIGHT
Login Time    : 03:43:36 UTC Wed May 20 2015
Duration      : 0h:00m:10s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                               VLAN        : none
Audt Sess ID  : ac10206400027000555c02e8
Security Grp  : none
```

.....



DTLS-Tunnel:

<some output omitted for clarity>

Filter Name : #ACSACL#-IP-DENY\_ALL\_QUARANTINE-5561da76

## Troubleshooting

Esta seção fornece a informação que você pode usar a fim pesquisar defeitos sua configuração.

### FireSight (centro da defesa)

O script da remediação ISE reside neste lugar:

```
root@Defence:/var/sf/remediations/ISE_1.3.19# ls
_lib_ ise-instance ise-test.pl ise.pl module.template
```

Este é um script simples *Perl* que usa o subsistema de registro padrão de SourceFire (SF). Uma vez que a remediação é executada, você pode confirmar os resultados através de */var/log/messages*:

```
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) Starting remediation
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) 172.16.31.202 - Success 200 OK - Quarantined
172.16.50.50 as admin
```

## ISE

É importante que você permite o serviço de controle de rede adaptável no ISE. A fim ver o detalhado entra um processo do tempo de execução (*prrt-management.log* e *prrt-server.log*), você deve permitir o nível de debug para o Runtime-AAA. Navegue à **administração > ao sistema > registrando > debugam a configuração do log** a fim permitir debuga.

Você pode igualmente navegar às **operações > aos relatórios > ao valor-limite e aos usuários > auditoria adaptável do controle de rede** a fim ver a informação para cada tentativa e o resultado de um pedido da quarentena:

## Erros

Refira a identificação de bug Cisco [CSCuu41058](#) (inconsistência da quarentena do valor-limite ISE 1.4 e falha VPN) para obter informações sobre de um erro ISE que seja relacionado às falhas da sessão de VPN (trabalhos 802.1x/MAB muito bem).

## Informações Relacionadas

- [Configurar a integração WSA com o ISE para serviços clientes de TrustSec](#)
- [Integração do pxGrid da versão 1.3 ISE com aplicativo do pxLog IPS](#)
- [Guia do administrador do Cisco Identity Services Engine, liberação 1.4 – Controle de rede](#)

## adaptável da instalação

- [Guia de referência do Cisco Identity Services Engine API, liberação 1.2 – Introdução aos serviços repousantes externos API](#)
- [Guia de referência do Cisco Identity Services Engine API, liberação 1.2 – Introdução ao RESTO API da monitoração](#)
- [Guia do administrador do Cisco Identity Services Engine, liberação 1.3](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)