配置与ISE和Firepower集成的修正服务

目录

简介

本文描述如何使用在思科FireSight设备的修正模块为了检测攻击和自动地修正与使用的攻击者思科身份服务引擎(ISE)作为策略服务器。在本文提供的示例描述使用远程VPN用户修正通过ISE验证的方法，但是它可能也用于802.1x/MAB/WebAuth有线的或无线用户。

> **Note**:被参考本文思科不正式支持的修正模块。它在门户的社区共享，并且可以由任何人使用。在版本5.4和以上，也有根据*pxGrid*协议的一更新的修正模块联机。版本6.0不支持计划未来版本支持此模块，然而。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科可适应安全工具(ASA) VPN配置
- Cisco AnyConnect安全移动客户端配置
- 思科FireSight基本配置
- 思科Firepower基本配置
- 思科ISE配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco ASA版本9.3或以上
- Cisco ISE软件版本1.3及以后
- Cisco AnyConnect安全移动客户端版本3.0和以上
- Cisco FireSight管理中心版本5.4
- 思科Firepower版本5.4 (虚拟机)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

请使用在此部分被提供为了配置您的系统的信息。

> **Note**:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

在本文描述的示例使用此网络设置：

这是此网络设置的流：

1. 用户启动有ASA的一远程VPN会话(通过Cisco AnyConnect安全移动性版本4.0)。
2. 用户尝试访问*http://172.16.32.1*。(流量通过Firepower移动，在VM安装和由FireSight管理。)
3. Firepower配置，以便阻塞(线型)该特定的流量(访问策略)，但是也有被触发的相关性策略。结果，它通过其余Application Programming Interface (API) (*QuarantineByIP*方法)启动ISE修正。
4. 一旦ISE收到其余API呼叫，为会话查寻并且发送RADIUS崔凡吉莱授权(CoA)对ASA，终止该会话。
5. ASA断开VPN用户。因为AnyConnect配置与*不间断工作的*VPN访问，个新会话设立;然而，这次一个不同的ISE授权规则(为被检疫的主机)匹配，并且提供被限制的网络访问。在此阶段，不重要用户如何连接并且验证对网络;只要ISE使用认证和授权，用户限制了由于的网络访问检疫。

如前所提及，此方案为任一种认证的会话(VPN，有线的802.1x/MAB/Webauth工作，无线802.1x/MAB/Webauth)，只要ISE使用验证，并且网络接入设备支持RADIUS CoA (所有现代Cisco设备)。

> **提示**：为了移动用户出于检疫，您能使用ISE GUI。修正模块的未来版本也许也支持它。

Firepower

> **Note**:VM设备使用在本文描述的示例。仅初始配置通过CLI被执行。所有策略从思科防御中心配置。欲了解更详细的信息，参考本文相关信息部分。

VM有三个接口，一管理的和两轴向检查的(内部/外部)。

所有从VPN用户的流量通过Firepower移动。

FireSight管理中心(防御中心)

访问控制策略

在您安装正确许可证并且添加Firepower设备后，请导航到**策略>访问控制**并且创建使用为了下降HTTP数据流到172.16.32.1的访问策略：

其他流量接受。

ISE修正模块

在社区门户共享ISE模块的当前版本是*ISE 1.2修正Beta 1.3.19* ：

导航到**策略>操作>补救>模块**并且安装文件：

应该然后创建正确实例。导航对**策略>操作>补救>实例**并且与为其余API是需要的ISE管理凭证一起提供策略管理节点(PAN)的IP地址， (推荐有*ERS Admin*角色的一个分开的用户) ：

应该也用于源IP地址(攻击者)修正：

相关性策略

您必须当前配置一个特定关联规则。此规则在匹配以前已配置的访问控制规则的连接的开始被触发(*DropTCP80*)。为了配置规则，请导航对**策略>相关性>规则管理**：

此规则用于相关性策略。导航对**策略>相关性>Policy管理**为了创建一项新的策略，然后增加配置的规则。点击在右边的**修正**并且添加两操作：**sourceIP** (及早配置)和**Syslog的修正**：

保证您启用相关性策略：

ASA

ASA作为的VPN网关配置为了使用ISE验证。对启用帐户和RADIUS CoA也是必要的：

```
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

Configure network接入设备(纳季)

导航到作为RADIUS客户端的**Administration >网络设备**并且添加ASA。

启用自适应网络控制

导航到**管理>System >设置>自适应网络控制**为了启用检疫API和功能：

> **Note**:在版本1.3和以下，此功能呼叫*Endpoint保护业务*。

检疫DACL

为了创建可下载的访问控制表(DACL)使用被检疫的主机，请导航对**策略>结果>授权>可下载的ACLs**。

检疫的授权配置文件

导航对**策略>结果>授权>授权配置文件**并且创建与新的DACL的一授权配置文件：

授权规则

您必须创建两个授权规则。第一个规则(ASA-VPN)为在ASA终止的所有VPN会话提供完全权限。规则*ASA-VPN_quarantine*为重新鉴别的VPN会话点击，当主机已经是检疫时(提供有限的网络访问)。

为了创建这些规则，请导航对**策略>授权**：

验证

请使用在此部分被提供为了验证的信息您的配置适当地工作。

AnyConnect启动ASA VPN会话

ASA创建会话，不用任何DACL (全双工网络访问) ：

```
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>
```

用户尝试访问

一旦用户尝试访问http://172.16.32.1，访问策略点击，对应阻塞线型，并且系统消息从Firepower管理IP地址传送的流量：

```
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: 0000000000000000000000000000000000000000,
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:
0000000000000000000000000000000000000000000000000000000000000000, SSL Ticket Id:
00000000000000000000000000000000000000, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80
```

FireSight相关性策略命中数

FireSight管理(防御中心)相关性策略点击，由系统消息报告从防御中心传送：

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

在此阶段，防御中心使用其余API (检疫)呼叫对ISE，是HTTPS会话，并且可以解密在Wireshark (与插件的安全套接字协议层(SSL)和PAN管理证书的专用密钥) ：

在GET要求攻击者的IP地址通过(172.16.50.50)，并且该主机由ISE检疫。

导航对**分析>相关性>状态**为了确认成功的修正：

ISE执行检疫并且发送CoA

在此阶段， ISE *prrt-management.log*通知应该发送CoA ：

```
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
```

运行时间(prrt-server.log)发送CoA terminatemessage给纳季，终止会话(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]
    [26] cisco-av-pair - value: [audit-session-id=ac10206400021000555b9d36],
RadiusClientHandler.cpp:47
```

*ise.psc发送*通知类似于此：

```
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 PDPIPAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault
```

当您导航对**操作>验证时**，应该显示*成功的动态授权*。

VPN会话被断开

最终用户发送通知为了表明会话被断开(对于有线的802.1x/MAB/guest/无线，此进程透明) ：

从思科AnyConnect日志的详细信息显示：

```
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
```

有有限访问的(检疫) VPN会话

由于*不间断工作的VPN*配置，个新会话立即被构件。这时， ISE *ASA-VPN_quarantine*规则点击，提供有限的网络访问：

> **Note**:DACL在一个分开的RADIUS请求下载。

有有限访问的一会话在与CLI命令**显示vpn-sessiondb详细信息的anyconnect的**ASA可以验证：

```
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 ommited for clarity>
  Filter Name  : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

故障排除

此部分提供您能使用为了排除故障您的配置的信息。

FireSight (防御中心)

ISE修正脚本位于此位置：

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

这是使用标准的SourceFire的一个简单*Perl脚本*(SF)记录日志子系统。一旦修正被执行，您能通过*/var/log/messages*证实结果：

```
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

重要的是您启用在ISE的自适应网络管理服务。为了查看详细登陆一运行时进程(*prrt-management.log*和*prrt-server.log*)，您必须启用运行时间AAA的调试级别。导航对**管理>System >记录日志>调试日志配置**为了启用调试。

您能也导航到**操作>报告>终端和用户>自适应网络控制审计**为了查看检疫请求的每种尝试和结果的

信息：

Bug

与VPN会话故障关于ISE bug的信息的参考的Cisco Bug ID CSCuu41058 (ISE 1.4终端检疫不一致和VPN失败) (802.1x/MAB涉及良好工作)。

相关信息

- 配置与ISE的WSA集成TrustSec意识服务的
- ISE版本1.3与IPS pxLog应用程序的pxGrid集成
- 思科身份服务引擎管理员指南，版本1.4 –设置自适应网络控制
- 思科身份服务引擎API参考指南，版本1.2 –外部宁静的服务API简介
- 思科身份服务引擎API参考指南，版本1.2 –监听其余API简介
- 思科身份服务引擎管理员指南，版本1.3
- 技术支持和文档 - Cisco Systems