Servicios de la corrección de la configuración con la integración ISE y de FirePOWER

Contenido

Introducción

Este documento describe cómo utilizar el módulo de la corrección en un dispositivo de Cisco FireSIGHT para detectar los ataques y automáticamente el remediate el atacante con el uso del motor del servicio de la identidad de Cisco (ISE) como servidor de políticas. El ejemplo que se proporciona en este documento describe el método que se utiliza para la corrección de un usuario de VPN remoto que autentique vía el ISE, solamente lo se puede también utilizar para un 802.1x/MAB/WebAuth atado con alambre o el usuario de red inalámbrica.

Note: El módulo de la corrección que se refiere a este documento no es soportado oficialmente por Cisco. Se comparte en una comunidad porta y puede ser utilizado por cualquier persona. En las versiones 5.4 y posterior, hay también un módulo más nuevo de la corrección disponible que se basa en el protocolo del *pxGrid*. Este módulo no se soporta en la versión 6.0 sino se planea para ser soportado en las versiones futuras.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración VPN adaptante del dispositivo de seguridad de Cisco (ASA)
- Configuración de Cliente de movilidad Cisco AnyConnect Secure
- Configuración básica de Cisco FireSIGHT
- Configuración básica de Cisco FirePOWER
- Configuración de Cisco ISE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Versión de ASA 9.3 de Cisco o más adelante
- Versiones de software 1.3 de Cisco ISE y posterior
- 3.0 de las versiones del Cliente de movilidad Cisco AnyConnect Secure y posterior
- Versión 5.4 del centro de administración de Cisco FireSIGHT
- Versión 5.4 de Cisco FirePOWER (máquina virtual (VM))

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Utilice la información que se proporciona en esta sección para configurar su sistema.

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

El ejemplo que se describe en este documento utiliza esta configuración de la red:

Aquí está el flujo para esta configuración de la red:

1. El usuario inicia a una sesión de VPN remota con el ASA (vía la versión 4.0 segura de la movilidad de Cisco AnyConnect).

2. El usuario intenta acceder *http://172.16.32.1*. (El tráfico se mueve vía FirePOWER, que está instalado en el VM y manejado por FireSIGHT.)

3. Se configura FirePOWER de modo que bloquee que (en línea) el tráfico específico (políticas de acceso), solamente él también tiene una directiva de la correlación se accione que. Como consecuencia, inicia la corrección ISE vía la interfaz de programación de aplicaciones del RESTO (API) (el método de *QuarantineByIP*).

4. Una vez que el ISE recibe la llamada del RESTO API, mira para arriba para la sesión y envía un cambio RADIUS de la autorización (CoA) al ASA, que termina esa sesión.

5. El ASA desconecta al usuario de VPN. Puesto que AnyConnect se configura con Siempre-*en el* acceso VPN, se establece una nueva sesión; sin embargo, este vez una diversa regla de la autorización ISE se corresponde con (para los host quarantined) y se proporciona el acceso a la red limitado. En esta etapa, no importa cómo el usuario conecta y autentica a la red; mientras el ISE se utilice para la autenticación y autorización, el usuario ha limitado el acceso a la red debido quarantine.

Como se mencionó anteriormente, este escenario trabaja para cualquier tipo de la sesión autenticada (VPN, 802.1x/MAB/Webauth atado con alambre, la Tecnología inalámbrica 802.1x/MAB/Webauth) mientras el ISE se utilice para la autenticación y las compatibilidades de dispositivos de acceso a la red el CoA RADIUS (todos los dispositivos de Cisco modernos).

> **Tip**: Para mover al usuario de la cuarentena, usted puede utilizar el ISE GUI. Las versiones futuras del módulo de la corrección pudieron también soportarlo.

FirePOWER

> **Note**: Un dispositivo VM se utiliza para el ejemplo que se describe en este documento. Solamente la configuración inicial se realiza vía el CLI. Todas las directivas se configuran del centro de la defensa de Cisco. Para más detalles, refiera a la sección de información relacionada de este documento.

El VM tiene tres interfaces, una para la Administración y dos para el examen en línea (interno y externo).

Todo el tráfico de los usuarios de VPN se mueve vía FirePOWER.

Centro de administración de FireSIGHT (centro de la defensa)

Directiva del control de acceso

Después de que usted instale las licencias correctas y agregue el dispositivo de FirePOWER, navegue a las **directivas > al control de acceso** y cree la política de acceso que se utiliza para caer el tráfico HTTP a 172.16.32.1:

Se valida el resto del tráfico.

Módulo de la corrección ISE

La versión actual del módulo ISE que se comparte en el portal de la comunidad es la *corrección 1.3.19 beta ISE 1.2*:

Navegue a las **directivas > a las acciones > a las correcciones > a los módulos** y instale el archivo:

El caso correcto debe entonces ser creado. Navegue a las **directivas > a las acciones > a las correcciones > a los casos** y proporcione la dirección IP del nodo de la administración de la política (CACEROLA), junto con las credenciales administrativas ISE que son necesarias para el RESTO API (recomiendan un usuario separado con el papel *ERS Admin*):

La dirección IP de origen (atacante) se debe también utilizar para la corrección:

Directiva de la correlación

Usted debe ahora configurar una regla específica de la correlación. Esta regla se acciona al inicio de la conexión que hace juego la regla previamente configurada del control de acceso (*DropTCP80*). Para configurar la regla, navegue a las **directivas > a la Administración de la correlación > de la regla**:

Esta regla se utiliza en la directiva de la correlación. Navegue a las **directivas > a la correlación > a la Administración de políticas** para crear una nueva directiva, y después agregue la regla configurada. Haga clic **Remediate** a la derecha y agregue dos acciones: **corrección para el sourceIP** (configurado anterior) y el **Syslog**:

Asegúrese de que usted habilite la directiva de la correlación:

ASA

Un ASA que actúa como gateway de VPN se configura para utilizar el ISE para la autenticación. Es también necesario habilitar las estadísticas y el CoA RADIUS:

```
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

Dispositivo de acceso a la red (NAD) de la configuración

Navegue a la **administración > a los dispositivos de red** y agregue el ASA que actúa como cliente RADIUS.

Habilite el control de red adaptante

Navegue a la **administración > al sistema > a las configuraciones > control de red adaptante** para habilitar la cuarentena API y las funciones:

> **Note**: En las versiones 1.3 y anterior, esta característica se llama *servicio de protección de Endpoint*.

Cuarentena DACL

Para crear una lista de control de acceso transferible (DACL) que se utilice para los host quarantined, navegue a la **directiva > a los resultados > a la autorización > ACL descargable**.

Perfil de la autorización para la cuarentena

Navegue a la **directiva > a los resultados > a la autorización > al perfil de la autorización** y cree un perfil de la autorización con el nuevo DACL:

Reglas de la autorización

Usted debe crear dos reglas de la autorización. La primera regla (ASA-VPN) proporciona el acceso total para todas las sesiones de VPN que se terminen en el ASA. La regla *ASA-VPN_quarantine* se golpea para la sesión de VPN reauthenticated cuando el host está ya en la cuarentena (se proporciona el acceso a la red limitado).

Para crear estas reglas, navegue a la **directiva > a la autorización**:

Verificación

Utilice la información que se proporciona en esta sección para verificar que su configuración trabaja correctamente.

AnyConnect inicia a la sesión de VPN ASA

El ASA crea la sesión sin ningún DACL (acceso a la red 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>
```

Acceso de las tentativas del usuario

Una vez que el usuario intenta acceder http://172.16.32.1, se golpea la política de acceso, el tráfico que corresponde se bloquea en línea, y el mensaje de Syslog se envía del IP Address de administración de FirePOWER:

```
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**

Golpe de la directiva de la correlación de FireSIGHT

Se golpea la directiva de la correlación de la Administración de FireSIGHT (centro de la defensa), que es señalada por el mensaje de Syslog que se envía del centro de la defensa:

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)

En esta etapa, el centro de la defensa utiliza la llamada del RESTO API (cuarentena) al ISE, que es sesiones HTTP y se puede desencriptar en Wireshark (con Secure Sockets Layer (SSL) plug-in y la clave privada del certificado administrativo de la CACEROLA):

En la petición get para la dirección IP del atacante se pasa (172.16.50.50), y ese host quarantined por el ISE.

Navegue al **análisis > a la correlación > al estatus** para confirmar la corrección acertada:

El ISE realiza la cuarentena y envía el CoA

En esta etapa, el ISE *prrt-management.log* notifica que el CoA debe 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=ac1020640002100055 5b9d36
Calling-Station-ID=192.168.10.21
Acct-Terminate-Cause=Admin Reset
```

El tiempo de ejecución (prrt-server.log) envía el terminatemessage CoA al NAD, que termina la sesión (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
```

El ise.psc envía una notificación similar a esto:

```
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
```

Cuando usted navega a las **operaciones > a la autenticación**, debe mostrar la *autorización dinámica tenida éxito*.

La sesión de VPN es disconnected

El usuario final envía una notificación para indicar que la sesión es disconnected (para 802.1x/MAB/guest atado con alambre/Tecnología inalámbrica, este proceso es transparente):

Detalles de la demostración de los registros 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
```

Sesión de VPN con el acceso limitado (cuarentena)

Porque siempre-*en el VPN* se configura, la nueva sesión se construye inmediatamente. Esta vez, la regla ISE *ASA-VPN_quarantine* se golpea, que proporciona el acceso a la red limitado:

> **Note**: El DACL se descarga en un pedido de RADIUS separado.

Una sesión con el acceso limitado se puede verificar en el ASA con el comando CLI del **anyconnect del detalle de VPN-sessiondb de la demostración**:

```
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
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

FireSIGHT (centro de la defensa)

El script de la corrección ISE reside en esta ubicación:

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

El es un script simple *Perl* que utiliza el subsistema estándar del registro de SourceFire (SF). Una vez que se ejecuta la corrección, usted puede confirmar los resultados vía */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

Es importante que usted habilita el servicio de control de red adaptante en el ISE. Para ver el detallado abre una sesión un proceso del tiempo de ejecución (*prrt-management.log* y *prrt-server.log*), usted debe habilitar el nivel de debug para el Runtime-AAA. Navegue a la **administración > al sistema > a la configuración del registro del registro > del debug** para habilitar los debugs.

Usted puede también navegar a las **operaciones > a los informes > al punto final y a los usuarios > auditoría adaptante del control de red** para ver la información para cada tentativa y el resultado de una petición de la cuarentena:

Bug

Refiera al Id. de bug Cisco CSCuu41058 (inconsistencia de la cuarentena del punto final ISE 1.4 y error VPN) para la información sobre un bug ISE que se relacione con los errores de la sesión de VPN (trabajos 802.1x/MAB muy bien).

Información Relacionada

- Integración de la configuración WSA con el ISE para los servicios enterados de TrustSec
- Integración del pxGrid de la versión 1.3 ISE con la aplicación del pxLog IPS
- Guía del administrador del Cisco Identity Services Engine, versión 1.4 – Control de red adaptante de la configuración
- Guía de referencia del Cisco Identity Services Engine API, versión 1.2 – Introducción a los servicios relajantes externos API
- Guía de referencia del Cisco Identity Services Engine API, versión 1.2 – Introducción al RESTO API de la supervisión
- Guía del administrador del Cisco Identity Services Engine, versión 1.3
- Soporte Técnico y Documentación - Cisco Systems