Configurez les services de correction avec ISE et intégration de puissance de feu

Contenu

Introduction

Ce document décrit comment utiliser le module de correction sur une appliance de Cisco FireSight afin de détecter les attaques et automatiquement le remediate l'attaquant avec l'utilisation de l'engine de gestion d'identité de Cisco (ISE) comme policy server. L'exemple qui est fourni dans ce document décrit la méthode qui est utilisée pour la correction d'un utilisateur du distant VPN qui authentifie par l'intermédiaire de l'ISE, mais lui peut également être utilisé pour un 802.1x/MAB/WebAuth de câble ou l'utilisateur de sans fil.

Remarque: Le module de correction qui est mis en référence dans ce document n'est pas officiellement pris en charge par Cisco. Il est partagé sur une communauté portaile et peut être utilisé par n'importe qui. Dans les versions 5.4 et ultérieures, il y a également un plus nouveau module de correction disponible qui est basé sur le protocole de *pxGrid*. Ce module n'est pas pris en charge dans la version 6.0 mais est prévu pour être pris en charge dans les versions futures.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration du VPN de l'appliance de sécurité adaptable Cisco (ASA)
- Configuration de Client à mobilité sécurisé Cisco AnyConnect
- Configuration de base de Cisco FireSight
- Configuration de base de puissance de feu de Cisco
- Configuration de Cisco ISE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Version 9.3 ou ultérieures de Cisco ASA
- Versions de logiciel 1.3 de Cisco ISE et plus tard
- Versions 3.0 et ultérieures de Client à mobilité sécurisé Cisco AnyConnect
- Version 5.4 de centre de Gestion de Cisco FireSight
- Version 5.4 de puissance de feu de Cisco (virtual machine (VM))

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Utilisez les informations qui sont fournies dans cette section afin de configurer votre système.

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

L'exemple qui est décrit dans ce document utilise cette configuration réseau :

Voici l'écoulement pour cette configuration réseau :

1. L'utilisateur initie une session VPN à distance avec l'ASA (par l'intermédiaire de la version 4.0 sécurisée de mobilité de Cisco AnyConnect).

2. Les tentatives d'utilisateur d'accéder à *http://172.16.32.1*. (Le trafic se déplace par l'intermédiaire de la puissance de feu, qui est installée sur la VM et est gérée par FireSight.)

3. La puissance de feu est configurée de sorte qu'elle bloque (en ligne) ce trafic spécifique (stratégies d'accès), mais elle a également une stratégie de corrélation qui est déclenchée. En conséquence, il initie la correction ISE par l'intermédiaire de l'interface de programmation de REPOS (API) (la méthode de *QuarantineByIP*).

4. Une fois que l'ISE reçoit l'appel du REPOS API, il des consultations pour la session et envoie une modification de RAYON de l'autorisation (CoA) à l'ASA, qui termine cette session.

5. L'ASA déconnecte l'utilisateur VPN. Puisqu'AnyConnect est configuré avec l'accès VPN *illimité*, une nouvelle session est établie ; cependant, cette fois une règle différente d'autorisation ISE est appariée (pour les hôtes mis en quarantaine) et l'accès au réseau limité est fourni. À ce stade, il n'importe pas comment l'utilisateur se connecte et authentifie au réseau ; tant que l'ISE est utilisé pour l'authentification et l'autorisation, l'utilisateur a limité l'accès au réseau devant mettre en quarantaine.

Comme précédemment mentionné, ce scénario fonctionne pour n'importe quel type de session authentifiée (VPN, 802.1x/MAB/Webauth de câble, radio 802.1x/MAB/Webauth) tant que l'ISE est utilisé pour l'authentification et le périphérique d'accès au réseau prend en charge le CoA de RAYON (tous les périphériques modernes de Cisco).

> **Conseil** : Afin de déplacer l'utilisateur hors de la quarantaine, vous pouvez utiliser le GUI ISE. Les versions futures du module de correction pourraient également le prendre en charge.

Puissance de feu

> Remarque: Une appliance VM est utilisée pour l'exemple qui est décrit dans ce document. Seulement la configuration initiale est exécutée par l'intermédiaire du CLI. Toutes les stratégies sont configurées du centre de la défense de Cisco. Pour plus de détails, référez-

vous à la section Informations connexes de ce document.

La VM a trois interfaces, une pour la Gestion et deux pour l'inspection intégrée (interne et externe).

Tout les trafic des utilisateurs VPN se déplace par l'intermédiaire de la puissance de feu.

Centre de Gestion de FireSight (centre de la défense)

Stratégie de contrôle d'accès

Après que vous installiez les permis corrects et ajoutiez le périphérique de puissance de feu, naviguez vers les **stratégies > le contrôle d'accès** et créez la stratégie d'Access qui est utilisée afin de relâcher le trafic http à 172.16.32.1 :

Tout autre trafic est reçu.

Module de correction ISE

La version en cours du module ISE qui est partagé sur le portail de la communauté est la *correction bêtas 1.3.19 ISE 1.2* :

Naviguez vers des **stratégies > des actions > des corrections > des modules** et installez le fichier :

L'exemple correct devrait alors être créé. Naviguez vers des **stratégies > des actions > des corrections > des exemples** et fournissez l'adresse IP du noeud de gestion de stratégie (CASSEROLE), avec les qualifications administratives ISE qui sont nécessaires pour le REPOS API (un utilisateur distinct avec le rôle d'*admin ERS* est recommandé) :

L'adresse IP source (attaquant) devrait également être utilisée pour la correction :

Stratégie de corrélation

Vous devez maintenant configurer une règle spécifique de corrélation. Cette règle est déclenchée au début de la connexion qui apparie la règle précédemment configurée de contrôle d'accès (*DropTCP80*). Afin de configurer la règle, naviguez vers les **stratégies > la Gestion de corrélation > de règle** :

Cette règle est utilisée dans la stratégie de corrélation. Naviguez vers des **stratégies > la corrélation > la Gestion des stratégies** afin de créer une nouvelle stratégie, et puis ajoutez la règle configurée. Cliquez sur **Remediate** du côté droit et ajoutez deux actions : **correction pour le sourceIP** (configuré plus tôt) et le **Syslog** :

Assurez-vous que vous activez la stratégie de corrélation :

ASA

Une ASA qui agit en tant que passerelle VPN est configurée afin d'utiliser l'ISE pour l'authentification. Il est également nécessaire d'activer la comptabilité et le CoA de RAYON :

```
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

Périphérique d'Access de configure network (NAD)

Naviguez vers des **périphériques de gestion > de réseau** et ajoutez l'ASA qui agit en tant que client RADIUS.

Network Control d'adaptatif d'enable

Naviguez vers la **gestion > le système > les configurations > Network Control adaptatif** afin d'activer la quarantaine API et la fonctionnalité :

> Remarque: Dans les versions 1.3 et antérieures, cette caractéristique s'appelle le *service de protection de Endpoint*.

Quarantaine DACL

Afin de créer une liste de contrôle d'accès téléchargeable (DACL) qui est utilisée pour les hôtes mis en quarantaine, naviguez vers la **stratégie > les résultats > l'autorisation > ACL téléchargeable**.

Profil d'autorisation pour la quarantaine

Naviguez vers la **stratégie > les résultats > l'autorisation > le profil d'autorisation** et créez un profil d'autorisation avec le nouveau DACL :

Règles d'autorisation

Vous devez créer deux règles d'autorisation. La première règle (ASA-VPN) fournit l'accès complet pour toutes les sessions VPN qui sont terminées sur l'ASA. La règle *ASA-VPN_quarantine* est frappée pour la session VPN authentifiée à nouveau quand l'hôte est déjà dedans quarantaine (l'accès au réseau limité est fourni).

Afin de créer ces règles, naviguez vers la **stratégie > l'autorisation** :

Vérifiez

Utilisez les informations qui sont fournies dans cette section afin de vérifier que votre configuration fonctionne correctement.

AnyConnect initie la session VPN ASA

L'ASA crée la session sans n'importe quel DACL (plein accès au réseau) :

```
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>
```

Tentatives Access d'utilisateur

Une fois que les tentatives d'utilisateur d'accéder à http://172.16.32.1, la stratégie d'accès est frappées, le trafic qui correspond est en ligne bloqué, et le message de Syslog est envoyé de l'adresse IP de Gestion de puissance de feu :

```
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:
00000000000000000000000000000000000000000, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80
```

Hit de stratégie de corrélation de FireSight

La stratégie de corrélation de Gestion de FireSight (centre de la défense) est frappée, qui est signalée par le message de Syslog qui est envoyé du centre de la défense :

```
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)
```

Àce stade, le centre de la défense utilise l'appel du REPOS API (quarantaine) à l'ISE, qui est une session HTTPS et peut être déchiffré dans Wireshark (avec le module d'extension de Secure Sockets Layer (SSL) et la clé privée du certificat administratif de CASSEROLE) :

Dans la demande GET pour l'adresse IP de l'attaquant est passé (172.16.50.50), et cet hôte est mis en quarantaine par l'ISE.

Naviguez vers l'**analyse > la corrélation > l'état** afin de confirmer la correction réussie :

ISE exécute la quarantaine et envoie le CoA

Àce stade, l'ISE *prrt-management.log* annonce que le CoA devrait être envoyé :

```
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
```

Le délai d'exécution (prrt-server.log) envoie le terminatemessage CoA au NAD, qui termine la session (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
```

L'ise.psc envoie une notification semblable à ceci :

```
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
```

Quand vous naviguez vers des **exécutions > l'authentification**, elle devrait afficher l'*autorisation dynamique réussie*.

La session VPN est déconnectée

L'utilisateur final envoie une notification afin d'indiquer que la session est déconnectée (pour 802.1x/MAB/guest de câble/radio, ce processus est transparent) :

Détails de l'exposition de 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
```

Session VPN avec Access limité (quarantaine)

Puisque le *VPN illimité* est configuré, la nouvelle session est établie immédiatement. Cette fois, la règle ISE *ASA-VPN_quarantine* est frappée, qui fournit l'accès au réseau limité :

> Remarque: Le DACL est téléchargé dans une demande RADIUS distincte.

Une session avec l'accès limité peut être vérifiée sur l'ASA avec la commande CLI d'**anyconnect de détail de VPN-sessiondb d'exposition** :

```
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
```

Dépannez

Cette section fournit les informations que vous pouvez employer afin de dépanner votre configuration.

FireSight (centre de la défense)

Le script de correction ISE réside dans cet emplacement :

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

C'est un script simple *Perl* qui utilise le SourceFire standard (SF) se connectant le sous-système. Une fois que la correction est exécutée, vous pouvez confirmer les résultats par l'intermédiaire 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

Il est important que vous activiez le service de Network Control adaptatif sur l'ISE. Afin de visualiser le détaillé ouvre une session un processus d'exécution (*prrt-management.log* et *prrt-server.log*), vous doit activer le niveau de DEBUG pour le Délai d'exécution-AAA. Naviguez vers la **gestion > le système > en se connectant > configuration de log de debug** afin d'activer met au point.

Vous pouvez également naviguer vers des **exécutions > des états > le point final et des utilisateurs > audit adaptatif de Network Control** afin de visualiser les informations pour chaque tentative et le résultat d'une demande de quarantaine :

Bogues

Référez-vous à l'ID de bogue Cisco CSCuu41058 (incohérence de quarantaine de point final ISE 1.4 et panne VPN) pour des informations sur une bogue ISE qui est liée aux pannes de session VPN (802.1x/MAB fonctionne bien).

Informations connexes

- Configurez l'intégration WSA avec ISE pour des services avertis de TrustSec
- Intégration de pxGrid de version 1.3 ISE avec l'application de pxLog IPS
- Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 1.4 – Network Control d'adaptatif d'installation
- Guide de référence du Logiciel Cisco Identity Services Engine API, version 1.2 – Introduction aux services reposants externes API
- Guide de référence du Logiciel Cisco Identity Services Engine API, version 1.2 – Introduction au REPOS API de surveillance
- Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 1.3
- Support et documentation techniques - Cisco Systems