ISE と Firepower の統合での修復サービスの設定

目次

概要

このドキュメントでは、Cisco Identity Services Engine（ISE）をポリシー サーバとして使用して攻撃者検出と攻撃者自動修復を実行するため、Cisco FireSight アプライアンス上で修復モジュールを使用する方法について説明します。 このドキュメントで説明されている例は、ISE 経由で認証するリモート VPN ユーザの修復のために使用される方法を示すものですが、802.1x/MAB/WebAuth の有線または無線ユーザにも使用可能です。

注: このドキュメントで参照される修復モジュールは、正式にはシスコでサポートされていません。 これはコミュニティ ポータルで共有され、誰でも使用できます。 バージョン 5.4 以降では、*pxGrid* プロトコルに基づく新しい修復モジュールが利用可能です。 このモジュールは、バージョン 6.0 ではサポートされていませんが、将来のリリースでサポートされる予定です。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco 適応型セキュリティ アプライアンス（ASA）VPN の設定
- Cisco AnyConnect セキュア モビリティ クライアントの設定
- Cisco FireSight の基本設定
- Cisco FirePower の基本設定
- Cisco ISE の設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Microsoft Windows 7
- Cisco ASA バージョン 9.3 以降
- Cisco ISE ソフトウェア バージョン 1.3 以降
- Cisco AnyConnect Secure Mobility Client バージョン 3.0 以降
- Cisco FireSight Management Center バージョン 5.4
- Cisco FirePOWER バージョン 5.4（仮想マシン（VM））

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

システムを設定するには、このセクションで説明する情報を使用してください。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントで説明されている例では、次のネットワーク設定が使用されています。

ネットワーク設定のフローを次に示します：

1. ユーザは ASA とのリモート VPN セッションを開始します（Cisco AnyConnect Secure Mobility バージョン 4.0 による）。

2. ユーザは *http://172.16.32.1* へのアクセスを試みます。（トラフィックは VM にインストールされていて、FireSight によって管理される FirePOWER 経由で移動します。）

3. FirePower は、その特定のトラフィックを（インラインで）ブロックするように設定されていますが（アクセス ポリシー）、トリガーされる相関ポリシーもあります。 その結果、REST アプリケーション プログラミング インターフェイス（API）（*QuarantineByIP* メソッド）による ISE 修復が開始されます。

4. ISE が REST API コールを受信すると、セッションを検索し、ASA に RADIUS Change of Authorization（CoA）を送信します。それにより、セッションは終了します。

5. ASA は VPN ユーザを切断します。 AnyConnect は *Always-on* の VPN アクセスで設定されているため、新しいセッションが確立されます。 ただし、今回は別の（隔離されたホストのための）ISE 認可ルールに一致し、提供されるネットワーク アクセスは制限されたものになります。 この段階では、ユーザがどのようにネットワークに接続し、認証するとしても、 認証および認可に ISE が使用される限り、ユーザのネットワーク アクセスは隔離のため制限されたものになります。

前に説明したように、このシナリオは、ISE が認証に使用され、ネットワーク アクセス デバイスが RADIUS CoA（シスコのすべての最新のデバイス）をサポートする限り、認証済みセッション（VPN、有線、ワイヤレス 802.1x/MAB/Webauth 802.1x/MAB/Webauth）の任意のタイプで動作します。

ヒント： ユーザの隔離を解除するには、ISE GUI を使用できます。 修復モジュールの今後のバージョンでは、それがサポートされる可能性があります。

FirePOWER

注: このドキュメントで説明されている例では、VM アプライアンスが使用されています。 初期設定のみ、CLI によって実行されます。 ポリシーはすべて Cisco Defence Center から設定されます。 詳細については、このドキュメントの「関連情報」のセクションを参照してください。

この VM には、管理のために 1 つ、インライン検査のために 2 つ（内部/外部）、合計 3 つのイ

ンターフェイスがあります。

VPN ユーザからのすべてのトラフィックは、FirePOWER を経由します。

FireSight Management Center（Defence Center）

アクセス制御ポリシー

正しいライセンスをインストールして、FirePower デバイスを追加した後、[Policies] > [Access Control] に移動し、172.16.32.1 への HTTP トラフィックをドロップするために使用されるアクセス ポリシーを作成します：

他のトラフィックはすべて受け入れられます。

ISE 修復モジュール

コミュニティ ポータルで共有される ISE モジュールの現在のバージョンは、*ISE 1.2 Remediation Beta 1.3.19* です。

[Policies] > [Actions] > [Remediations] > [Modules] に移動し、ファイルをインストールします。

次に、正しいインスタンスを作成しなければなりません。 [Policies] > [Actions] > [Remediations] > [Instances] に移動し、ポリシー管理ノード（PAN）の IP アドレス、および REST API に必要な ISE 管理クレデンシャル（*ERS Admin* の役割を付与された別個のユーザを推奨）を指定します。

送信元 IP アドレス（攻撃者）も、修復に使用しなければなりません。

相関ポリシー

ここで、特定の相関ルールを設定する必要があります。 このルールは、以前に設定されたアクセス制御ルール（*DropTCP80*）に一致する接続の開始時にトリガーされます。 ルールを設定するには、[Policies] > [Correlation] > [Rule Management] に移動します。

このルールは、相関ポリシーで使用されます。 新しいポリシーを作成するため、[Policies] > [Correlation] > [Policy Management] に移動し、設定されたルールを追加します。 右側の [Remediate] をクリックし、次の 2 つのアクションを追加します。 **remediation for sourceIP**（以前に設定）および **syslog**：

相関ポリシーが有効であることを確認します。

ASA

認証に ISE を使用するため、VPN ゲートウェイとして動作する ASA を設定します。 また、アカウンティングおよび RADIUS CoA を有効にすることも必要です。

```
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

ネットワーク アクセス デバイス（NAD）の設定

[Administration] > [Network Devices] に移動し、RADIUS クライアントとして動作する ASA を追加します。

適応型ネットワーク制御を有効にする

隔離 API および機能を有効にするため、[Administration] > [System] > [Settings] > [Adaptive Network Control] に移動します。

> **注:** バージョン 1.3 以前において、この機能は*エンドポイント保護サービス*と呼ばれています。

隔離 DACL

隔離されたホストで使用されるダウンロード可能アクセス コントロール リスト（DACL）を作成するには、[Policy] > [Results] > [Authorization] > [Downloadable ACL] に移動します。

隔離用認可プロファイル

[Policy] > [Results] > [Authorization] > [Authorization Profile] に移動し、新しい DACL により認可プロファイルを作成します。

認可規則

2 つの認可ルールを作成する必要があります。 最初のルール (ASA-VPN) は ASA で終端する VPN セッションすべてへのフル アクセスを提供します。 ホストがすでに隔離されている場合、*ASA-VPN_quarantine* ルールは再認証された VPN セッションにヒットします (ネットワーク アクセスは制限付きで提供されます) 。

これらのルールを作成するため、[Policy] > [Authorization] に移動します。

確認

設定が適切に機能することを確認するために、この項に記載する情報を活用してください。

AnyConnect が ASA VPN セッションを開始する

ASA は DACL なしでセッションを作成します (フル ネットワーク アクセス) 。

```
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>
```

ユーザによるアクセスの試行

ユーザが http://172.16.32.1 にアクセスしようとすると、アクセス ポリシーがヒットし、対応するトラフィックはインラインでブロックされ、syslog メッセージが FirePower 管理 IP アドレスから送信されます。

```
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 相関ポリシーのヒット

FireSight Management (Defense Center) 相関ポリシーがヒットします。これは、Defense Center から送信される syslog メッセージで報告されます。

```
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)
```

この段階で Defense Center は、ISE に対する REST API (隔離) 呼び出しを使用します。これは HTTPS セッションであり、(Secure Sockets Layer (SSL) プラグインおよび PAN 管理証明書の秘密鍵を使用して) Wireshark で復号化できます。

GET 要求では、攻撃者の IP アドレス (172.16.50.50) が渡され、そのホストが ISE により隔離されます。

修復か正常に実行されたことを確認するため、[Analysis] > [Correlation] > [Status] に移動します。

ISE が隔離を実行し、CoA を送信する

この段階で、ISE の *prrt-management.log* に、CoA を送信する必要があることが通知されます。

```
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
```

ランタイム (prrt-server.log) により、セッション (ASA) を終了する NAD に、CoA の terminatemessage が送信されます。

```
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 が、次のような通知を送信します。

```
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
```

[Operations] > [Authentication] に移動すると、[Dynamic Authorization succeeded] が表示されるはずです。

VPN セッションが切断される

エンドユーザはセッションが切断されていることを示すために通知を送信します（802.1x/MAB/ゲスト有線/ワイヤレスの場合、このプロセスは透過的）。

Cisco AnyConnect ログの show コマンドの詳細：

```
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
```

アクセス制限（隔離）のある VPN セッション

always-on VPN が設定されているため、新しいセッションが直ちに作成されます。 今回は、制限付きネットワーク アクセスを提供する ISE ASA-VPN_quarantine ルールがヒットします。

> **注:** 別個の RADIUS 要求で DACL がダウンロードされます。

アクセスが限られているセッションについては、**show vpn-sessiondb detail anyconnect** の CLI コマンドを使用して、ASA で確認できます。

```
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
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

FireSight (Defence Center)

ISE 修復スクリプトは次の場所にあります。

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

これは標準 SourceFire (SF) ロギング サブシステムを使用する簡単な *perl スクリプト*です。 修復が実行されると、*/var/log/messages* で結果を確認できます。

```
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

ISE 上の適応型ネットワーク制御サービスを有効にすることが重要です。 ランタイム プロセスで詳細なログ (*prrt-management.log* と *prrt-server.log*) を表示するには、Runtime-AAA の DEBUG レベルを有効にする必要があります。 デバッグを有効にするため、[Administration] > [System] > [Logging] > [Debug Log Configuration] に移動します。

また、[Operations] > [Reports] > [Endpoint and Users] > [Adaptive Network Control Audit] に移動すると、隔離要求のすべての試行と結果の情報を表示することができます。

バグ

VPN セッション障害 (802.1x/MAB は適切に動作) に関連する ISE のバグについての詳細は、Cisco Bug ID CSCuu41058 (ISE 1.4 エンドポイント隔離の非一貫性と VPN 障害) を参照してください。

関連情報

- TrustSec Aware サービスのための ISE との WSA 統合の設定
- IPS pxLog アプリケーションとの ISE バージョン 1.3pxGrid 統合
- Cisco Identity Services Engine 管理者ガイド、リリース 1.4 – 適応型ネットワーク制御サービスの設定
- 『Cisco Identity Services Engine API リファレンス ガイド、リリース 1.2』の「適応型ネットワーク制御サービスの設定」
- 『Cisco Identity Services Engine API Reference Guide, Release 1.2』の「Introduction to the Monitoring REST APIs」
- Cisco Identity Services Engine 管理者ガイド リリース 1.3
- テクニカル サポートとドキュメント - Cisco Systems