iPEP ISE および ASA を使用した VPN インライン ポスチャ

目次

はじめに

このドキュメントでは、適応型セキュリティ アプライアンス（ASA）および Identity Services Engine（ISE）でインライン ポスチャを設定する方法について説明します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、ASA のバージョン 8.2(4) および ISE のバージョン 1.1.0.665 に基づいています。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ISE は、多くの AAA サービス（ポスチャ、プロファイル、認証など）を提供します。 ネットワーク デバイス（NAD）によっては、ポスチャまたはプロファイル結果に基づいてエンド デバイスの認可プロファイルをダイナミックに変更できる RADIUS Change Of Authorization（CoA）をサポートします。 また、ASA などの NAD は、この機能をサポートしません。 つまり、Inline Posture Enforcement モード（iPEP）で実行する ISE は、エンド デバイスのネットワーク アクセス ポリシーをダイナミックに変更する必要があります。

基本的な概念では、すべてのユーザ トラフィックは、RADIUS プロキシとしても機能するノードを使用して、iPEP を通過します。

基本フロー

1. VPN ユーザがログインします。
2. ASA が要求を iPEP ノード（ISE）に送信します。
3. iPEP は、要求をリライトし（Cisco AV-PAIR 属性を追加し iPEP 認証であることを示します）、その要求を ISE Policy Node（PDP）に送信します。
4. PDP は、NAD に転送される iPEP に応答します。
5. ユーザが認証されると、NAD は、アカウンティング開始要求を送信する必要があります（CSCtz84826 を参照）。 これにより、iPEP でセッションが開始します。 この段階では、ユーザは、ポスチャにリダイレクトされます。 また、ISE には RADIUS アカウンティングの属性 framed-ip-address があると想定されるので、WEBVPN ポータルから確立されたトンネルで interim-accounting-update をイネーブルにする必要があります。 ただし、ポータルに接続する場合、クライアントの VPN IP アドレスは、トンネルが確立されていないため、認識されません。 このため、トンネルが確立される場合など、ASA により、暫定アップデートが送信されます。
6. ユーザがポスチャ アセスメントを通過すると、その結果に基づいて、PDP により、iPEP の CoA を使用してセッションが更新されます。

このプロセスを次のスクリーンショットに示します。

トポロジの例

ASA の設定

ASA 設定は、IPSEC リモート VPN です。

```
!
interface Ethernet0/0
nameif ISE
security-level 50
ip address 192.168.102.253 255.255.255.0
!
interface Ethernet0/1
nameif outside
security-level 0
ip address 10.48.39.236 255.255.255.0
!
```

```
access-list split extended permit ip 192.168.0.0 255.255.0.0 any
!
aaa-server ISE protocol radius
interim-accounting-update
!--- Mandatory if tunnel established from WEBVPN Portal aaa-server ISE (ISE) host
192.168.102.254 !--- this is the iPEP IP key cisco crypto ipsec transform-set TS1 esp-aes esp-
sha-hmac crypto ipsec security-association lifetime seconds 28800 crypto ipsec security-
association lifetime kilobytes 4608000 crypto dynamic-map DMAP1 10 set transform-set TS1 crypto
dynamic-map DMAP1 10 set reverse-route crypto map CM1 10 ipsec-isakmp dynamic DMAP1 crypto map
CM1 interface outside crypto isakmp enable outside crypto isakmp policy 1 authentication pre-
share encryption aes hash sha group 2 lifetime 86400 ! ip local pool VPN 192.168.5.1-
192.168.5.100 ! group-policy DfltGrpPolicy attributes dns-server value 192.168.101.3 !--- The
VPN User needs to be able to resolve the CN from the !--- ISE HTTPS Certificate (which is sent
in the radius response) vpn-tunnel-protocol IPSec svc webvpn split-tunnel-policy tunnelspecified
split-tunnel-network-list value split address-pools value VPN ! tunnel-group cisco general-
attributes address-pool VPN authentication-server-group ISE accounting-server-group ISE !---
Does not work without this (see introduction) ! tunnel-group cisco ipsec-attributes pre-shared-
key cisco ! route outside 0.0.0.0 0.0.0.0 10.48.39.5 1 route ISE 192.168.0.0 255.255.0.0
192.168.102.254 1 !--- You need to make sure the traffic to the local subnets !--- are going
through the inline ISE !
```

ISE 設定

iPEP の設定

最初に、ISE を iPEP ノードとして追加します。 プロセスの追加情報については、次を参照してください。

http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_ipep_deploy.html#wp1110248.

これは、基本的には、さまざまなタブで構成する必要があります（このセクションのスクリーンショットを参照）。

- 信頼できない IP およびグローバル IP 設定を構成します（この場合、信頼できない IP は 192.168.102.254 です）。
- 導入はルーテッド モードです。
- iPEP ボックスを通過するように ASA のスタティック フィルタを許可します（許可しない場合、iPEP ボックスを介した ISE 間の接続が切断されます）。
- ポリシー ISE を RADIUS サーバとして、ASA を RADIUS クライアントとして設定します。
- ASA をポイントするルートを VPN サブネットに追加します。
- Monitoring ISE を Logging Host として設定します（デフォルトではポート 20514 です。 この場合、ポリシー ISE もモニタします）。

重要な証明書設定要件：

iPEP ノードを登録しようとする前に、次の証明書のキーの拡張用途の要件を満たしている必要があります。 証明書が iPEP および Admin ノードで正しく設定されていない場合でも、登録プロセスは完了します。 ただし、iPEP ノードへの管理アクセスを失います。 次の詳細は、『ISE 1.1.x iPEP Deployment Guide』からの推定です。

管理およびインライン ポスチャ ノードのローカル証明書の属性の組み合わせによっては、相互認証が動作しなくなることがあります。

その属性は次のとおりです。

- キーの拡張用途（EKU）：サーバ認証

- キーの拡張用途（EKU）：クライアント認証
- Netscape 証明書タイプ：SSL サーバ認証
- Netscape 証明書タイプ：SSL クライアント認証

管理証明書には、次のいずれかの組み合わせが必要です。

- EKU 属性は、両方ともディセーブルにするか（インライン ポスチャ証明書で両方の EKU 属性がディセーブルの場合）、両方ともイネーブルにします（インライン ポスチャ証明書でサーバ属性がイネーブルの場合）。
- Netscape 証明書タイプ属性は、両方ともディセーブルにするか、両方ともイネーブルにします。

インライン ポスチャ証明書には、次のいずれかの組み合わせが必要です。

- EKU 属性は、両方とも無効にするか、両方ともイネーブルにするか、サーバ属性のみをイネーブルにします。
- Netscape 証明書タイプ属性は、両方ともディセーブルにするか、両方ともイネーブルにするか、サーバ属性のみをイネーブルにします。
- 自己署名ローカル証明書が管理ノードとインライン ポスチャ ノードで使用されている場合は、管理ノードの自己署名証明書をインライン ポスチャ ノードの信頼リストにインストールする必要があります。 加えて、プライマリとセカンダリの両方の管理ノードが展開内にある場合は、両方の管理ノードの自己署名証明書をインライン ポスチャ ノードの信頼リストにインストールする必要があります。
- CA 署名付きのローカル証明書が管理ノードとインライン ポスチャ ノードで使用されている場合、相互認証は正しく動作します。 この場合は、登録の前に署名 CA の証明書が管理ノードにインストールされ、この証明書がインライン ポスチャ ノードに複製されます。
- 管理およびインライン ポスチャ ノード間の通信をセキュリティ保護するために CA 発行のキーが使用される場合は、インライン ポスチャ ノードを登録する前に、管理ノードからの公開キー（CA 証明書）をインライン ポスチャ ノードの CA 証明書リストに追加する必要があります。

基本設定：

導入モードの設定：

フィルタの設定：

RADIUS の設定：

スタティック ルート：

ロギング：

認証とポスチャの設定

ポスチャの状態は次の 3 種類があります。

- 不明： ポスチャは作成されていません。
- 準拠： ポスチャが作成され、システムに準拠します。
- 非準拠： ポスチャが作成されますが、システム チェックが少なくとも一度失敗しています。

認証プロファイルを作成する必要があります（これは、インライン認証プロファイルで、 Cisco

AV ペアの ipep-authz=true 属性を追加します）。これは、別の状況で使用されます。

通常、不明プロファイルは、ユーザのトラフィックを ISE に転送するリダイレクト URL（ポスチャ ディスカバリ）を返し、NAC エージェントのインストールを要求します。 NAC エージェントがすでにインストールされている場合、その HTTP ディスカバリ要求を ISE に転送できます。

このプロファイルでは、少なくとも ISE および DNS への HTTP トラフィックを許可する ACL が使用されます。

準拠および非準拠プロファイルは、通常、ダウンロード可能な ACL を返し、ユーザ プロファイルに基づいてネットワーク アクセスを付与します。 非準拠プロファイルでは、ユーザは、Web サーバにアクセスし、たとえば、アンチウイルスをダウンロードしたり、制限付きネットワーク アクセスを付与したりできます。

この例では、不明および準拠プロファイルが作成され、要件としての notepad.exe の存在がチェックされます。

ポスチャ プロファイルの設定

最初に、ダウンロード可能 ACL（dACL）およびプロファイルを作成します。

注: プロファイル名とマッチングする dACL 名を使用することは必須ではありません。

- 準拠ACL： ipep-unknown許可プロファイル： ipep-unknown
- 非準拠ACL： ipep-non-compliant許可プロファイル： ipep-non-compliant

不明 dACL：

不明プロファイル：

準拠 dACL：

準拠プロファイル：

認可の設定

プロファイルが作成されたら、iPEP から送信される RADIUS 要求をマッチングして、正しいプロファイルを適用する必要があります。 iPEP ISE は、認証ルールで使用される特別なデバイス タイプで定義されます。

NAD：

許可：

注: エージェントがマシンにインストールされていない場合、クライアント プロビジョニング ルールを定義できます。

結果

エージェントをインストールするように求められます（この例では、クライアント プロビジョニングがすでに設定されています）。

この段階での出力の一部：

```
ciscoasa# show vpn-sessiondb remote

Session Type: IPsec
Username     : cisco                  Index        : 26
Assigned IP  : 192.168.5.2            Public IP    : 10.48.39.134
Protocol     : IKE IPsec
License      : IPsec
Encryption   : AES128                 Hashing      : SHA1
Bytes Tx     : 143862                 Bytes Rx     : 30628
Group Policy : DfltGrpPolicy          Tunnel Group : cisco
Login Time   : 13:43:55 UTC Mon May 14 2012
Duration     : 0h:09m:37s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

iPEP：

```
w-ise-ipep-1/admin# show pep table session

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 2 0
w-ise-ipep-1/admin# show pep table accesslist normal
#ACSACL#-IP-ipep-unknown-4fb10ac2:
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
```

エージェントがダウンロードおよびインストールされた場合：

エージェントは自動的に ISE を検出して、ポスチャ割り当てを実行します（ポスチャ ルールがすでに設定されていることを前提とします（これは別の問題とします））。 この例では、ポスチャは成功し、次のように表示されます。

注: 上記のスクリーンショットには 2 つの認証があります。 ただし、iPEP ボックスは ACL をキャッシュするので、ダウンロードされない場合もあります。

iPEP：

```
w-ise-ipep-1/admin# show pep table session

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 3 0
w-ise-ipep-1/admin# show pep table accesslist normal
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406:
permit ip any any

#ACSACL#-IP-ipep-unknown-4fb10ac2:
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
w-ise-ipep-1/admin#
```

関連情報

- テクニカル サポートとドキュメント – Cisco Systems