IPS pxLog アプリケーションとの ISE バージョン 1.3 pxGrid 統合

目次

はじめに
前提条件
要件
使用するコンポーネント
ネットワーク ダイアグラムとトラフィック フロー
pxLog
アーキテクチャ
インストール
Snort
ISE
設定
ペルソナと証明書
エンドポイント保護サービス（EPS）
認可規則
トラブルシューティング
テスト
ステップ 1 pxGrid の登録
ステップ 2 pxLog 規則の設定
ステップ 3 最初の Dot1x セッション
ステップ 4 Microsoft Windows PC からのアラームをトリガーするパケットの送信
ステップ 5 pxLog
ステップ 6 ISE 隔離
ステップ 7 pxLog 隔離解除
ステップ 8 ISE 隔離解除
pxLog 機能
pxGrid プロトコルの要件
[グループ（Groups）]
証明書と Java キーストア
[hostname]
開発者向けの注
Syslog
Snort
Cisco 適応型セキュリティ アプライアンス（ASA）インスペクション
Cisco Sourcefire 次世代侵入防御システム（NGIPS）
Juniper Netscreen
Juniper JunOS

[Linux iptable](#)
[FreeBSD IPFirewall（IPFW）](#)
[VPN 対応状況および CoA 処理](#)
[pxGrid パートナーとソリューション](#)
[ISE API： REST、EREST、pxGrid](#)
[ダウンロード](#)
[関連情報](#)

概要

Identity Services Engine（ISE）バージョン 1.3 では、pxGrid と呼ばれる新しい API がサポートされています。 認証、暗号化、および特権（グループ）をサポートするこの新しく柔軟なプロトコルにより、他のセキュリティ ソリューションとの統合が容易になります。 このドキュメントでは、コンセプト実証として作成された pxLog アプリケーションの使用方法を説明します。 pxLog は侵入防御システム（IPS）から syslog メッセージを受信し、攻撃者を隔離するために pxGrid メッセージを ISE に送信することができます。 その結果、ISE はネットワーク アクセスを制限するエンドポイントの許可ステータスを変更するために、RADIUS 認可変更（CoA）を使用します。 これらの処理はすべて、エンドユーザに対しては透過的に行われます。

このドキュメントの例では Snort が IPS として使用されていますが、その他のソリューションを使用することもできます。 実際にはこれは IPS である必要はありません。 必要な処理は、攻撃者の IP アドレスが含まれている syslog メッセージを pxLog に送信することだけです。 このため、多数のソリューションを統合できる可能性があります。

このドキュメントでは、pxGrid ソリューションのトラブルシューティングおよびテストの方法と、よく発生する問題と制約事項について説明します。

免責事項： シスコは pxLog アプリケーションをサポートしていません。 この記事は、コンセプト実証として作成されました。 主な目的は、ISE における pxGrid 実装のベータテストで使用することです。

前提条件

要件

Cisco ISE 構成の経験と、次のトピックに関する基本的な知識があることが推奨されます。

- ISE の導入および認可の設定
- Cisco Catalyst スイッチの CLI 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 Catalyst 3750X シリーズ スイッチ ソフトウェア バージョン 15.0 以降
- Cisco ISE ソフトウェア バージョン 1.3 以降

- Cisco AnyConnect Mobile Security（Network Access Manager（NAM）を含む）バージョン 3.1 以降
- Snort バージョン 2.9.6 および Data Acquisition（DAQ）
- MySQL バージョン 5 が稼働する Tomcat 7 にインストールされている pxLog アプリケーション

ネットワーク ダイアグラムとトラフィック フロー

次のネットワーク ダイアグラムにトラフィック フローを示します。

1. Microsoft Windows 7 ユーザがスイッチに接続し、802.1x 認証を実行します。

2. スイッチは、認証、許可、アカウンティング（AAA）サーバとして ISE を使用します。 **Dot1x Full Access** 認可規則が一致し、フル ネットワーク アクセスが付与されます（DACL: PERMIT_ALL）。

3. ユーザは、信頼ネットワークへの接続を試行しますが、Snort 規則に違反します。

4. その結果、Snort から pxLog アプリケーションへ（syslog により）アラートが送信されます。

5. pxLog アプリケーションは、ローカル データベースに対して検証を実行します。 これは Snort から送信される syslog メッセージをキャッチし、攻撃者の IP アドレスを抽出するように設定されています。 次に、攻撃者の IP アドレスを隔離するために、pxGrid を使用して ISE に要求を送信します（ISE は pxGrid コントローラです）。

6. ISE は認可ポリシーを再評価します。 エンドポイントが隔離されるため、**Session: EPSStatus EQUALS Quarantine** 条件に一致し、別の認可プロファイルに一致します（**Dot1x Quarantine**）。 セッションを終了するために、ISE は CoA 終了をスイッチに送信します。 これにより再認証がトリガーされ、新しいダウンロード可能 ACL（DACL）（PERMIT_ICMP）が適用されます。これにより、エンドユーザに対して制限付きネットワーク アクセスが提供されます。

7. この段階で、管理者はエンドポイントの隔離解除を決定することができます。 これは pxLog の GUI で行えます。 ISE 宛ての pxGrid メッセージが再度送信されます。

8. ISE はステップ 6 に似た操作を実行します。 この時点では、エンドポイントは隔離されず、フル アクセスが提供されます。

pxLog

アーキテクチャ

解決策として、Linux マシンに一連のアプリケーションをインストールします。

1. pxLog アプリケーションは Java で作成されており、Tomcat サーバに導入されます。 この

アプリケーションは次のコンポーネントで構成されます。

Web 要求を処理するサーブレット：Web ブラウザから管理パネルへアクセスできるようにするために使用されます。

Enforcer モジュール：サーブレットと共に開始されるスレッド。 Enforcer はファイルから syslog メッセージを読み取り（最適化）、設定されている規則に基づいてこれらのメッセージを処理し、アクション（pxGrid を介した隔離など）を実行します。

2. pxLog（規則とログ）の設定が含まれている MySQL データベース。

3. 外部システムから syslog メッセージを受信し、ファイルに書き込む syslog サーバ。

インストール

pxLog アプリケーションでは次のライブラリが使用されます。

- jQuery（AJAX サポート用）
- JavaServer Pages Standard Tag Library（JSTL）（Model View Controller（MVC）モデル、データはロジックから切り離されます。 JavaServer Page（JSP）コードはレンダリングだけに使用され、Java クラスに HTML コードはありません）
- Log4j（ロギング サブシステム）
- MySQL コネクタ
- テーブルのレンダリング/ソート用の displaytag
- シスコの pxGrid API（現在のバージョンは alpha 147 です）

これらすべてのライブラリはプロジェクトの lib ディレクトリにすでに含まれているため、その他の Java ARchive（JAR）ファイルをダウンロードする必要はありません。

アプリケーションをインストールするには、次の手順を実行します。

1. Tomcat Webapp ディレクトリにディレクトリ全体を解凍します。

2. **WEB-INF/web ファイル**を編集します。 唯一の必要な変更は serveripvariable です。これは ISE を指している必要があります。 また、（デフォルトの代わりに）Java 証明書キーストア（1 つの信頼キーストアと 1 つの ID キーストア）が生成されることがあります。 これは、クライアント証明書とサーバ証明書の両方を使用する Secure Sockets Layer（SSL）セッションを使用する pxGrid API によって使用されます 通信の両側に証明書が提供され、両側が相互を信頼する必要があります。 詳細については、「pxGrid プロトコルの要件」の項を参照してください。

3. ISE ホスト名が pxLog で正しく解決されることを確認します（ドメイン ネーム サーバ（DNS）または **/etc/hosts エントリ**のレコードを参照）。 詳細については、「pxGrid プロトコルの要件」の項を参照してください。

4. **mysql/init.sql スクリプト**を使用して MySQL データベースを設定します。 クレデンシャルは変更できますが、**INF/web.xml ファイル**に変更を反映する必要があります。

Snort

この記事では、特定の IPS について詳しく説明するのではなく、簡単な説明だけを記載しています。

Snort は DAQ サポートによりインラインとして設定されます。 トラフィックは iptables によりリダイレクトされます。

```
iptables -I FORWARD -j ACCEPT
iptables -I FORWARD -j NFQUEUE --queue-num 1
```

インスペクション後に、デフォルトの iptable 規則に従ってトラフィックが注入および転送されます。

いくつかのカスタム Snort 規則が設定されています（**/etc/snort/rules/test.rules** ファイルはグローバル コンフィギュレーションに含まれています）。

```
alert icmp any any -> any any (itype:8; dsize:666<>686; sid:100122)
alert icmp any any -> any any (itype:8; ttl: 6; sid:100124)
```

Snort は、パケットの存続可能時間（TTL）が 6 と同等であるか、またはペイロードのサイズが 666 ~ 686 である場合に、syslog メッセージを送信します。 トラフィックが Snort によってブロックされることはありません。

また、アラートが頻繁にトリガーされないようにするために、しきい値を設定する必要もあります（**/etc/snort/threshold.conf**）。

```
event_filter gen_id 1, sig_id 100122, type limit, track by_src, count 1, seconds 60
event_filter gen_id 1, sig_id 100124, type limit, track by_src, count 1, seconds 60
```

次に syslog サーバが pxLog マシンを指し示します（**/etc/snort/snort.conf**）。

```
output alert_syslog: host=10.222.0.61:514, LOG_AUTH LOG_ALER
```

一部の Snort バージョンでは、syslog 設定に関連するバグがあります。localhost を指し示すデフォルト設定を使用できますが、特定のメッセージを pxLog ホストに転送するように syslog-ng を設定できます。

ISE

設定

ペルソナと証明書

1. [Administration] > [Deployment] で、ISE ではデフォルトで無効にされている pxGrid ロールを有効にします。

2. [Administration] > [Certificates] > [System Certificates] で、pxGrid に証明書が使用されているかどうかを確認します。

エンドポイント保護サービス (EPS)

[Administration] > [Settings] から EPS を有効にする必要があります (デフォルトでは無効) 。

これにより、隔離/隔離解除機能を使用できるようになります。

認可規則

最初の規則は、エンドポイントが隔離される場合にのみ発生します。 RADIUS CoA により制限付きアクセスが動的に適用されます。 正しい共有秘密を使用してスイッチをネットワーク デバイスに追加する必要もあります。

トラブルシューティング

pxGrid のステータスは CLI で確認できます。

```
lise/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          6717
Database Server                        running          51 PROCESSES
Application Server                     running          9486
Profiler Database                      running          7804
AD Connector                           running          10058
M&T Session Database                   running          7718
M&T Log Collector                      running          9752
M&T Log Processor                      running          9712
Certificate Authority Service          running          9663
pxGrid Infrastructure Service          running          14979
pxGrid Publisher Subscriber Service    running          15281
pxGrid Connection Manager              running          15248
pxGrid Controller                      running          15089
Identity Mapping Service               running          9962
```

また、pxGrid の別のデバッグもあります ([Administration] > [Logging] > [Debug Log Configuration] > [pxGrid]) 。 デバッグ ファイルは pxGrid ディレクトリに保存されます。 最も重要なデータは **pxgrid/pxgrid-jabberd.log** と pxgrid/pxgrid-controller.log **にあります。**

テスト

ステップ 1 pxGrid の登録

pxLog アプリケーションは、Tomcat の起動時に自動的に導入されます。

1. pxGrid を使用するには、ISE に 2 つのユーザ（セッション アクセス権限を持つユーザと隔離のためのユーザ）を登録します。 これは、[Pxgrid Operations] > [Register users] から実行できます。

   登録は自動的に開始します。

2. この段階で、ISE で登録ユーザを承認する必要があります（デフォルトでは自動承認は無効になっています）。

   承認後、pxLog は（AJAX コールを使用して）管理者に自動的に通知します。

   ISE は、この 2 つのユーザのステータスとして [Online] または [Offline] を表示します（[Pending] は使用されなくなりました）。

ステップ 2 pxLog 規則の設定

pxLog は syslog メッセージを処理し、それに基づいてアクションを実行する必要があります。 新しい規則を追加するには、[Manage Rules] を選択します。

Enforcer モジュールが syslog メッセージで次の正規表現（RegExp）を検索します。 "snort[" 検出されたら、すべての IP アドレスが検索され、最後のアドレスの 1 つ前の IP アドレスが選択されます。 これはほとんどのセキュリティ ソリューションに一致します。 詳細については「Syslog」の項を参照してください。 その IP アドレス（攻撃者）は pxGrid により隔離されます。 また、さらに細かな規則を使用できます（例：シグニチャ番号を含む規則など）。

ステップ 3 最初の Dot1x セッション

Microsoft Windows 7 端末は、有線 dot1x セッションを開始します。 Cisco Anyconnect NAM がサプリカントとして使用されています。 Extensible Authentication Protocol-Protected EAP（EAP-PEAP）方式が設定されます。

ISE **Dot1x Full Access** 認可プロファイルが選択されます。 スイッチは、フル アクセス権限を付与するためにアクセス リストをダウンロードします。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
```

```
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ALL-53fc9dbe
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E6BAB267CF
     Acct Session ID:  0x00003A70
              Handle:  0xA100080E

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
    permit ip any any
```

ステップ 4 Microsoft Windows PC からのアラームをトリガーするパケットの送信

Microsoft Windows から TTL = 7 でパケットを送信した場合の動作を次に示します。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ALL-53fc9dbe
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E6BAB267CF
     Acct Session ID:  0x00003A70
              Handle:  0xA100080E

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
    permit ip any any
```

この値はフォワーディング チェーン内の Snort で減少し、アラームが発生します。 その結果、pxLog 宛ての syslog メッセージが送信されます。

```
Sep  6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 ->
10.222.0.61
```

ステップ 5 pxLog

pxLog は syslog メッセージを受信し、このメッセージを処理し、その IP アドレスを隔離することを要求します。 これは、ログを調べると確認できます。

ステップ 6 ISE 隔離

ISE から、IP アドレスが隔離されたことが報告されます。

その結果、ISE はその特定のエンドポイントのスイッチで認可ステータスを更新するために、認可ポリシーをレビューし、隔離を選択し、RADIUS CoA を送信します。

これは、サプリカントに対し新しいセッションの開始と制限付きアクセス（Permit_ICMP）の取得を強制的に実行させる CoA 終了メッセージです。

スイッチでその結果を確認できます（エンドポイントの制限付きアクセス）。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

ステップ 7 pxLog 隔離解除

この段階で、管理者はエンドポイントの隔離解除を決定します。

同じ操作を ISE から直接実行できます。

ステップ 8 ISE 隔離解除

ISE は規則を再度レビューし、スイッチの認可ステータスを更新します（フル ネットワーク アクセスが付与されます）。

レポートで次の内容が確認されます。

pxLog 機能

pxLog アプリケーションは、pxGrid API の機能を実証する目的で作成されました。 次の操作を実行できます。

- ISE でのセッションと EPS ユーザの登録
- ISE でアクティブなすべてのセッションに関する情報のダウンロード
- ISE での特定のアクティブ セッションに関する情報のダウンロード（IP アドレスに基づく）
- ISE での特定のアクティブ ユーザに関する情報のダウンロード（ユーザ名に基づく）
- すべてのプロファイルに関する情報の表示（プロファイラ）
- ISE で定義されている TrustSec Security Group Tag（SGT）に関する情報の表示
- バージョンの確認（pxGrid の機能）
- IP アドレスまたは MAC アドレスに基づく隔離
- IP アドレスまたは MAC アドレスに基づく隔離解除

今後その他の機能も予定されています。

次に pxLog のスクリーンショットの例を示します。

pxGrid プロトコルの要件

[グループ（Groups）]

クライアント（ユーザ）は一度に 1 つのグループのメンバーになることができます。 最もよく使用される 2 つのグループは次のとおりです。

- Session：セッション/プロファイル/SGT に関する情報を参照/ダウンロードするために使用されます。
- EPS： 隔離を実行するために使用されます。

証明書と Java キーストア

前述したように、クライアント アプリケーション pxLog と pxGrid コントローラ（ISE）の両方で、通信のために証明書が設定されている必要があります。 pxLog アプリケーションは証明書を Java キーストア ファイルに保持します。

- **store/client.jks**：クライアント証明書と認証局（CA）証明書が含まれています。
- **store/root.jks**：ISE チェーン： モニタリングおよびトラブルシューティング ノード（MnT）ID と CA 証明書が含まれています。

ファイルはパスワード（デフォルト： cisco123）で保護されています。 ファイルの場所とパスワードは **WEB-INF/web.xml** で変更できます。

新規 Java キーストアを生成する手順を次に示します。

1. ルート（信頼）キーストアを生成するには、CA 証明書をインポートします（cert-ca.der は DER フォーマットである必要があります）。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

2. 新しいキーストアを作成する場合はパスワードを選択します。このパスワードは後でキーストアにアクセスするときに使用されます。

3. ルート キーストアに MnT ID 証明書をインポートします（cert-mnt.der は ISE から取得される ID 証明書であり、DER 形式である必要があります）。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F
```

```
Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

4. クライアント キーストアを作成するために、CA 証明書をインポートします。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

5. クライアント キーストアで秘密キーを作成します。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
```

```
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

6. クライアント キー ストアで証明書署名要求 (CSR) を生成します。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

7. cert-client.csr に署名し、署名したクライアント証明書をインポートします。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
```

```
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

8. 両方のキーストアに正しい証明書が含まれていることを確認します。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

注意： ISE 1.3 ノードのアップグレード時には、ID 証明書を維持することができますが、CA の署名は削除されます。 その結果、アップグレード後の ISE は新しい証明書を使用しますが、SSL/ServerHello メッセージに CA 証明書を付加することはありません。 これが原因で、（RFC に基づき）完全なチェーンが確認されることを前提としているクライアントでエラーとなります。

[hostname]

さまざまな機能（セッションのダウンロードなど）のための pxGrid API は追加検証を実行します。 クライアントは ISE にコンタクトし、ISE ホスト名を受信します。このホスト名は、CLI で hostname コマンドを使用して定義されるものです。 次に、クライアントはそのホスト名の DNS 解決と、IP アドレスからのデータへのアクセスと取得を試行します。 ISE ホスト名の DNS 解決が失敗した場合、クライアントはデータの取得を試行しません。

注意： この解決ではホスト名だけが使用されることに注意してください。このシナリオでは、これは完全修飾ドメイン名（FQDN）（このシナリオでは **lise.example.com**）ではなく **lise** です。

開発者向けの注

シスコは pxGrid API を公開およびサポートしています。 次のような名前のパッケージが 1 つあります。

pxgrid-sdk-1.0.0-167

このパッケージの内容は次のとおりです。

- クラスを含む pxGrid JAR ファイル。Java ファイルに容易にデコードしてコードを確認できます。
- 証明書が格納されているサンプル Java キーストア
- pxGrid を使用するサンプル Java クラスを使用するサンプル スクリプト

Syslog

攻撃者の IP アドレスを含む syslog メッセージを送信するセキュリティ ソリューションのリストを次に示します。 設定で正しい RegExp 規則を使用している限り、これらのソリューションは pxLog に容易に統合できます。

Snort

Snort は 次の形式の syslog アラートを送信します。

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

```
3750#show ip access-lists interface g0/17
     permit icmp any any
```
次に例を示します。

```
snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61
```
攻撃者の IP アドレスは常に最後のアドレス（宛先）の 1 つ前のアドレス（最後から 2 番目のアドレス）です。 特定のシグニチャに対するきめ細かな RegExp を作成し、攻撃者の IP アドレスを抽出することは簡単です。 シグニチャ 100124 およびインターネット制御メッセージ プロトコル（ICMP）メッセージに対する RegExp の例を次に示します。

```
snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61
```

Cisco 適応型セキュリティ アプライアンス（ASA）インスペクション

ASA が HTTP（例）インスペクションに対応して設定されている場合、対応する syslog メッセージは次のようになります。

```
Mar 12 2014 14:36:20: %ASA-5-415006: HTTP - matched Class 23:
        MS13-025_class in policy-map MS_Mar_2013_policy, URI matched -
        Dropping connection from inside:192.168.60.88/2135 to
        outside:192.0.2.63/80
```
ここでも、これらのメッセージをフィルタリングして攻撃者の IP アドレス（最後から 2 番目のアドレス）を抽出するために、きめ細かな RegExp を使用できます。

Cisco Sourcefire 次世代侵入防御システム（NGIPS）

Sourcefire センサーから送信されるメッセージの例を次に示します。

```
Jan 28 19:46:19 IDS01 SFIMS: [CA IDS][Policy1][119:15:1] http_inspect: OVERSIZE
REQUEST-URI DIRECTORY [Classification: Potentially Bad Traffic] [Priority: 2]
{TCP} 10.12.253.47:55504 -> 10.15.224.60:80
```
この場合も同じロジックが適用されるため、攻撃者の IP アドレスの抽出は簡単です。 また、ポリシー名とシグニチャが示されるため、pxLog 規則を細かく設定できます。

Juniper Netscreen

古い Juniper Intrusion Detection & Prevention（IDP）から送信されるメッセージの例を次に示します。

```
dayId="20061012" recordId="0" timeRecv="2006/10/12
21:52:21" timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0"
device_ip="10.209.83.4" cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN"
srcZn="NULL" srcIntf="NULL" srcAddr="192.168.170.20" srcPort="63396"
natSrcAddr="NULL" natSrcPort="0" dstZn="NULL" dstIntf="NULL"
dstAddr="192.168.170.10" dstPort="27374" natDstAddr="NULL" natDstPort="0"
protocol="TCP" ruleDomain="" ruleVer="5" policy="Policy2" rulebase="IDS"
ruleNo="4" action="NONE" severity="LOW" alert="no" elaspedTime="0" inbytes="0"
```

```
outbytes="0" totBytes="0" inPak="0" outPak="0" totPak="0" repCount="0"
packetData="no" varEnum="31" misc="<017>'interface=eth2" user="NULL"
app="NULL" uri="NULL"
```
攻撃者の IP アドレスは同じ方法で抽出できます。

Juniper JunOS

JunOS は次のようになります。

```
Jul 16 10:09:39 JuniperJunOS: asp[8265]:
ASP_IDS_TCP_SYN_ATTACK: asp 3: proto 6 (TCP),
ge-0/0/1.0 10.60.0.123:2280 -> 192.168.1.12:80, TCP
SYN flood attack
```

Linux iptable

Linux iptable の例を次に示します。

```
Jun 15 23:37:33 netfilter kernel: Inbound IN=lo OUT=
MAC=00:13:d3:38:b6:e4:00:01:5c:22:9b:c2:08:00 src=10.0.0.1 DST=10.0.0.100 LEN=60
TOS=0x10 PREC=0x00 TTL=64 ID=47312 DF PROTO=TCP SPT=40945 DPT=3003 WINDOW=32767
RES=0x00 SYN URGP=0
```
iptable モジュールが提供する拡張機能（接続追跡、xtable、rpfilter、パターン マッチなど）を使用して、あらゆるタイプのパケットに関する syslog 情報を送信できます。

FreeBSD IPFirewall（IPFW）

フラグメントをブロックする IPFW に関するメッセージの例を次に示します。

```
Sep  7 15:03:14 delta ipfw: 11400 Deny UDP 10.61.216.50 10.81.199.2 in via fxp0
(frag 52639:519@1480)
```

VPN 対応状況および CoA 処理

ISE は CoA 処理においてセッションのタイプを認識できます。

- 有線 802.1x/MAC 認証バイパス（MAB）の場合、ISE は CoA 再認証を送信し、これにより 2 番目の認証がトリガーされます。
- ワイヤレス 802.1x/MAB の場合、ISE は CoA 終了を送信し、これにより 2 番目の認証がトリガーされます。
- ASA VPN の場合、ISE は新しい DACL が添付された CoA を送信します（2 番目の認証は行われません）。

EPS モジュールは単純です。 隔離の実行時には、常に CoA 終了パケットを送信します。 有線/ワイヤレス セッションの場合、これは問題にはなりません（すべての 802.1X サプリカントは、2 番目の EAP セッションを透過的に開始できます）。 ただし、ASA が CoA 終了を受信すると、

VPN セッションが廃棄され、エンドユーザに対して次のようなメッセージが表示されます。

AnyConnect VPN が自動的に再接続するようにするには、2 種類の解決策があります（XML プロファイルで設定します）。

- 自動再接続。VPN ゲートウェイとの接続が失われた場合にのみ機能しますが、管理的な強制終了には使用できません。

- 常時接続。常に機能し、AnyConnect がセッションを自動的に再確立するようにします。

新しいセッションの確立時にも、ASA は新しい audit-session-id を選択します。 ISE の観点では、これは新しいセッションであり、隔離規則が発生することはありません。 VPN では、有線/ワイヤレス dot1x とは対照的に、エンドポイントの MAC アドレスを ID として使用することはできません。

解決策として、強制的に EPS を ISE として動作させ、セッションに基づいて正しいタイプの CoA を送信させます。 この機能は、ISE バージョン 1.3.1 で導入されました。

pxGrid パートナーとソリューション

pxGrid パートナーとソリューションのリストを次に示します。

- LogRhythm（セキュリティ情報およびイベント管理（SIEM））：Representational State Transfer（REST）API をサポート
- Splunk（SIEM）：REST API をサポート
- HP Arcsight（SIEM）：REST API をサポート
- Sentinel NetIQ（SIEM）：pxGrid をサポート予定
- Lancope StealthWatch（SIEM）：pxGrid をサポート予定
- Cisco Sourcefire：pxGrid をサポート予定（1HCY15）
- Cisco Web セキュリティ アプライアンス（WSA）：pxGrid をサポート予定（2014 年 4 月）

その他のパートナーとソリューションを次に示します。

- Tenable（脆弱性評価）
- Emulex（パケット キャプチャと調査）
- Bayshore Networks（データ漏洩防止（DLP）および Internet of Things（IoT）ポリシー）
- Ping Identity（アイデンティティおよびアクセス管理（IAM）/シングル サインオン（SSO））
- Qradar（SIEM）
- LogLogic（SIEM）
- Symantec（SIEM およびモバイル デバイス管理（MDM））

すべてのセキュリティ ソリューションのリストについては、Marketplace のソリューション カタログを参照してください。

ISE API： REST、EREST、pxGrid

ISE バージョン 1.3 では 3 種類の API を使用できます。

次にこれらの比較を示します。

	REST[REST]	外部 RESTful	pxGrid
クライアント認証	ユーザ名 + パスワード（基本 HTTP 認証）	ユーザ名 + パスワード（基本 HTTP 認証）	証明書
特権分離	いいえ	制限（ERS Admin）	はい（グループ）
アクセス	MnT	MnT	MnT
トランスポート	tcp/443（HTTPS）	tcp/9060（HTTPS）	tcp/5222（XMPP）
HTTP メソッド	GET	GET/POST/PUT	GET/POST
デフォルトで有効	yes	いいえ	いいえ
操作の数	少	多	少
CoA 終了	サポート対象	いいえ	サポート対象
CoA 再認証	サポート対象	いいえ	サポート対象*
ユーザ操作	いいえ	yes	いいえ
エンドポイント操作	いいえ	yes	いいえ
エンドポイント ID グループ操作	いいえ	yes	いいえ
隔離（IP、MAC）	いいえ	いいえ	yes
隔離解除（IP、MAC）	いいえ	いいえ	yes
ポートバウンス/シャットダウン	いいえ	いいえ	yes
ゲスト ユーザ操作	いいえ	yes	いいえ
ゲスト ポータル操作	いいえ	yes	いいえ
ネットワーク デバイス操作	いいえ	yes	いいえ
ネットワーク デバイス グループ操作	いいえ	yes	いいえ

* 隔離では ISE バージョン 1.3.1 の統合 CoA サポートが使用されます。

ダウンロード

pxLog は Sourceforge からダウンロードできます。

ソフトウェア開発キット（SDK）はすでに含まれています。 pxGrid の最新の SDK および API ドキュメントについては、パートナーまたはシスコ アカウント チームにお問い合わせください。

関連情報

- Cisco ISE 1.2 REST API
- Cisco ISE 1.2 外部 RESTful API
- Cisco ISE 1.3 アドミニストレータ ガイド
- テクニカル サポートとドキュメント – Cisco Systems