Catalyst 3750 シリーズ スイッチでの ISE トラフィック リダイレクション

目次

はじめに
前提条件
要件
使用するコンポーネント
背景説明
トラブルシューティング
テスト シナリオ
トラフィックがリダイレクト ACL に到達しない
トラフィックがリダイレクト ACL に到達する
シナリオ 1 - 宛先ホストが同じ VLAN にあり、存在し、SVI 10 が稼働している
シナリオ 2 - 宛先ホストが同じ VLAN にあり、存在せず、SVI 10 が稼働している
シナリオ 3 - 宛先ホストが異なる VLAN にあり、存在し、SVI 10 が稼働している
シナリオ 4 - 宛先ホストが異なる VLAN にあり、存在せず、SVI 10 が稼働している
シナリオ 5 - 宛先ホストが異なる VLAN にあり、存在し、SVI 10 がダウンしている
シナリオ 6 - 宛先ホストが異なる VLAN にあり、存在せず、SVI 10 がダウンしている
シナリオ7 - HTTP サービスがダウンしている
リダイレクト ACL - 誤ったプロトコルとポート、リダイレクションなし
関連情報

概要

この記事では、ユーザ トラフィックのリダイレクトの動作と、スイッチによってパケットをリダイレクトするために必要な条件について説明します。

前提条件

要件

Cisco Identity Services Engine（ISE）の設定の経験があり、次のトピックについて基本的な知識があることが推奨されます。

- ISE の導入と中央 Web 認証（CWA）のフロー
- 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
- ISE ソフトウェア バージョン 1.1.4 以降

背景説明

ほとんどの ISE 導入において、スイッチでのユーザ トラフィックのリダイレクトは重要なコンポーネントです。 次のフローはすべて、スイッチによるトラフィックのリダイレクトを使用します。

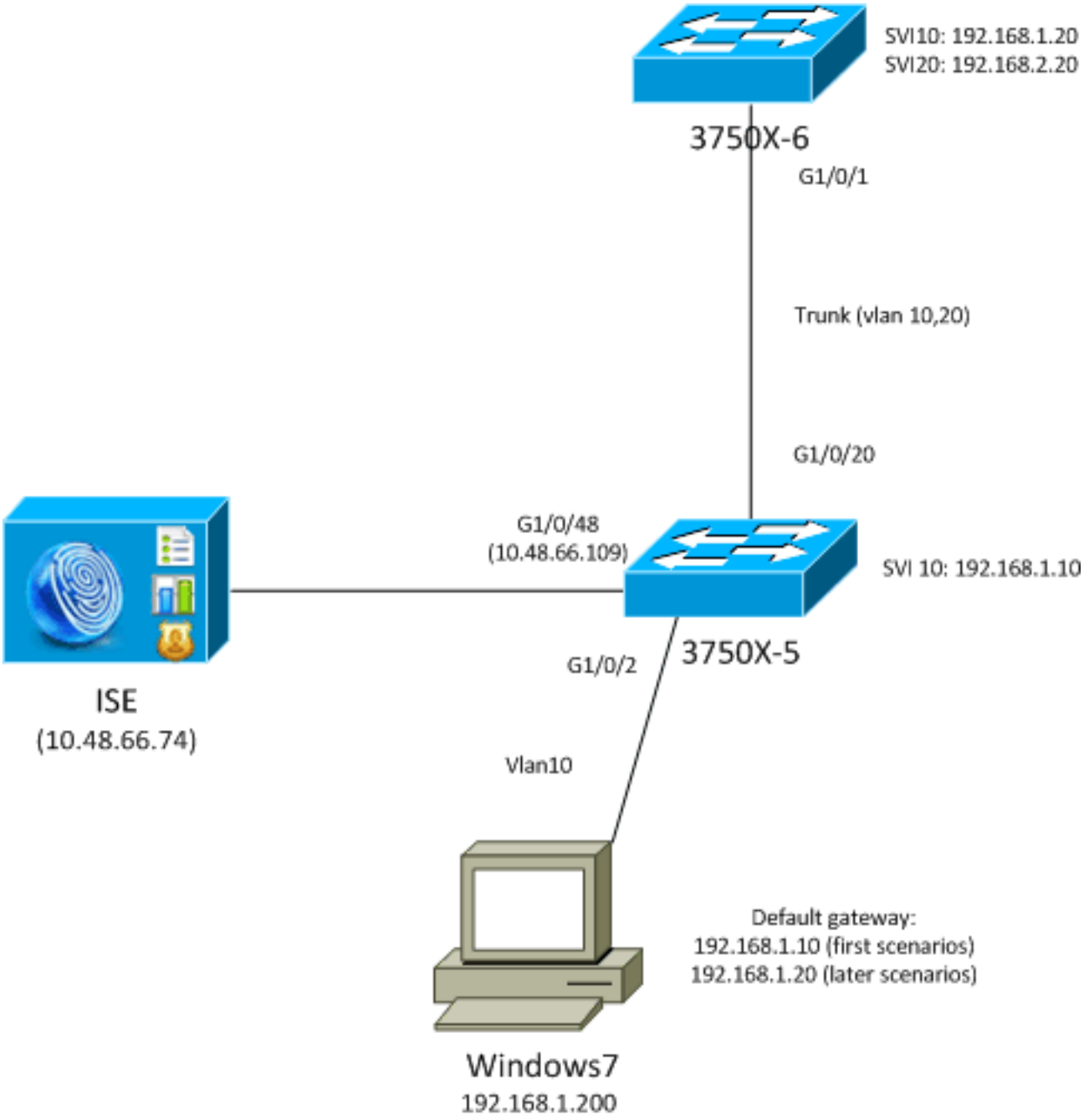
- [CWA]
- クライアント プロビジョニング（CPP）
- デバイス登録（DRW）
- ネイティブ サプリカント プロビジョニング（Native Supplicant Provisioning）（NSP）
- モバイル デバイス管理（MDM）

リダイレクトの設定を誤ると、導入においてさまざまな問題を引き起こします。 たとえば、ネットワーク アドミッション コントロール（NAC）エージェントが正しくポップアップしない、ゲスト ポータルを表示できないなどの問題が生じます。

スイッチに、クライアント VLAN と同じスイッチ仮想インターフェイス（SVI）がない場合は、最後の 3 つの例を参照してください。

トラブルシューティング

テスト シナリオ



テストは、プロビジョニング（CPP）用 ISE にリダイレクトされる必要があるクライアントで実行されます。 ユーザは、MAC 認証バイパス（MAB）または 802.1x によって認証されます。 ISE は、許可プロファイルとともに、リダイレクト アクセス コントロール リスト（ACL）の名前（REDIRECT_POSTURE）と、リダイレクト URL（ISE へのリダイレクト）を返します。

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           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:  10
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

```
    URL Redirect ACL:  REDIRECT_POSTURE
        URL Redirect:  https://10.48.66.74:8443/guestportal/gateway?sessionId=
C0A8000100000D5D015F1B47&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D5D015F1B47
     Acct Session ID:  0x00011D90
              Handle:  0xBB000D5E

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

ダウンロード可能 ACL（DACL）は、この段階ですべてのトラフィックを許可します。

```
bsns-3750-5#show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1 (per-user)
   10 permit ip any any
```

リダイレクト ACL は、このトラフィックをリダイレクトせずに許可します。

- ISE へのすべてのトラフィック（10.48.66.74）
- ドメイン ネーム システム（DNS）とインターネット制御メッセージ プロトコル（ICMP）のトラフィック

その他のトラフィックはすべてリダイレクトされます。

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
   30 deny icmp any any (10 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

スイッチは、ユーザと同じ VLAN に SVI を持っています。

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
   30 deny icmp any any (10 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

次のセクションでは、潜在的な影響を示すために、これが変更されます。

リダイレクト ACL に到達しないトラフィック

任意のホストを ping しようとすると、そのトラフィックがリダイレクトされないため、応答が受信されます。 確認するには、この debug を実行します。

```
debug epm redirect
```

クライアントから送信される各 ICMP パケットについて、次の debug が表示される必要があります。

```
Jan 9 09:13:07.861: epm-redirect:IDB=GigabitEthernet1/0/2: In
epm_host_ingress_traffic_qualify ...
Jan 9 09:13:07.861: epm-redirect:epm_redirect_cache_gen_hash:
IP=192.168.1.201 Hash=562
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: CacheEntryGet Success
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: Ingress packet on
[idb= GigabitEthernet1/0/2] didn't match with [acl=REDIRECT_POSTURE]
```

確認するには、ACL を検証します。

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
    30 deny icmp any any (4 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

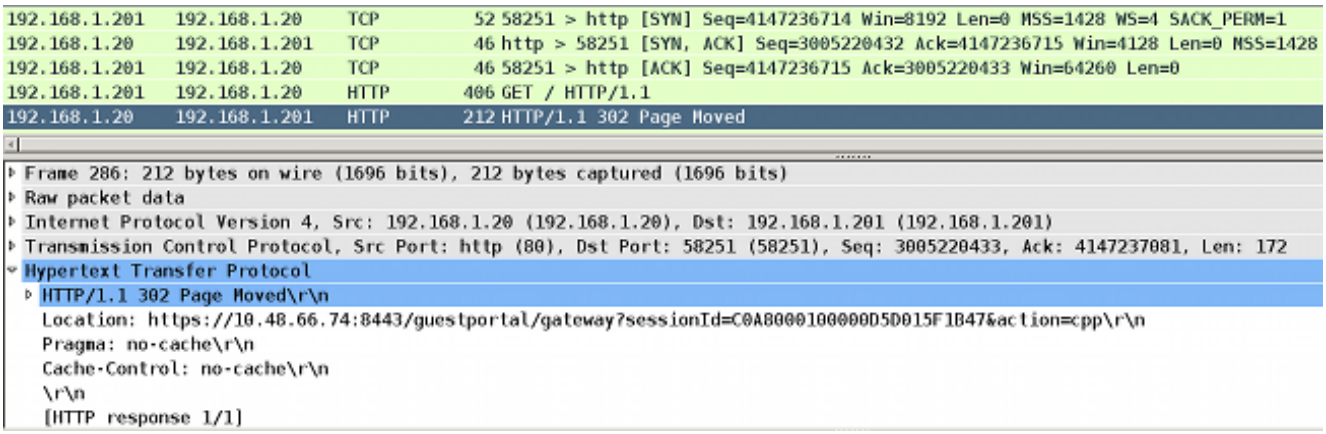
リダイレクト ACL に到達するトラフィック

シナリオ 1：宛先ホストは同じ VLAN にあり、存在し、SVI 10 UP である

スイッチ（スイッチのネットワークには SVI インターフェイスがある）によって直接レイヤ 3（L3）に到達可能な IP アドレスへのトラフィックを開始すると、次のことが起こります。

1. クライアントは同じ VLAN の宛先ホスト（192.168.1.20）のアドレス解決プロトコル（ARP）の解決要求を開始し、応答を受信します（ARP トラフィックはリダイレクトされません）。

2. スイッチに宛先 IP アドレスが設定されていない場合でも、スイッチはセッションをインターセプトします。 クライアントとスイッチ間の TCP ハンドシェイクが完了します。 この段階で、他のパケットはスイッチ外に送信されません。 このシナリオでは、クライアント（192.168.1.201）がその VLAN（192.168.1.20）に存在する他のホストと TCP セッションを開始し、これに対してスイッチが SVI インターフェイス UP（IP アドレスは 192.168.1.10）を持っています。



3. TCP セッションが確立され、HTTP 要求が送信されると、スイッチは ISE（ロケーションヘッダー）へのリダイレクトによって HTTP 応答を返します。

次の手順は、debug によって確認します。 複数の ACL がヒットしています。

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2]
matched with [acl=REDIRECT_POSTURE]
epm-redirect:Fill in URL=https://10.48.66.74:8443/guestportal/gateway?sessionId=
C0A8000100000D5D015F1B47&action=cpp for redirection
epm-redirect:IP=192.168.1.201: Redirect http request to https:
//10.48.66.74:8443/guestportal/gateway?sessionId=C0A8000100000D5D015F1B47&action=cpp
epm-redirect:EPM HTTP Redirect Daemon successfully created
```

これも、より詳細な debug によって確認できます。

```
debug ip http all

http_epm_http_redirect_daemon: got redirect request
HTTP: token len 3: 'GET'
http_proxy_send_page: Sending http proxy page
http_epm_send_redirect_page: Sending the Redirect page to ...
```

4. クライアントが ISE に直接接続します（10.48.66.74:8443 への Secure Sockets Layer（SSL）セッション）。 このパケットはリダイレクトをトリガーしません。

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] didn't
match with [acl=REDIRECT_POSTURE]
```

注: このセッションはスイッチによってインターセプトされるため、そのトラフィックは Embedded Packet Capture（EPC）を搭載しているスイッチでキャプチャされます。 前のキャプチャは、スイッチの EPC で行われます。

シナリオ 2：宛先ホストは同じ VLAN にあり、存在せず、SVI 10 UP である

宛先ホスト 192.168.1.20 がダウンした（応答がない）場合、クライアントは ARP 応答を受信せず（スイッチが ARP をインターセプトしない）、クライアントは TCP SYN を送信しません。 このため、リダイレクトは行われません。

NAC エージェントが検出にデフォルト ゲートウェイを使用するのはそのためです。 デフォルト ゲートウェイは常に応答し、リダイレクトをトリガーします。

シナリオ 3：宛先ホストは異なる VLAN にあり、存在し、SVI 10 UP である

このシナリオでは次のことが実行されます。

1. クライアントが HTTP://8.8.8.8 へのアクセスを試みます。
2. このネットワークは、スイッチ上のどの SVI にもありません。

3. クライアントはそのセッションの TCP SYN をデフォルト ゲートウェイ 192.168.1.10（既知の宛先 MAC アドレス）に送信します。

4. 最初の例とまったく同じにリダイレクトがトリガーされます。

5. スイッチはそのセッションをインターセプトし、HTTP 応答を返します。この HTTP 応答は ISE サーバにリダイレクトされます。

6. クライアントは問題なく ISE サーバにアクセスします（そのトラフィックはリダイレクトされません）。

   注: デフォルト ゲートウェイが同じスイッチまたはアップストリーム デバイスにあっても問題ありません。 リダイレクト プロセスをトリガーするのに必要な受信は、そのゲートウェイからの ARP 応答だけです。 さらに、デフォルト ゲートウェイを介した ISE のアクセシビリティを許可する必要があります。 また、ファイアウォールがパッチにあり、特に、それがレイヤ 2（L2）ファイアウォールで、L2 パケットが異なるリンクを通過する場合は、十分に注意する必要があります（ファイアウォールに TCP 状態バイパスが必要な場合があります）。

シナリオ 4：宛先ホストは異なる VLAN にあり、存在せず、SVI 10 UP である

このシナリオは、シナリオ 3 とまったく同じです。 宛先ホストがリモート VLAN に存在するかどうかは問題ではありません。

シナリオ 5：宛先ホストは異なる VLAN にあり、存在し、SVI 10 DOWN である

スイッチが、クライアントと同じ VLAN に SVI UP を持っていない場合、特定の条件が一致した場合にだけリダイレクトが行われます。

スイッチにとって問題になるのは、異なる SVI からクライアントに応答を返す方法です。 使用する送信元 MAC アドレスを決定するのは困難を伴います。

フローは SVI が UP である場合とは異なります。

1. クライアントは、アップストリーム スイッチに定義されたデフォルト ゲートウェイに設定された宛先 MAC アドレスを使用して、別の VLAN（192.168.2.20）のホストに TCP SYN を送信します。 そのパケットは debug で表示されるリダイレクト ACL に到達します。
2. スイッチは、クライアントに返されるルーティングがあるかどうかを確認します。 SVI 10 が DOWN であることを思い出してください。
3. スイッチが、クライアントに戻るルーティングを持つ別の SVI を持っていない場合、Enterprise Policy Manager（EPM）ログに ACL に到達したことが示されていても、そのパケットはインターセプトまたはリダイレクトされません。 リモート ホストは SYN ACK を返す可能性があります。ただし、スイッチはクライアントに戻るルーティング（VLAN10）を持たず、パケットはドロップされます。 パケットはリダイレクト ACL に達したため、L2 にスイッチバックされません。
4. スイッチが、異なる SVI を介するクライアント VLAN へのルーティングを持っている場合、そのパケットはインターセプトされ、通常のリダイレクトが行われます。 URL リダイレ

クトによる応答はクライアントには直接送信されませんが、ルーティングの決定に基づいて異なるスイッチ/ルータを介して送信されます。

ここでは非対称性に注目してください。

- クライアントから受信したトラフィックは、スイッチによってローカルにインターセプトされます。
- その応答には HTTP リダイレクトが含まれ、ルーティングに基づいてアップストリーム スイッチを介して送信されます。
- このときファイアウォールのよくある問題が発生する可能性があり、TCP バイパスが必要になります。
- ISE へのトラフィック（リダイレクトされない）は、対称です。 リダイレクト自体のみが非対称です。

シナリオ 6：宛先ホストは異なる VLAN にあり、存在せず、SVI 10 DOWN である

このシナリオは、シナリオ 5 とまったく同じです。 リモート ホストが存在するかどうか問題ではありません。 重要なのは、正しいルーティングです。

シナリオ 7：HTTP サービスがダウンしている

シナリオ 6 で示されているように、スイッチの HTTP プロセスは重要な役割を果たします。 HTTP サービスが無効の場合、EPM は、パケットがリダイレクト ACL に到達したことを示します。

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] matched
with [acl=REDIRECT_POSTURE]
```

ただし、リダイレクトは行われません。

スイッチの HTTPS サービスは、HTTP リダイレクトには必要ありませんが、HTTPS リダイレクトには必要です。 NAC エージェントは両方の ISE 検出を使用できます。 そのため、両方を有効にすることを推奨します。

リダイレクト ACL：不正なプロトコルとポート、リダイレクトなし

スイッチは、標準ポート（TCP/80 および TCP/443）で稼働する HTTP または HTTPS トラフィックのみをインターセプトできることに注意してください。 HTTP/HTTPS が非標準ポートで稼働している場合は、**ip port-map http** コマンドを使用して設定できます。 また、スイッチは、そのポート（**ip http port**）で自身の HTTP サーバをリッスンさせる必要があります。

関連情報

- [スイッチおよび Identity Services Engine を使用した中央 Web 認証の設定例]

- 『Cisco Identity Services Engine User Guide, Release 1.2 (Cisco Identity Services Engine ユーザ ガイド リリース 1.2) 』
- テクニカル サポートとドキュメント – Cisco Systems