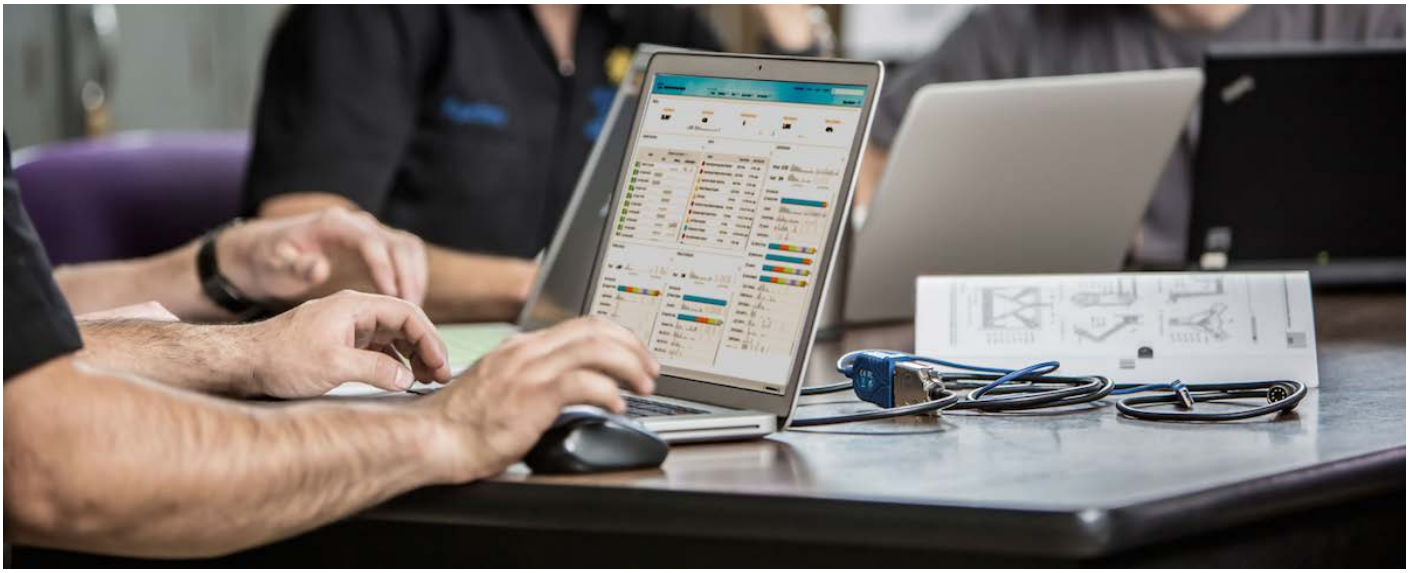

Cisco Identity Services Engine を使用したグローバル スイッチの設定

セキュア アクセスを実現するハウツー ガイド シリーズ

作成者:Fay Lee

日付:2012 年 8 月

目次

グローバル スイッチの設定

このマニュアルでは、グローバル スイッチの設定方法について説明します。Cisco TrustSec 2.1 システムにおいて、グローバル スイッチはいくつかの重要な機能を実行します。グローバル スイッチは、Web 認証用の URL のリダイレクションに加え、ポスチャ エージェント(Cisco Network Access Control (NAC)アプライアンス エージェント)から Cisco ISE サーバへのディスカバリ トラフィックのリダイレクションも処理します。このスイッチは、レイヤ 2 およびレイヤ 3 に対してネットワーク イングレスでトラフィックを適用します。レイヤ 2 にトラフィックを適用することにより、ネットワークにアクセスできるのを認証済みユーザとデバイスに制限することができます。

すべての導入で使用できるベスト プラクティスとして、一連の推奨設定を以下に示します。ベスト プラクティスの目的は、展開時のさまざまな段階、および選択したさまざまな展開タイプにおいて、設定の一貫性を保つことです。これにより、Cisco Prime™インフラストラクチャなどのソフトウェア ツールを使用して、アクセス レイヤでの複数のポート設定とトラブルシューティング作業を容易にするポート テンプレートを設定できます。

Cisco のベスト プラクティス: Cisco Prime LAN Management Solution(LMS)などのネットワーク設定管理ソリューションを使用して、企業全体の設定を管理することを推奨します。ただし、これは Cisco TrustSec 2.1 テスト ラボの一部ではないため、このマニュアルに含めることはできません。これは将来のバージョンに含める予定です。

スイッチの設定:グローバル設定

これまでの NAC ソリューションでは、アプライアンスで Web トラフィックをキャプチャし、Web 認証ページへのリダイレクションを実行する必要がありましたが、レイヤ 2 アクセス(エッジ)デバイスでの URL リダイレクションの実行により、大幅に改善されました。これにより、Web 認証とポスチャ エージェントのディスカバリ プロセスの配置が簡素化されます。

注:事前に必要な設定:このガイドでは、スイッチの基本設定が事前に完了していることを前提としています。たとえば、Network Time Protocol(NTP)を使用した正しい日付と時刻の設定はベスト プラクティスと見なされていますが、このガイドでは説明しません。

ベスト プラクティス:HTTP リダイレクションを正しく機能させるため、スイッチがクライアント サブネットと通信できることを常に確認してください。セキュリティ上のベスト プラクティスとして、スイッチを管理できるアドレスを制限するためにアクセス クラスを使用します。このトピックについては、このマニュアルでは説明しません。

スイッチで HTTPS サーバを設定する

ステップ 1 スイッチで DNS ドメイン名を設定します。

a. Cisco IOS® ソフトウェアでは、デバイス上で事前に DNS ドメイン名を定義していない場合、証明書や自己生成キーを作成およびインストールすることはできません。次を入力します。

```
C3750X(config)#ip domain-name domain_name
```

ステップ 2　次のコマンドを入力して、HTTPS で使用されるキーを生成します。

```
C3750X(config)#crypto key generate rsa general-keys mod 2048
```

注: Web リダイレクション中に発生する可能性がある証明書の不一致エラーを回避するため、ローカル証明書の代わりに、信頼できる認証局が発行した証明書を使用することを推奨します。このトピックについては、このマニュアルでは説明しません。

ステップ 3　スイッチ上で HTTP サーバをイネーブルにします。

HTTP/HTTPS キャプチャおよびリダイレクションを実行できるようにするには、HTTP サーバがスイッチ上でイネーブルになっている必要があります。次を入力します。

```
C3750X(config)#ip http server
C3750X(config)#ip http secure-server
```

注: ステップ 2 でキーを生成する前に、**ip http secure-server** コマンドを実行しないでください。正しくない順序でコマンドを実行すると、スイッチは自動的に小さいキー サイズの証明書を生成します。HTTPS トラフィックをリダイレクトするときに、この証明書により、望ましくない動作が発生する可能性があります。

グローバル AAA コマンドの設定

ステップ 1　アクセス スイッチ上で認証、許可、およびアカウンティング（AAA）をイネーブルにします。

デフォルトでは、シスコ スイッチの AAA「サブシステム」はディセーブルになっています。AAA サブシステムをイネーブルにする前の時点では、設定で必要なコマンドがすべて使用不可です。次を入力します。

```
C3750X(config)#aaa new-model
```

注: このコマンドは、AAA ネットワーク セキュリティ サービスが提供するすべてのサービス（たとえばローカル ログインの認証と許可、認証方式リストの定義と適用など）をイネーブルにします。詳細については、『Cisco IOS Security Configuration Guide』を参照してください。

ステップ 2　802.1X の認証方式を作成します。

802.1X 認証要求にどの RADIUS サーバ グループを使用するかをスイッチに指示するには、認証方式が必要です。

```
C3750X(config)#aaa authentication dot1x default group radius
```

ステップ 3　802.1X の認可方式を作成します。

ステップ 2 で作成した方式により、ユーザ/デバイス ID（ユーザ名/パスワードまたは証明書）を RADIUS サーバで検証できるようになります。ただし、有効なクレデンシャルを単に持っているだけでは不十分です。認可も必要になります。認可とは、ユーザまたはデバイスが実際にネットワークにアクセスできること、および実際に許可されるアクセス レベルを定義することです。

```
C3750X(config)#aaa authorization network default group radius
```

ステップ 4　802.1X のアカウンティング方式を作成します。

RADIUS アカウンティング パケットは非常に役立ち、多くの ISE 機能で必要とされます。これらのタイプのパケットにより、RADIUS サーバ（Cisco ISE）はスイッチポートとエンドポイントの正確な状態を認識することができます。アカウンティング パケットがなければ、Cisco ISE が認識できるのは認証と認可の通信だけになります。アカウンティング パケットは、認可されたセッションの長さや、スイッチによるローカル決定に関する情報を提供します（AuthFail VLAN 割り当てなど）。

```
C3750X(config)#aaa accounting dot1x default start-stop group radius
```

グローバル RADIUS コマンドの設定

RADIUS サーバの可用性を予防的に検査する方式を設定します。このプラクティスでは、スイッチが RADIUS サーバ（Cisco ISE）に定期的なテスト認証メッセージを送信します。そしてサーバからの RADIUS 応答を待機します。成功メッセージは必須ではありません。認証失敗であっても、サーバが稼働していることを示しているため、問題ありません。

ベスト プラクティス: Cisco ISE 1.1(377)でロギング サーバからこれらの認証をフィルタリングすることはできません。フィルタリングにより、Cisco ISE ダッシュボードに表示される認証成功/失敗が非対称になります。このため、認証が成功し、認可ではアクセスが拒否されるアカウントを使用することを推奨します。

ステップ 1 グローバル コンフィギュレーション モードで、RADIUS キープアライブ インターバルのユーザ名とパスワードを入力します。

ここで作成するユーザ名は、後の手順で Cisco ISE のローカル ユーザ データベースに追加されます。このアカウントは、後の手順で RADIUS サーバを定義する際に使用されます。

```
C3750X(config)#username radius-test password password
```

ステップ 2 RADIUS グループに Cisco ISE サーバを追加します。

この手順では、すでに作成したテスト アカウントを使用して、各 Cisco ISE ポリシー サービス ノード(PSN)をスイッチ設定に追加します。各 PSN に対して、この手順を繰り返します。

```
C3750X(config)#radius-server host ise_ip_address auth-port 1812 acct-port 1813 test username
radius-test key shared_secret
```

注: サーバは、通常のプロセスで発生する認証または認可に加えて、1 時間に 1 回、応答があるかどうか予防的に検査されます。

ステップ 3 デッド条件を設定します。

Cisco ISE サーバでの RADIUS 応答を予防的に検査するよう、スイッチが設定されました。次に、サーバが動作中/デッド状態のどちらであるか判断するために、スイッチでカウンタを設定します。この設定では、RADIUS サーバからの応答を 5 秒間待ち、テストを 3 回試行した後で、サーバにデッド マークを付けます。Cisco ISE サーバから 15 秒以内に有効な応答がない場合、デッド マークが付きます。

```
C3750X(config)#radius-server dead-criteria time 5 tries 3
```

注: ハイ アベイラビリティについては、導入モードのセクションで詳しく説明します。

ステップ 4 認可変更(CoA)をイネーブルにします。

先ほど、スイッチからの RADIUS メッセージの送信先となる RADIUS サーバの IP アドレスを定義しました。しかし、ここでは次のようにして、別のリストで(さらにグローバル コンフィギュレーション モード内で)認可変更(RFC 3576)操作を実行できるサーバを定義します。

```
C3750X(config)#aaa server radius dynamic-author
C3750X(config-locsvr-da-radius)#client ise_ip_address server-key shared_secret
```

ステップ 5 Cisco ベンダー固有属性を使用するようにスイッチを設定します。

ここでは、認証要求およびアカウンティング更新時に、定義済みのベンダー固有属性（VSA）を Cisco ISE PSN に送信するようスイッチを設定します。

```
C3750X(config)#radius-server vsa send authentication
C3750X(config)#radius-server vsa send accounting
```

ステップ 6 次に、ベンダー固有属性（VSA）をイネーブルにします。

```
C3750X(config)#radius-server attribute 6 on-for-login-auth
C3750X(config)#radius-server attribute 8 include-in-access-req
C3750X(config)#radius-server attribute 25 access-request include
```

ステップ 7 スイッチが常に適切なインターフェイスからトラフィックを送信することを確認します。

複数の IP アドレスがスイッチに関連付けられることがよくあります。したがって、1 つの特定のインターフェイスを介してすべての管理通信が行われるようにするのがベスト プラクティスです。このインターフェイスの IP アドレスは、Cisco ISE ネットワーク オブジェクトで定義される IP アドレスに一致する必要があります。

Cisco ベスト プラクティス：ネットワーク管理のベスト プラクティスとして、すべての管理通信でループバック アダプタを使用し、内部ルーティング プロトコルにそのループバック インターフェイスをアドバタイズします。

```
C3750X(config)#ip radius source-interface interface_name
C3750X(config)#snmp-server trap-source interface_name
C3750X(config)#snmp-server source-interface informs interface_name
```

Cisco ISE との間のプロファイリングを許可するようにスイッチを設定します。

Cisco ISE は Simple Network Management Protocol（SNMP）を使用し、スイッチに対して特定の属性をクエリすることで、スイッチに接続されたデバイスを識別します。ここでは Cisco ISE がクエリできるように、また SNMP トラップが Cisco ISE に送信されるように、SNMP コミュニティを設定します。

ステップ 1 読み取り専用 SNMP コミュニティを設定します。

Cisco ISE は「読み取り専用」SNMP コマンドのみを必要とします。このコミュニティ ストリングが、Cisco ISE のネットワーク デバイス オブジェクトで設定されたものと一致することを確認します。

Cisco ベスト プラクティス：セキュリティの観点から、アクセス クラスによりスイッチへの SNMP アクセスを制限することがベスト プラクティスと考えられています。SNMP 設定は Cisco TrustSec 2.1 のテスト ベッドの一部ではないため、このマニュアルには含まれません。

```
C3750X(config)#snmp-server community community_string RO
```

ステップ 2 トラップを送信するようにスイッチを設定します。

次に、MAC アドレス テーブルの変更に伴い SNMP トラップが送信されるようにします。アドレス テーブルでアドレスが新規挿入、削除、または移動されるたびに、デバイスの MAC アドレスおよびインターフェイス ID を含むトラップが Cisco ISE に送信されます。

```
C3750X(config)#snmp-server enable traps mac-notification change move threshold
```

ステップ 3 SNMP トラップ レシーバとして Cisco ISE を追加します。

ここでは、設定済み MAC 通知のトラップ レシーバとしてサーバが追加されます。

```
C3750X(config)#snmp-server host ise_ip_address version 2c community_string mac-notification
```

ステップ 4 信頼できるポートの Dynamic Host Configuration Protocol（DHCP）スヌーピングを設定します。

DHCP スヌーピングは Cisco TrustSec 2.1 では必須でありませんが、ベスト プラクティスと見なされます。この機能により、不正な DHCP サーバを拒否することで可用性が改善するだけでなく、ダイナミック Address Resolution Protocol（ARP）検査などの他のセキュリティ ツール用にスイッチを準備できます。また、DHCP スヌーピングは、将来の Cisco TrustSec テクノロジー リリースで提供される機能用にスイッチを準備するうえでも役立ちます。

DHCP スヌーピングを設定する前に、信頼できる DHCP サーバの場所をよく確認してください。DHCP スヌーピングを設定すると、スイッチは、「trusted」と設定されていないすべてのポートからの DHCP サーバ応答を拒否します。アップリンク インターフェイスのインターフェイス コンフィギュレーション モードを開始し、信頼できるポートとして設定します。

注: アップリンク ポートがレイヤ 3 インターフェイスではなく、スイッチ ポートまたはトランクである場合にのみ、この手順が必要です。このセクションの最後にある設定例で **ip dhcp snooping trust** コマンドがに記載されていないのは、このためです。

```
C3750X(config)#interface interface_name
C3750X(config-if)#ip dhcp snooping trust
```

ステップ 5 DHCP スヌーピングをイネーブルにします。

DHCP スヌーピングがグローバル コンフィギュレーション モードでイネーブルになります。DHCP スヌーピングをイネーブルにした後、それを処理する VLAN を次のように設定する必要があります。

```
C3750X(config)#ip dhcp snooping
C3750X(config)#ip dhcp snooping vlan vlan_id_or_vlan_range
```

ローカル アクセス コントロール リストの設定

URL リダイレクションなど、スイッチのいくつかの機能では、ローカルに設定されたアクセス コントロール リスト（ACL）を使用する必要があります。作成するこれらの ACL にはすぐに使用されるものもありますが、導入の後半のフェーズまで使用されないものもあります。このセクションの目的は、可能なすべての導入モデルのスイッチを一度に準備し、スイッチ設定の繰り返しによる運用コストを抑えることです。

ステップ 1 モニタ モードでスイッチポートに使用する次の ACL を追加します。

```
C3750X(config)#ip access-list ext ACL-ALLOW
C3750X(config-ext-nacl)#permit ip any any
```

ステップ 2 ロー インパクトおよびクローズ モードでスイッチポートに使用する次の ACL を追加します。

```
C3750X(config)#ip access-list ext ACL-DEFAULT
C3750X(config-ext-nacl)#remark DHCP
C3750X(config-ext-nacl)#permit udp any eq bootpc any eq bootps
C3750X(config-ext-nacl)#remark DNS
C3750X(config-ext-nacl)#permit udp any any eq domain
C3750X(config-ext-nacl)#remark Ping
C3750X(config-ext-nacl)#permit icmp any any
C3750X(config-ext-nacl)#remark PXE / TFTP
C3750X(config-ext-nacl)#permit udp any any eq tftp
C3750X(config-ext-nacl)#remark Drop all the rest
C3750X(config-ext-nacl)#deny ip any any log
```

ステップ 3 Web 認証による URL リダイレクションで使用する次の ACL を追加します。

```
C3750X(config)#ip access-list ext ACL-WEBAUTH-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect all applicable traffic to the ISE Server
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#permit tcp any any eq 443
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the redirection
```

ステップ 4 ポスチャ エージェントによる URL リダイレクションで使用する次の ACL を追加します。

```
C3750X(config)#ip access-list ext ACL-AGENT-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect HTTP traffic only
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the redirection
```

グローバル 802.1X コマンドの設定

ステップ 1 スイッチで 802.1X 認証をグローバルにイネーブルにします。

スイッチで 802.1X をグローバルにイネーブルにしても、実際にはどのスイッチポートの認証もイネーブルになりません。認証は設定されますが、モニタ モードを設定するまではイネーブルになりません。

```
C3750X(config)#dot1x system-auth-control
```

ステップ 2 ダウンロード可能な ACL が機能するようにします。

ダウンロード可能アクセス コントロール リスト(dACL)は、Cisco TrustSec の導入において非常に一般的な適用メカニズムです。dACL がスイッチで正しく機能するには、IP デバイス トラッキングが次のようにグローバルにイネーブルにされている必要があります。

```
C3750X(config)#ip device tracking
```

注: Windows 7 や、ARP に応答しないデバイスの場合、特殊なケースでは **ip device tracking use SVI** コマンドを使用する必要が生じます。

ステップ 3 スイッチ上で syslog をイネーブルにします。

多くのイベントで syslog が Cisco IOS® ソフトウェア上に生成されることがあります。syslog メッセージの一部を、トラブルシューティング用に Cisco ISE に送信できます。Cisco ISE がスイッチからの適切な syslog メッセージを確実にコンパイルできるようにするには、次のコマンドを使用します。

注:モニタ ペルソナを使用して Cisco ISE ノードにログを送信する必要があります。

```
C3750X(config)#logging monitor informational
C3750X(config)#logging origin-id ip
C3750X(config)#logging source-interface <interface_id>
C3750X(config)#logging host <ISE_MNT_PERSONA_IP_Address_x> transport udp port 20514
```

Cisco ISE の機能に関連して発生する可能性があるトラブルシューティングや記録をサポートするには、次のように、スイッチで標準のロギング機能を設定します。適用ポリシー モジュール(EPM)は、Web 認証やダウンロード可能 ACL などの機能を担当する Cisco IOS ソフトウェアの一部です。

EPM ロギングをイネーブルにすると、ダウンロード可能 ACL 認可に関連した syslog が生成され、そのようなログが Cisco ISE に送られる場合はログの一部を Cisco ISE 内で関連付けることができます。

注: コンセプト実証またはパイロットのためには syslog をイネーブルにするのが適切です。すでに確立された大規模な導入では、トラフィック量が懸念される場合は syslog を無効にできます。

```
C3750X(config)#epm logging
```

実際に収集されて Cisco ISE によって使用される NAD syslog メッセージは、次のものだけです。

- AP-6-AUTH_PROXY_AUDIT_START
- AP-6-AUTH_PROXY_AUDIT_STOP
- AP-1-AUTH_PROXY_DOS_ATTACK
- AP-1-AUTH_PROXY_RETRIES_EXCEEDED
- AP-1-AUTH_PROXY_FALLBACK_REQ
- AP-1-AUTH_PROXY_AAA_DOWN
- AUTHMGR-5-MACMOVE
- AUTHMGR-5-MACREPLACE
- MKA-5-SESSION_START
- MKA-5-SESSION_STOP
- MKA-5-SESSION_REAUTH
- MKA-5-SESSION_UNSECURED
- MKA-5-SESSION_SECURED
- MKA-5-KEEPALIVE_TIMEOUT
- DOT1X-5-SUCCESS / FAIL
- MAB-5-SUCCESS / FAIL
- AUTHMGR-5-START / SUCCESS / FAIL
- AUTHMGR-SP-5-VLANASSIGN / VLANASSIGNERR
- EPM-6-POLICY_REQ
- EPM-6-POLICY_APP_SUCCESS / FAILURE
- EPM-6-IPEVENT:
- DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND
- RADIUS-4-RADIUS_DEAD

グローバル設定の例

```
hostname C3750X
username radius-test password 0 Cisco123
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 10.1.100.3 server-key Cisco123
!
ip dhcp snooping vlan 10-13
ip dhcp snooping
ip domain-name cts.local
ip device tracking
!
dot1x system-auth-control
!
ip http server
ip http secure-server
!
ip access-list extended ACL-AGENT-REDIRECT
 remark explicitly prevent DNS from being redirected to address a bug
 deny   udp any any eq domain
 remark redirect HTTP traffic only
 permit tcp any any eq www
 remark all other traffic will be implicitly denied from the redirection
ip access-list extended ACL-ALLOW
 permit ip any any
ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark Ping
 permit icmp any any
 remark PXE / TFTP
 permit udp any any eq tftp
 remark Drop all the rest
 deny   ip any any log
ip access-list extended ACL-WEBAUTH-REDIRECT
 remark explicitly prevent DNS from being redirected to accommodate certain switches
 deny   udp any any eq domain
 remark redirect all applicable traffic to the ISE Server
 permit tcp any any eq www
 permit tcp any any eq 443
 remark all other traffic will be implicitly denied from the redirection
!
ip radius source-interface Loopback0
snmp-server community Cisco123 RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.1.100.3 version 2c Cisco123  mac-notification
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
radius-server host 10.1.100.3 auth-port 1812 acct-port 1813 test username radius-test key
Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
logging monitor informational
epm logging
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.100.3 transport udp port 20514
```

スイッチ：ユニバーサル スイッチポートの設定

前のセクションでは、RADIUS、SNMP、プロファイリング、および AAA メソッドといったアクセス レイヤ スイッチのグローバル設定に関するユニバーサル コマンドを定義しました。

このセクションでは、使用するスイッチ タイプや導入モデルに関係なく、Cisco TrustSec 導入全体で使用できる 1 つのポート設定の作成について説明します。

注：Cisco Prime LAN Management Solution（LMS）4.1 などの一括構成ツールを使用する場合、状況によっては、他の何らかのコマンドを実行する前に、このコマンドを必ず実行する必要があります。

基本的なスイッチポートの設定

スイッチポートでの認証設定を行う前に、スイッチ ポートがレイヤ 3 ポートではなく、レイヤ 2 ポートとして設定されていることを確認する必要があります。ここで実行するコマンドは、単純な一語のコマンドであり、それ以降、実行される他のコマンドがすべて有効になります。

ステップ 1 スイッチポート範囲のインターフェイス コンフィギュレーション モードを次のように開始します。

```
C3750X(config)#interface range first_interface - last_interface
```

ステップ 2 ポートがレイヤ 2 のスイッチポートであることを確認します。

```
C3750X(config-if-range)#switchport
```

ステップ 3 ホスト マクロを使用して、レイヤ 2 エッジのポートを設定します。

ホスト マクロは自動的に 3 つのコマンドを実行します。これにより、ポートはアクセス ポート（非トランク）になるように設定され、チャネル グループは無効になり、スパニング ツリーが PortFast モードになるように設定されます。

```
C3750X(config-if-range)#switchport host
! - Switch Output:
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

認証設定 – フレキシブル認証およびハイ アベイラビリティ

802.1X のデフォルト動作では、認証に失敗するとネットワークへのアクセスが拒否されます。この動作は多くのお客様の導入環境で望ましくないものであることが分かりました。ゲスト アクセスが許可されず、従業員が自分のコンピュータ システムを修復してフル ネットワーク アクセスを取得することもできないためです。802.1X 認証失敗を扱う次のフェーズとして、「認証失敗 VLAN」を提供し、認証に失敗したデバイス/ユーザが、限定的なリソースを提供する VLAN にアクセスできるようになりました。

この手順は適切であるとはいえ、依然として十分に実用的ではありません。特に、すべてのプリンタその他の非認証デバイスに MAC 認証バイパスを使用する必要がある環境ではそうです。802.1X のデフォルト動作の場合、管理者は、サプリカントを持たないプリンタその他のデバイスに関して、認証を行うポートとは異なる方法でポートを設定する必要があります。

そのため、シスコはフレキシブル認証（Flex-Auth）を開発しました。Flex-Auth を使用することにより、ネットワーク管理者はスイッチポートでの認証順序とプライオリティを設定でき、結果としてポートは 802.1X、MAC 認証バイパス、Web 認証の順に試行できます。すべてのアクセス ポートで同じ設定を維持しながらこれらすべての機能を提供できるため、従来の 802.1X 導入よりもさらに簡単な運用モデルがお客様に提供されます。

前述のように、スイッチ ポートの認証には複数の方式、つまり、802.1X （dot1x）、MAC 認証バイパス（MAB）、および Web ベースの認証（Web-Auth）があります。802.1X 認証を使用した場合、スイッチは、リンク状態が「up」に変更されるとアイデンティティ要求（EAP ID 要求）を定期的に送信します（推奨されるタイマー変更については、「認証設定 - タイマー」セクションを参照）。また、エンドポイント サプリカントは、スイッチポートに EAP over LAN Start（EAPoL 開始）メッセージを定期的に送信し、認証を高速化する必要があります。デバイスが認証できない場合は、dot1x タイムアウトを待つだけです。その後、MAC 認証バイパス（MAB）が発生します。デバイスの MAC アドレスが正しいデータベース内にあれば、ネットワークにアクセスする権限が付与されます（図 3）。

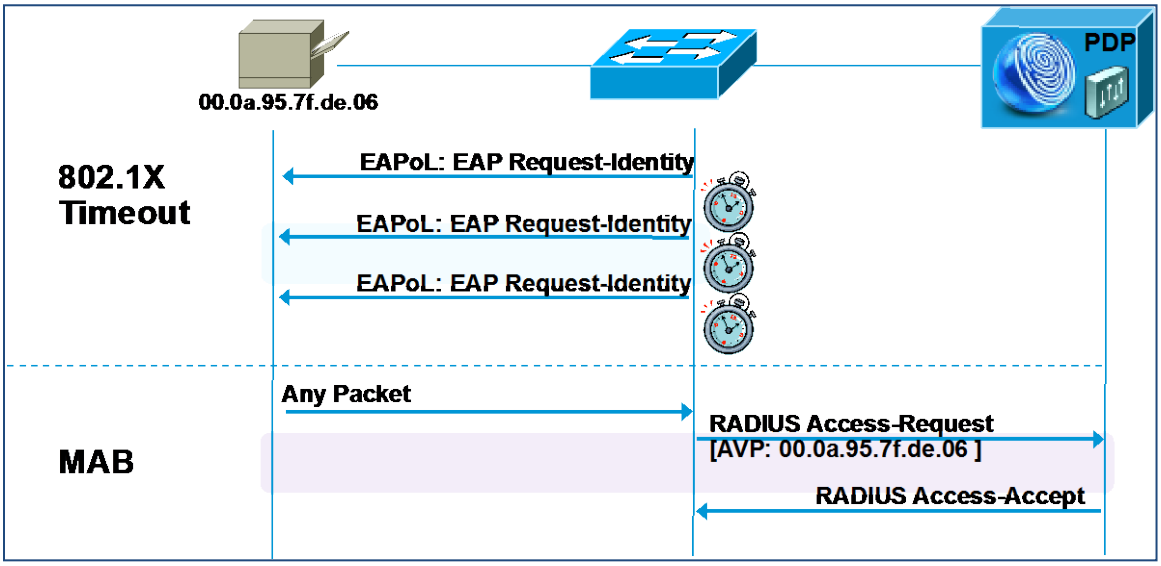

図 1.　フレキシブル認証

次の手順では、認証のハイ アベイラビリティを実現するためのフレキシブル認証（Flex-Auth）の設定について、および設定可能なアクションについて説明します。

ステップ 4 スイッチポートでの認証方式のプライオリティを設定します。

ベスト プラクティスは、より強力な認証方式（dot1x）を常に優先させることです。dot1x 方式は、すべてのシスコ スイッチにおけるデフォルトでもあります。

```
C3750X(config-if-range)#authentication priority dot1x mab
```

ステップ 5 スイッチ ポートでの認証方式の順序を設定します。

特定の導入方式では、802.1X 認証の前に MAC 認証バイパス（MAB）を実行すべき場合もあります。このような稀なケースの場合、シスコ スイッチでは、ユーザ定義可能な認証順序をネットワーク管理者が設定することができます。ただし、ベスト プラクティスは、dot1x の次に MAB という順序を維持することです。

```
C3750X(config-if-range)#authentication order dot1x mab
```

注：authentication order コマンドのオプションとして、このほかに Web 認証もあります。ここで設定される Web 認証（Web-Auth）とは、ローカル Web 認証を指しています。ベスト プラクティスは、中央集中型 Web 認証を使用することです。Web 認証の詳細については、「Web 認証」を参照してください。

ステップ 6 Flex-Auth を使用するポートを次のように設定します。

```
C3750X(config-if-range)#authentication event fail action next-method
```

ステップ 7 RADIUS サーバがダウンしているときにローカル VLAN を使用するようポートを設定します。

「グローバル RADIUS コマンドの設定」の手順では、Cisco ISE が RADIUS 要求への応答を停止した場合に、予防的にスイッチに警告を出すテスト アカウントを使用するように RADIUS サーバ エントリを設定しました。ここでは、そのサーバが「デッド状態」であるとわかった場合にローカルにポートを認証し、サーバが再稼働したときに認証を再初期化するようにスイッチポートを設定します。

```
C3750X(config-if-range)#authentication event server dead action reinitialize vlan vlan-id
```

この機能は、単一ポートでの複数の認証ホストに関する問題を解決するために導入されました。つまり、RADIUS サーバが動作状態であるときに認証ホストの一部がすでに認証され、RADIUS サーバがダウンしているときに他のホスト（新しいホスト）が認証を試行しているという状況です。

この新しい機能が導入される前は、（RADIUS サーバが稼働しているときに）すべての認証済みホストにネットワークへのフル アクセス権限が与えられるのに対し、他のホスト（新しいホスト）にはネットワークアクセス権限が与えられませんでした。この新しいコマンドライン インターフェイス（CLI）機能を使用すると、RADIUS サーバがダウンしているときに新しいホストがネットワークにアクセスしようとすると、そのポートがただちに再初期化され、（このポート内の）すべてのホストが同じ VLAN を取得します。

ステップ 8 RADIUS サーバのダウン時にネットワーク上で電話を使用できるようにポートを設定します。

device-traffic-class=voice 属性を渡すよう RADIUS サーバを設定すると、認証の成功後に電話が音声ドメインに配置されます。しかし、RADIUS サーバが使用不可になると電話は音声ネットワークにアクセスできず、機能できません。ここでクリティカル音声 VLAN という新機能を使用できます。この新機能では、ポートがクリティカル認証モードである場合、ホストからのトラフィックに音声 VLAN タグが付いていると、ポートに関して設定された音声 VLAN にデバイス(電話)が配置されます。電話は Cisco Discovery Protocol (CDP)、Link Layer Discovery Protocol(LLDP)、または DHCP を介して音声 VLAN の ID を認識します。この機能を有効にするコマンドは次のとおりです。

```
C3750X(config-if-range)#authentication event server dead action authorize voice
```

ステップ 9 ポートのホスト モードを設定します。

802.1X 対応ポートのデフォルト動作では、ポートごとに 1 つの MAC アドレスだけを許可します。その他にも、マルチドメイン認証(MDA)モードおよびマルチ認証(Multi-Auth)モードなどのオプションがあります。Cisco TrustSec 導入の初期フェーズにおけるベスト プラクティスは、802.1X の導入時にサービス拒否が発生しないようマルチ認証モードを使用することです。

注: Cisco TrustSec 導入ではポート セキュリティは推奨されません。これは、802.1X がこの機能をネイティブに扱うためです。

マルチ認証(Multi-Auth)モードを使用すると、スイッチポートごとに実質的に無制限の MAC アドレスを使用でき、すべての MAC アドレスで認証済みセッションが必要になります。導入プロセスで認証フェーズの後半または適用フェーズに移ったら、マルチドメイン モードを使用することが推奨されます。マルチドメイン認証では、データドメイン内の 1 つの MAC アドレス、および音声ドメイン内の 1 つの MAC アドレスをポートごとに使用できるようになります。

```
C3750X(config-if-range)#authentication host-mode multi-auth
```

ステップ 10 違反アクションを設定します。

ポートで許可される数よりも多くの MAC アドレスが存在するといった、認証違反が発生した場合、デフォルトのアクションは、ポートを error-disabled 状態にすることです。この動作は適切かつ安全に思えるかもしれませんが、特に導入の初期フェーズでは誤ってサービス拒否を発生させる可能性があります。このため、制限するアクションを設定します。この動作モードでは、最初に認証されたデバイスの許可を継続し、追加のデバイスをすべて拒否することができます。

```
C3750X(config-if-range)#authentication violation restrict
```

認証設定 – オープン認証および追加の手順

802.1X はデフォルトでバイナリとして設計されています。認証の成功は、ユーザがネットワークにアクセスできることを意味します。認証の失敗は、ユーザがネットワークにアクセスできないことを意味します。このパラダイムは現代の組織にはあまり適していません。ほとんどの組織では、Pre-Execution Environments（PXE）によるワークステーションのイメージングを行う必要があります。または、サプリカントを実行できず、DHCP で起動する必要があるシン クライアントを抱えている場合もあります。

さらに、802.1X をいち早く採用した組織が認証を企業全体に導入した際、いくつかの反動もありました。たとえば、サプリカントの設定が間違っていたり、サプリカントの欠如などのさまざまな理由により、不明なデバイスを認証できないといった問題です。以下の図 1 を参照してください。

シスコは導入を支援するためにオープン認証モードを作成しました。オープン認証では、ポートが承認されなくても、すべてのトラフィックがスイッチポートを通過できます。この機能により、アクセス拒否を発生させずに、認証を組織全体に設定できます。

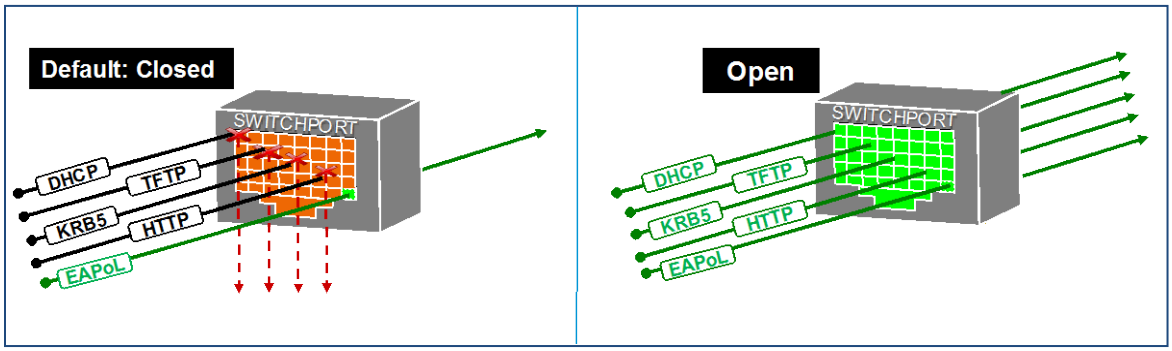

図 2.　デフォルトの認証モード（クローズ）とオープン認証モード

ステップ 1　オープン認証用のポートを設定します。

```
C3750X(config-if-range)#authentication open
```

ステップ 2　ポート上で MAC 認証バイパスをイネーブルにします。

```
C3750X(config-if-range)#mab
```

ステップ 3　IEEE 802.1X 認証を実行するようにポートを設定します。

```
C3750X(config-if-range)#dot1x pae authenticator
```

認証設定:タイマー

導入時に、必要に応じて多くのタイマーを変更できます。特定の問題が発生していて、タイマーを調整すると不適切な動作が修正される可能性があるような場合を除き、802.1X 送信タイマー(tx-period)以外のすべてのタイマーをデフォルト値のままにしておくことを推奨します。

tx-period タイマーのデフォルト値は 30 秒です。この値を 30 のままにしておくと、スイッチポートが次の認証方式を開始するまで、デフォルトで 90 秒間(tx-period の 3 倍)待機し、未認証デバイス用の MAB プロセスが開始されます。

Cisco ベスト プラクティス:多数の導入事例に基づくベスト プラクティスとして、tx-period 値を 10 秒に設定することで MAB デバイスに最適な時間を指定するようお勧めします。10 秒未満の値を設定すると、ポートが MAC 認証バイパスに移行するタイミングが速すぎる可能性があります。

ステップ 1 tx-period タイマーを設定します。

```
C3750X(config-if-range)#dot1x timeout tx-period 10
```

ポートで最初の ACL を適用して認証をイネーブルにする

この手順では、モニタ モード用にポートを準備します。どのトラフィックも拒否することなく、ポートでデフォルト ACL を適用します。

ステップ 1 最初の ACL(ACL-ALLOW)を適用します。

```
C3750X(config-if-range)#ip access-group ACL-ALLOW in
```

ステップ 2 認証をオンにします。

```
C3750X(config-if-range)#authentication port-control auto
```

注:認証(802.1X、MAB、Web 認証)をイネーブルにするにはこのコマンドが必要です。このコマンドを使用しないと、すべての機能が動作しているように見えても、実際にはどの認証も RADIUS サーバに送信されません。

付録 A：参照

Cisco TrustSec システム：

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

デバイス設定ガイド：

Cisco Identity Services Engine ユーザ ガイド：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco NX-OS ソフトウェア リリースの詳細については、次の URL を参照してください。

- Cisco Catalyst 2900 シリーズ スイッチの場合：
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000 シリーズ スイッチの場合：
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000-X シリーズ スイッチの場合：
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 4500 シリーズ スイッチの場合：
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 6500 シリーズ スイッチの場合：
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- Cisco ASR 1000 シリーズ ルータの場合：
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

Cisco Wireless LAN Controller の場合：
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html