シングルホストとマルチドメインのシナリオ用 IBNS 2.0 の設定

目次

概要

本書では、シングルホスト シナリオとマルチドメイン シナリオ用に Identity Based Networking Services 2.0（IBNS）を設定する方法について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- ローカル エリア ネットワーク上の Extensible Authentication Protocol（EAPoL）
- RADIUS プロトコル
- Cisco Identity Services Engine バージョン 2.0

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。

- Cisco Identity Service Engine バージョン 2.0 パッチ 2
- Windows 7 OS 搭載エンドポイント
- IOS 15.2(4)E1 搭載 Cisco スイッチ 3750X
- 03.02.03.SE 搭載 Cisco スイッチ 3850
- Cisco IP Phone 9971

このドキュメントの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。 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

構成理論

IBNS 2.0 を有効にするには、Cisco スイッチ上から権限モードでコマンドを実行する必要があります。

```
#authentication display new-style
```

以下のコマンドを使用して、IBNS 2.0 のスイッチポートを設定します。

```
 access-session host-mode {single-host | multi-domain | multi-auth}
 access-session port-control auto
 dot1x pae authenticator
{mab} service-policy type control subscriber TEST
```

上記のコマンドは、インターフェイスで dot1x 認証とオプションで MAC 認証バイパス（MAB）を有効にします。 新しい構文を使用するときには、access-session で始まるコマンドを使用します。 これらのコマンドの目的は、古い構文（**authentication** キーワードで始まる構文）を使用するコマンドと同じです。 インターフェイスに使用する必要のある **policy-map** を指定するには、**service-policy** を適用します。

上記の **policy-map** は、認証中にスイッチ（オーセンティケータ）の動作を定義します。 たとえば、認証に失敗した場合に実行する処理を指定できます。 **イベント**ごとに、設定されている **class-map** 内の一致したイベントのタイプに基づいて、複数のアクションを設定できます。 例として、下記のリスト（**policy-map TEST4**）を参照してください。 このポリシーが適用されているインターフェイスに接続されている dot1x エンドポイントが失敗すると、**DOT1X_FAILED** で定義されたアクションが実行されます。 **MAB_FAILED** や **DOT1X_FAILED** などのクラスに対して同じ動作を指定するには、デフォルト クラスの **class-map always** を使用できます。

```
policy-map type control subscriber TEST4
(...)
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
(...)
  40 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
(...)
```

IBNS 2.0 に使用する **policy-map** のタイプは必ず**コントロール サブスクライバ**である必要があります。

使用可能なイベントのリストは、次の方法で表示できます。

```
Switch(config-event-control-policymap)#event ?
  aaa-available                 aaa-available event
  absolute-timeout              absolute timeout event
  agent-found                   agent found event
  authentication-failure        authentication failure event
  authentication-success        authentication success event
  authorization-failure         authorization failure event
  inactivity-timeout            inactivity timeout event
  session-started               session started event
  tag-added                     tag to apply event
  tag-removed                   tag to remove event
  template-activated            template activated event
  template-activation-failed    template activation failed event
  template-deactivated          template deactivated event
  template-deactivation-failed  template deactivation failed event
  timer-expiry                  timer-expiry event
  violation                     session violation event
```

イベント構成では、クラスの評価方法を定義することができます。

```
Switch(config-event-control-policymap)#event authentication-failure ?
  match-all    Evaluate all the classes
  match-first  Evaluate the first class
```

class-maps にも同様のオプションを定義することができます。ただしここでは、クラスが一致する場合のアクションの実行方法を指定します。

```
Switch(config-class-control-policymap)#10 class always ?
  do-all            Execute all the actions
  do-until-failure  Execute actions until one of them fails
  do-until-success  Execute actions until one of them is successful
```

新しいスタイルの dot1x の設定の最後の部分（オプション）は **class-map** です。これはさらに、**コントロール サブスクライバ** タイプである必要があり、特定の動作またはトラフィックと照合するために使用されます。 **class-map** 条件評価の要件を設定します。 すべての条件が一致する必要があるか、いずれかの条件が一致すればいいのか、どの条件も一致してはならないのかを指定できます。

```
Switch(config)#class-map type control subscriber ?
  match-all   TRUE if everything matches in the class-map
  match-any   TRUE if anything matches in the class-map
  match-none  TRUE if nothing matches in the class-map
```

これは、dot1x 認証の失敗を照合するために使用する **class-map** の例です。

```
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
```

一部のシナリオでは、service-template が使用されているときにはほとんどの場合に、認可変更（CoA）の設定を追加する必要があります。

```
aaa server radius dynamic-author
 client 10.48.17.232 server-key cisco
```

単一ホストのシナリオ

ネットワーク図

設定

IOS 15.2(4)E1 搭載の Catalyst 3750X でテストされた単一ホストのシナリオには、802.1X の基本構成が必要です。 シナリオは、Windows Native Supplicant および Cisco AnyConnect でテストされました。

```
aaa new-model
!
aaa group server radius tests
 server name RAD-1
!
aaa authentication dot1x default group tests
aaa authorization network default group tests
!
dot1x system-auth-control
!
policy-map type control subscriber TEST
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
!
interface GigabitEthernet1/0/21
 switchport access vlan 613
 switchport mode access
 access-session host-mode single-host
 access-session port-control auto
 dot1x pae authenticator
 service-policy type control subscriber TEST
!
radius server RAD-1
 address ipv4 10.48.17.232 auth-port 1812 acct-port 1813
 key cisco
```

マルチドメインのシナリオ

ネットワーク図

設定

マルチドメインのシナリオは、IP フォン（Cisco IP Phone 9971）の PoE（Power over Ethernet）要件に従い、IOS 03.02.03.SE の Catalyst 3850 でテストされました。

```
aaa new-model
!
aaa group server radius tests
 server name RAD-1
!
aaa authentication dot1x default group tests
aaa authorization network default group tests
!
aaa server radius dynamic-author
 client 10.48.17.232 server-key cisco
!
dot1x system-auth-control
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
policy-map type control subscriber TEST4
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
  20 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  40 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
```

```
!
interface GigabitEthernet1/0/1
 switchport access vlan 613
 switchport mode access
 switchport voice vlan 612
 access-session host-mode multi-domain
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber TEST4
!
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 vsa send cisco-nas-port
!
radius server RAD-1
 address ipv4 10.48.17.232 auth-port 1812 acct-port 1813
 key cisco
```

確認

このセクションでは、設定が正常に機能していることを確認します。

確認のため、次のコマンドを使用して、すべてのスイッチポートのセッションをリストします。

```
show access-session
```

また、単一のスイッチポートのセッションに関する詳細情報を表示することもできます。

```
show access-session interface [Gi 1/0/1] {detail}
```

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。

802.1X 関連の問題をトラブルシューティングするには、802.1X の古い構文と同じ方法でデバッグを有効にします。

```
debug mab all
debug dot1x all
debug pre all*
```

* debug pre ではオプションで、IBNS 2.0 関連情報への出力を制限するイベントやルールのみを使用できます。