為單主機和多域方案配置IBNS 2.0

目錄

簡介

本文檔介紹如何為單主機和多域方案配置基於身份的網路服務2.0(IBNS)。

必要條件

需求

思科建議您瞭解以下主題：

- 區域網路上的可擴充驗證通訊協定(EAPoL)
- Radius通訊協定
- 思科身分識別服務引擎版本2.0

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.0補丁2
- 使用Windows 7作業系統的終端
- 採用IOS 15.2(4)E1的Cisco交換器3750X
- 採用03.02.03.SE的思科交換器3850
- Cisco IP電話9971

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

組態原理

為了啟用IBNS 2.0，您需要在Cisco交換機上以特權模式執行命令：

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

使用以下命令配置IBNS 2.0的switchport:

```
 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
```

這些命令在介面上啟用dot1x身份驗證（可選）和MAC身份驗證旁路(MAB)。使用新語法時，會使用以access-session開頭的命令。這些命令的用途與使用舊語法的命令（以身份驗證關鍵字開頭）的用途相同。應用service-policy以指定可用於介面的策略對映。

所述的策略對映定義身份驗證期間交換機（身份驗證器）的行為。例如，您可以指定身份驗證失敗時會發生的情況。對於每個事件，您可以根據在其下配置的類對映中匹配的事件型別配置多個操作。例如，檢視所示的清單(policy-map TEST4)。如果連線到應用此策略的介面的dot1x端點失敗，則會執行DOT1X_FAILED中定義的操作。如果要為MAB_FAILED和DOT1X_FAILED等類指定相同的行為，則可以使用預設類 — class-map always。

```
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
(...)
```

用於IBNS 2.0的策略對映必須始終具有型別控制使用者。

您可以按以下方式檢視可用事件的清單：

```
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
```

在事件配置中，您可以定義如何評估類：

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

您可以為類對映定義類似的選項，但在此處指定如何在類匹配的情況下執行操作：

```
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
```

新樣式dot1x中配置的最後部分（可選）是類對映。 它還可以鍵入控制使用者，用於匹配特定行為或流量。配置類對映條件評估的要求。您可以指定必須匹配所有條件，或者必須匹配任何條件，或者不匹配任何條件。

```
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
```

以下是用於匹配dot1x身份驗證失敗的類對映示例：

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

對於某些情況（大多數情況下，當使用服務模板時），您需要為授權更改(CoA)新增配置：

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

單主機方案

網路圖表

組態

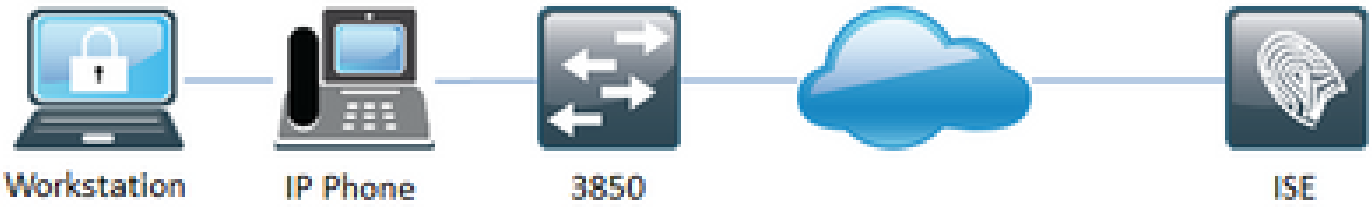
在採用IOS 15.2(4)E1的Catalyst 3750X上測試的單主機方案所需的基本802.1X配置。使用Windows Native Supplicant客戶端和Cisco AnyConnect測試的方案。

```
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
```

多域方案

網路圖表



組態

多域方案在採用IOS 03.02.03.SE的Catalyst 3850上進行了測試，原因是IP電話（Cisco IP電話9971）的PoE（乙太網供電）要求。

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

出於驗證目的，使用以下命令列出所有交換器連線埠的作業階段：

```
show access-session
```

您還可以從單個交換機埠檢視有關會話的詳細資訊：

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

若要疑難排解802.1X相關問題，可以採用與舊式802.1X語法相同的方式啟用偵錯：

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

*對於debug pre（可選），您只能使用事件和/或規則將輸出限製為IBNS 2.0相關資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。