配置单个主机和多域方案的IBNS 2.0

目录

简介

本文描述如何配置标识单个主机和多域方案的基于网络服务2.0 (IBNS)。

先决条件

要求

Cisco 建议您了解以下主题：

- 在局域网(EAPoL)的可扩展的认证协议
- RADIUS协议
- 思科身份服务引擎版本2.0

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco身份服务引擎版本2.0补丁程序2
- 与Windows 7 OS的终端
- 有IOS的15.2(4)E1 Cisco交换机3750X
- 有03.02.03.SE的Cisco交换机3850
- Cisco IP电话9971

本文档中的信息从在特定实验室环境的设备创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

配置理论

为了启用IBNS 2.0，您需要执行在您的Cisco交换机的in命令特权模式：

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

配置IBNS的2.0 switchport用命令如显示：

```
 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
```

这些enable命令dot1x验证和或者MAC验证旁路(MAB)在接口。当您跟随新的语法时，从访问会话开始的您使用命令。那些命令目的同一样为使用旧语法的命令(开始与**验证**关键字)。运用**服务策略**指定应该使用接口的**策略映射**。

以上提到的**策略映射**在验证时定义了交换机(验证器)的行为。例如，您能指定什么应该在认证失败的情况下发生。对于每个**事件**您能配置根据在**类映射**匹配的事件的种类的多样行动配置在它下。为例，请看一看在列表如显示(**策略映射测试4**)。如果连接对接口此策略应用的dot1x终端发生故障，则在**DOT1X_FAILED**定义的操作被执行。如果希望指定类的同一种行为类似**MAB_FAILED**和**DOT1X_FAILED**，则您能**总是**使用默认组-**类映射。**

```
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
(...)
```

用于IBNS的**策略映射**2.0必须总是有类型**控制用户。**

您能这样查看可用的事件列表：

```
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
```

在事件配置中您有定义的可能性如何应该评估类：

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

您能定义**类映射的**相似的选项，虽然此处您指定如何应该执行操作，万一您的类匹配：

```
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
```

最后一部分(可选)在新式的配置dot1x是**类映射**。它应该也键入**控制用户**，并且用于匹配特定行为或流量。配置**类映射**情况评估的需求。您能指定所有情况必须匹配或所有情况必须匹配或条件都不应该配比。

```
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
```

这是匹配dot1x认证失败使用的**类映射**示例：

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

对于一些方案，主要，当服务模板是在使用中的时，您需要授权(CoA)的崔凡吉莱的添加配置：

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

单个主机的方案

网络图

配置

为单个主机方案要求的基本802.1X配置测试在有IOS的15.2(4)E1 Catalyst 3750X。用Windows本地请求方和思科测试的方案AnyConnect。

```
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
```

多域的方案

网络图

配置

多域方案在有IOS的03.02.03.SE Catalyst 3850测试了由于IP电话的(Cisoc IP电话9971)柏吾(在以太网的电源)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
```

验证

使用本部分可确认配置能否正常运行。

验证目的，请使用这些命令列出从所有连接孔的会话：

```
show access-session
```

您能也查看关于会话的详细信息从单个switchport ：

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

故障排除

本部分提供了可用于对配置进行故障排除的信息。

为了排除故障802.1X相关问题，您能关闭调试方式和一样老式802.1X语法的：

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

* optionaly为调试前您能使用仅事件并且/或者规定对IBNS 2.0相关信息限制输出。