Настройте IBNS 2.0 для одного хоста и мультидоменных сценариев

Содержание

Введение

Этот документ описывает, как настроить Идентичность Базирующиеся Сетевые сервисы 2.0 (IBNS) для одного хоста и мультидоменных сценариев.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Расширяемый протокол аутентификации по локальной сети (EAPOL)
- Протокол RADIUS
- Версия 2.0 Платформы Cisco Identity Services Engine

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Идентификационное исправление 2 версии 2.0 Механизма Сервиса Cisco
- Оконечная точка с Windows 7 OS
- Коммутатор Cisco 3750X с IOS 15.2 (4) E1
- Коммутатор Cisco 3850 с 02.03.03. SE

- Cisco IP Phone 9971

Сведения в этом документе созданы от устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Настройка

Теория конфигурации

Для включения IBNS 2.0 необходимо выполнить команду в привилегированном режиме на коммутаторе Cisco:

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

Настройте порт коммутатора для IBNS 2.0 с командами как показано:

```
 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
```

Эти команды включают аутентификацию dot1x и дополнительно Обход проверки подлинности MAC (MAB) на интерфейсе. Когда вы придерживаетесь нового синтаксиса, вы используете команды, который запускается с сеанса доступа. Цель тех команд - то же что касается команд, которые используют старый синтаксис (начиная с **опознавательного** ключевого слова). Примените **стратегию обслуживания** для определения **policy-map**, который должен использоваться для интерфейса.

Упомянутый выше **policy-map** определяет поведение коммутатора (средство проверки подлинности) во время аутентификации. Например, можно задать то, что должно произойти в случае ошибки проверки подлинности. Для каждого **события** можно настроить множественные действия на основе типа события, с которым совпадают в **class-map**, настроенном под ним. Как пример, смотрите на список как показано **(policy-map TEST4)**. Если оконечная точка dot1x, которая связана с интерфейсом, где эта политика применена сбои, то действие, определенное в **DOT1X_FAILED**, выполняется. Если требуется задать то же поведение для классов как **MAB_FAILED** и **DOT1X_FAILED**, то можно использовать класс по умолчанию - **class-map всегда.**

```
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
(...)
```

Policy-map, используемый для IBNS 2.0 всегда, должен иметь **абонента контроля** за типом.

Можно просмотреть список доступных событий таким образом:

```
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
```

В конфигурации событий у вас есть возможность определить, как должны быть оценены классы:

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

Можно определить подобную опцию для **карт классов**, невзирая на то, что здесь вы задаете, как действия должны быть выполнены в случае, если совпадают с вашим классом:

```
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
```

Последняя часть (дополнительная) из конфигурации в новом стиле dot1x, является **class-map**. Это также должно ввести **абонента контроля**, и это используется для соответствия с определенным поведением или трафиком. Настройте требования для оценки условия **class-map**. Можно указать, что со всеми условиями нужно совпасть, или с любым условием нужно совпасть, или ни одно из условий не должно совпадать.

```
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
```

Это - пример **class-map**, используемого для соответствующей ошибки проверки подлинности dot1x:

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

Для некоторых сценариев, главным образом когда сервисный шаблон используются, необходимо добавить конфигурацию для изменения авторизации (CoA):

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

Сценарий для одного хоста

Схема сети

Конфигурации

Основная конфигурация 802.1X, требуемая для сценария одного хоста, протестированного на Catalyst 3750X с IOS 15.2 (4) E1. Сценарий, протестированный с Windows Native Supplicant и AnyConnect Cisco.

```
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
```

Сценарий для мультидоменного

Схема сети

Конфигурации

Мультидоменный сценарий был протестирован на Catalyst 3850 с IOS 02.03.03. SE из-за PoE (Питание над Ethernet) требования для IP-телефона (IP-телефон Cisoc 9971).

```
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
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

В целях проверки используйте их команда для распечатки сеансов от всего switchports:

```
show access-session
```

Можно также просмотреть подробные сведения о сеансах от одиночного порта коммутатора:

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

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Для устранения проблем связанных проблем 802.1X можно включить отладкам тот же путь что касается синтаксиса 802.1X старого стиля:

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

* дополнительно для отладки пред вы может использовать только событие и/или правило ограничить выходные данные связанными сведениями IBNS 2.0.