Configuración IBNS 2.0 para los escenarios del solo host y del Multi-dominio

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Configurar](#)
[Teoría de la configuración](#)
[Escenario para el solo host](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Escenario para el Multi-dominio](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Verificación](#)
[Troubleshooting](#)

Introducción

Este documento describe cómo configurar los servicios de red basados identidad 2.0 (IBNS) para los escenarios del solo host y del multi-dominio.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo extensible authentication sobre la red de área local (EAPoL)
- Protocolo RADIUS
- Versión 2.0 del Cisco Identity Services Engine

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Corrección 2 de la versión 2.0 del motor del servicio de la identidad de Cisco
- Punto final con Windows 7 OS
- Switch Cisco 3750X con IOS 15.2(4)E1
- Switch Cisco 3850 con 03.02.03.SE

- Cisco IP Phone 9971

La información en este documento se crea de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Teoría de la configuración

Para habilitar IBNS 2.0, usted necesita ejecutar el comando en el modo del privilegio en su switch Cisco:

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

Configure el switchport para IBNS 2.0 con los comandos como se muestra:

```
 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
```

Puente de la autenticación y opcionalmente de la autenticación de MAC del dot1x de estos comandos enable (MAB) en la interfaz. Cuando usted sigue la sintaxis nueva, usted utiliza los comandos que comienza con la acceso-sesión. El propósito de esos comandos es lo mismo que para los comandos que utilizan la sintaxis antigua (que comienza con la palabra clave de la **autenticación**). Aplique la servicio-**directiva** para especificar el directiva-**mapa** que se debe utilizar para la interfaz.

El directiva-mapa mencionado anteriormente define el comportamiento del Switch (authenticator) durante la autenticación. Por ejemplo, usted puede especificar qué debe suceder en caso de la falla de autenticación. Para cada **evento** usted puede configurar las acciones múltiples basadas en el tipo del evento correspondido con en el clase-**mapa** configurado bajo él. Como un ejemplo, heche una ojeada la lista como se muestra (directiva-**mapa TEST4**). Si el punto final del dot1x que está conectado con la interfaz donde está aplicada esta directiva falla, después la acción definida en **DOT1X_FAILED** se ejecuta. Si usted quisiera especificar el mismo comportamiento para las clases como **MAB_FAILED** y **DOT1X_FAILED**, después usted puede utilizar la clase predeterminada - clase-**mapa siempre.**

```
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
(...)
```

el Directiva-mapa usado para IBNS 2.0 siempre debe tener el **suscriptor del control del** tipo.

Usted puede ver la lista de eventos disponibles de esta manera:

```
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
```

En configuración de evento usted tiene posibilidad para definir cómo las clases deben ser evaluadas:

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

Usted puede definir la opción similar para **class-maps**, aunque aquí usted especifique cómo las acciones deben ser ejecutadas en caso de que se corresponda con su clase:

```
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
```

La parte más reciente (opcional) de la configuración en el nuevo estilo del dot1x es clase-**mapa**. También debe teclear al **suscriptor del control** y se utiliza para hacer juego el comportamiento o el tráfico específico. Los requisitos de la configuración para el clase-**mapa** condicionan la evaluación. Usted puede especificar que todas las condiciones tienen que ser correspondidas con o cualquier condición tiene que ser correspondida con o ningunas de las condiciones deben hacer juego.

```
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
```

Éste es ejemplo del clase-**mapa** usado para corresponder con la falla de autenticación del dot1x:

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

Para algunos escenarios, sobre todo cuando la servicio-plantilla es funcionando, usted necesita agregar la configuración para el cambio de la autorización (CoA):

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

Escenario para el solo host

Diagrama de la red

Configuraciones

Configuración básica del 802.1x requerida para el escenario del solo host probado en el Catalyst 3750X con IOS 15.2(4)E1. Escenario probado con el supplicant nativo y Cisco AnyConnect de Windows.

```
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
```

Escenario para el Multi-dominio

Diagrama de la red

Configuraciones

el escenario del Multi-dominio fue probado en el Catalyst 3850 con IOS 03.02.03.SE debido a los requisitos del PoE (poder sobre los Ethernetes) para el teléfono del IP (teléfono del IP 9971 de Cisoc).

```
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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para comprobar, utilice éstos ordenan para enumerar las sesiones de todos los switchports:

```
show access-session
```

Usted puede también ver la información detallada sobre las sesiones de un solo switchport:

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

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Para resolver problemas los asuntos relacionados del 802.1x, usted puede habilitar hace el debug de la misma manera que para el sintaxis del 802.1x del Estilo anterior:

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

* optionaly para el debug pre usted puede utilizar solamente el evento y/o la regla para limitar la salida a la información pertinente IBNS 2.0.