Configurar o IBNS 2.0 para cenários de host único e de vários domínios

Contents

Introdução

Este documento descreve como configurar o Identity Based Networking Services 2.0 (IBNS) para cenários de host único e de vários domínios.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo de autenticação extensível sobre rede local (EAPoL)
- protocolo Radius
- Cisco Identity Services Engine versão 2.0

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Service Engine versão 2.0 patch 2
- Endpoint com SO Windows 7
- Switch Cisco 3750X com IOS 15.2(4)E1
- Switch Cisco 3850 com 03.02.03.SE
- Telefone IP 9971 da Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Teoria da configuração

Para habilitar o IBNS 2.0, você precisa executar o comando no modo privilegiado no switch Cisco:

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

Configure a porta do switch para o IBNS 2.0 com comandos como mostrado:

```
 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
```

Esses comandos permitem a autenticação dot1x e, opcionalmente, o MAC Authentication Bypass (MAB) na interface. Ao usar a nova sintaxe, você usa comandos que começam com access-session. A finalidade desses comandos é a mesma dos comandos que usam sintaxe antiga (começando com a palavra-chave authentication). Aplique service-policy para especificar o mapa de políticas que pode ser usado para a interface.

O mapa de políticas mencionado define o comportamento do switch (autenticador) durante a autenticação. Por exemplo, você pode especificar o que pode acontecer em caso de falha de autenticação. Para cada evento, você pode configurar várias ações com base no tipo de evento correspondente no mapa de classe configurado nele. Por exemplo, observe a lista como mostrado (policy-map TEST4). Se o ponto final dot1x, que está conectado à interface onde esta política é aplicada falhar, a ação definida em DOT1X_FAILED será executada. Se você quiser especificar o mesmo comportamento para classes como MAB_FAILED e DOT1X_FAILED, poderá usar class-map default sempre.

```
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
(...)
```

O mapa de políticas usado para IBNS 2.0 sempre deve ter assinante de controle de tipo.

Você pode exibir a lista de eventos disponíveis desta maneira:

```
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
```

Na configuração do evento, você tem a possibilidade de definir como as classes podem ser avaliadas:

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

Você pode definir opções semelhantes para mapas de classe, embora aqui você especifique como as ações podem ser executadas caso sua classe seja correspondida:

```
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
```

A última parte (opcional) da configuração no novo estilo de dot1x é class-map. Ele também pode digitar o assinante de controle e é usado para corresponder ao comportamento ou tráfego específico. Configure os requisitos para a avaliação da condição de mapa de classe. Você pode especificar que todas as condições devem ser correspondidas, que qualquer condição deve ser correspondida ou que nenhuma das condições corresponde.

```
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
```

Este é um exemplo de mapa de classe usado para correspondência de falha de autenticação dot1x:

```
class-map type control subscriber match-all DOT1X_FAILED
```

```
 match method dot1x
 match result-type method dot1x authoritative
```

Para alguns cenários, principalmente quando o modelo de serviço está em uso, você precisa adicionar a configuração para a alteração de autorização (CoA):

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

Cenário para Host Único

Diagrama de Rede

Configurações

Configuração 802.1X básica necessária para o cenário de host único testado no Catalyst 3750X com IOS 15.2(4)E1. Cenário testado com o Windows Native Supplicant e o Cisco 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
```

Cenário para vários domínios

Diagrama de Rede

Configurações

O cenário de vários domínios foi testado no Catalyst 3850 com IOS 03.02.03.SE devido aos requisitos de PoE (Power over Ethernet) para telefone IP (Cisco IP Phone 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para fins de verificação, use este comando para listar sessões de todas as portas de switch:

```
show access-session
```

Você também pode exibir informações detalhadas sobre sessões de uma única porta de switch:

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

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para solucionar problemas relacionados ao 802.1X, você pode habilitar depurações da mesma forma que para a sintaxe 802.1X de estilo antigo:

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

* opcionalmente para depurar antes, você pode usar somente eventos e/ou regras para limitar a saída a informações relevantes do IBNS 2.0.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.