IBNS 2.0 configureren voor scenarioâ€™s met één host en meerdere domeinen

Inhoud

Inleiding

In dit document wordt beschreven hoe u op identiteit gebaseerde netwerkservices 2.0 (IBNS) kunt configureren voor scenario's met één host en meerdere domeinen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Uitbreidbaar verificatieprotocol via Local Area Network (EAPoL)
- Radius-protocol
- Cisco Identity Services Engine versie 2.0

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Service Engine versie 2.0, patch 2
- Endpoint met Windows 7 OS
- Cisco switch 3750X met IOS 15.2(4)E1
- Cisco switch 3850 met 03.02.03.SE
- Cisco IP-telefoon 9971

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Configuratietheorie

Om IBNS 2.0 in te schakelen, moet u de opdracht in de voorkeursmodus op uw Cisco-switch uitvoeren:

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

Configureer switchport voor IBNS 2.0 met opdrachten zoals getoond:

```
 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
```

Deze opdrachten maken dot1x-verificatie en optioneel MAC-verificatie-omleiding (MAB) op de interface mogelijk. Wanneer u de nieuwe syntaxis gebruikt, gebruikt u opdrachten die met toegangssessies beginnen. Het doel van deze opdrachten is hetzelfde als voor opdrachten met een oude syntaxis (te beginnen met verificatiesleutel). Pas dienst-beleid toe om beleid-kaart te specificeren die voor de interface kan worden gebruikt.

De genoemde policy-map definieert het gedrag van de switch (authenticator) tijdens de authenticatie. U kunt bijvoorbeeld instellen wat er kan gebeuren bij een verificatiefout. Voor elke gebeurtenis kunt u meerdere acties configureren op basis van het type van de gebeurtenis die is gekoppeld in de klasse-map die onder de gebeurtenis is geconfigureerd. Neem als voorbeeld een kijkje in de lijst zoals getoond (policy-map TEST4). Als dot1x endpoint, dat is verbonden met de interface waar dit beleid wordt toegepast, mislukt, wordt de actie die is gedefinieerd in DOT1X_FAILLIET uitgevoerd. Als u hetzelfde gedrag wilt opgeven voor klassen als MAB_MISLUKT en DOT1X_MISLUKTE, dan kunt u de standaardklasse - class-map altijd gebruiken.

```
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
(...)
```

Voor IBNS 2.0 gebruikte policy-map moet altijd een type control-abonnee hebben.

U kunt de lijst van beschikbare evenementen op deze manier bekijken:

```
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
```

In geval van configuratie, hebt u de mogelijkheid om te definiëren hoe klassen kunnen worden geëvalueerd:

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

U kunt soortgelijke opties voor class-maps definiëren, hoewel u hier specificeert hoe acties kunnen worden uitgevoerd als uw klasse wordt aangepast:

```
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
```

Het laatste (facultatieve) deel van configuratie in nieuwe stijl van dot1x is klasse-kaart. Het kan ook controle abonnee typen, en het wordt gebruikt om specifiek gedrag of verkeer aan te passen. Configureer de eisen voor de evaluatie van de klassekaartvoorwaarde. U kunt specificeren dat alle voorwaarden moeten worden aangepast, of om het even welke voorwaarde moet worden aangepast, of geen van de voorwaarden past aan.

```
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
```

Dit is een voorbeeld van class-map dat wordt gebruikt voor het matchen van dot1x-verificatiefout:

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

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

Voor sommige scenario's, meestal wanneer de dienst-malplaatje in gebruik is, moet u configuratie voor Verandering van Vergunning (CoA) toevoegen:

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

Scenario voor single-host

Netwerkdiagram

Configuraties

Basis 802.1X-configuratie vereist voor single-host scenario getest op Catalyst 3750X met IOS 15.2(4)E1. Scenario getest met Windows Native Supplicant en 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
```

Scenario voor multi-domein

Netwerkdiagram

Configuraties

Het scenario voor meerdere domeinen is getest op Catalyst 3850 met IOS 30.02.03.SE vanwege PoE (Power over Ethernet)-vereisten voor IP-telefoon (Cisco IP-telefoon 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
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Gebruik voor verificatiedoeleinden deze opdracht om sessies van alle switchports weer te geven:

```
show access-session
```

U kunt ook gedetailleerde informatie over sessies bekijken vanaf één switchpoort:

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

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Om problemen met 802.1X op te lossen, kunt u debugs op dezelfde manier inschakelen als voor de oude stijl 802.1X syntaxis:

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

* optioneel voor debug voordat u alleen gebeurtenis en/of regel kunt gebruiken om uitvoer te beperken tot relevante informatie over IBNS 2.0.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.