Configurazione di IBNS 2.0 per scenari a host singolo e a più domini

Sommario

Introduzione

In questo documento viene descritto come configurare Identity Based Networking Services 2.0 (IBNS) per scenari a host singolo e a più domini.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Extensible Authentication Protocol over Local Area Network (EAPoL)
- Protocollo Radius
- Cisco Identity Services Engine versione 2.0

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Patch 2 di Cisco Identity Service Engine versione 2.0
- Endpoint con Windows 7
- Switch Cisco 3750X con IOS 15.2(4)E1
- Cisco switch 3850 con 03.02.03.SE
- Cisco IP Phone 9971

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Teoria di configurazione

Per abilitare IBNS 2.0, è necessario eseguire il comando in modalità di esecuzione privilegiata sullo switch Cisco:

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

Configurare switchport per IBNS 2.0 con i comandi come mostrato:

```
 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
```

Questi comandi abilitano l'autenticazione dot1x e, facoltativamente, MAC Authentication Bypass (MAB) sull'interfaccia. Quando si utilizza la nuova sintassi, si utilizzano comandi che iniziano con access-session. Lo scopo di questi comandi è lo stesso dei comandi che utilizzano la sintassi precedente, a partire dalla parola chiave authentication. Applicare i criteri del servizio per specificare la mappa dei criteri che può essere utilizzata per l'interfaccia.

Il mapping dei criteri indicato definisce il comportamento dello switch (autenticatore) durante l'autenticazione. Ad esempio, è possibile specificare l'azione da eseguire in caso di errore di autenticazione. Per ogni evento è possibile configurare più azioni in base al tipo di evento corrispondente nella mappa classi configurata in base a esso. Ad esempio, osservare l'elenco come mostrato (policy-map TEST4). Se l'endpoint dot1x, connesso all'interfaccia a cui viene applicato il criterio, ha esito negativo, viene eseguita l'azione definita in DOT1X_FAILED. Se si desidera specificare lo stesso comportamento per classi quali MAB_FAILED e DOT1X_FAILED, è sempre possibile utilizzare la classe predefinita - mappa classe.

```
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
(...)
```

La mappa dei criteri utilizzata per IBNS 2.0 deve sempre avere un sottoscrittore di controllo del tipo.

È possibile visualizzare l'elenco degli eventi disponibili nel modo seguente:

```
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
```

Nella configurazione degli eventi è possibile definire la modalità di valutazione delle classi:

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

È possibile definire opzioni simili per le mappe di classe, anche se qui si specifica come eseguire le azioni in caso di corrispondenza della classe:

```
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
```

L'ultima parte (facoltativa) della configurazione nel nuovo stile di dot1x è class-map. Può inoltre digitare control subscriber e viene utilizzato per corrispondere a un comportamento o a un traffico specifico. Configurare i requisiti per la valutazione della condizione della mappa delle classi. È possibile specificare che devono essere soddisfatte tutte le condizioni, che devono essere soddisfatte tutte le condizioni o nessuna di esse.

```
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
```

Questo è un esempio di mappa di classe utilizzata per la corrispondenza dell'errore di autenticazione dot1x:

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

In alcuni scenari, soprattutto quando il modello di servizio è in uso, è necessario aggiungere la configurazione per la modifica dell'autorizzazione (CoA):

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

Scenario per host singolo

Esempio di rete

Configurazioni

Configurazione di base 802.1X richiesta per uno scenario a host singolo testato su Catalyst 3750X con IOS 15.2(4)E1. Scenario testato con Windows Native Supplicant e 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 per multidominio

Esempio di rete

Configurazioni

Lo scenario a più domini è stato testato su Catalyst 3850 con IOS 03.02.03.SE a causa dei requisiti PoE (Power over Ethernet) per IP Phone (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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

A scopo di verifica, usare questo comando per elencare le sessioni da tutte le porte switch:

```
show access-session
```

È inoltre possibile visualizzare informazioni dettagliate sulle sessioni da una singola porta switch:

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per risolvere i problemi relativi a 802.1X, è possibile abilitare i debug allo stesso modo della sintassi 802.1X precedente:

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

* se si desidera eseguire il debug pre, è possibile utilizzare solo l'evento e/o la regola per limitare l'output alle informazioni rilevanti di IBNS 2.0.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).