تكوين IBNS 2.0 لسيناريوهات المضيف الواحد والمجال المتعدد

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين خدمات الشبكة المستندة إلى الهوية 2.0 (IBNS) لسيناريوهات المضيف الواحد والمجال المتعدد.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بروتوكول المصادقة الموسع عبر شبكة المنطقة المحلية (EAPoL)
- بروتوكول RADIUS
- Cisco Identity Services Engine، الإصدار 2.0

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Identity Service Engine، الإصدار 2.0 Patch 2
- نقطة النهاية بنظام التشغيل Windows 7
- المحول Cisco Switch 3750X مع IOS 15.2(4)E1
- المحول Cisco 3850 مع 03.02.03.SE

- هاتف بروتوكول الإنترنت Cisco IP Phone 9971

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

نظرية التكوين

in order to تمكن IBNS 2.0، أنت تحتاج أن ينفذ الأمر في امتياز أسلوب على cisco مفتاح:

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

قم بتكوين switchport ل IBNS 2.0 باستخدام الأوامر كما هو موضح:

```
 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
```

تمكن هذه الأوامر مصادقة dot1x، واختياريا، تجاوز مصادقة MAC (MAB) على الواجهة. عندما تستخدم الصياغة الجديدة، فإنك تستخدم الأوامر التي تبدأ مع Access-session. الغرض من هذه الأوامر هو نفسه كما هو الحال بالنسبة للأوامر التي تستخدم الصياغة القديمة (بدء المصادقة بالكلمة الأساسية للمصادقة). تطبق سياسة الخدمة لتحديد خريطة السياسة التي يمكن إستخدامها للواجهة.

تحدد خريطة السياسة المذكورة سلوك المحول (المصدق) أثناء المصادقة. على سبيل المثال، يمكنك تحديد ما يمكن أن يحدث في حالة فشل المصادقة. لكل حدث يمكنك تكوين إجراءات متعددة استنادا إلى نوع الحدث المتطابق في خريطة الفئة التي تم تكوينها تحته. وكمثال على ذلك، ألق نظرة على القائمة كما هو موضح (Policy-map TEST4). في حالة فشل نقطة نهاية dot1x، المتصلة بالقارن حيث يتم تطبيق هذا النهج، يتم تنفيذ الإجراء المعرف في DOT1X_FAILED. إذا كنت ترغب في تحديد نفس السلوك للفئات مثل MAB_FAILED و DOT1X_FAILED، فيمكنك إستخدام الفئة الافتراضية - خريطة الفئة دائما.

```
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
(...)
```

يجب أن يحتوي مخطط السياسة المستخدم ل IBNS 2.0 دائما على مشترك التحكم في النوع.

يمكنك عرض قائمة الأحداث المتاحة بهذه الطريقة:

```
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
```

في تكوين الحدث، لديك إمكانية تحديد كيفية تقييم الفئات:

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

يمكنك تعريف خيارات مماثلة لخرائط الفئة، رغم عن أنك هنا تعين كيفية تنفيذ العمليات في حالة مطابقة الفئة الخاصة بك:

```
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
```

الجزء الأخير (إختياري) من التكوين في النمط الجديد dot1x هو خريطة الفئة. كما يمكنه تكوين مشترك التحكم، وتم إستخدامه لمطابقة سلوك أو حركة مرور معينة. تكوين كتابة متطلبات تقييم حالة خريطة الفئة. يمكنك تعيين أن كل الشروط يجب أن تتطابق، أو أي

شرط يجب أن يتطابق، أو ال أحد من الشروط تتطابق.

```
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
```

هذا مثال على خريطة الفئة المستخدمة في مطابقة فشل مصادقة dot1x:

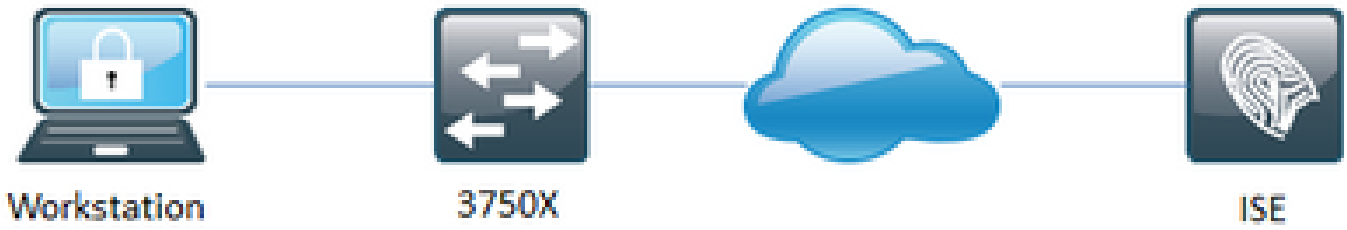
```
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
```

بالنسبة لبعض السيناريوهات، غالبا عند إستخدام قالب الخدمة، تحتاج إلى إضافة تكوين لتغيير التفويض (CoA):

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

سيناريو للمضيف الواحد

الرسم التخطيطي للشبكة



التكوينات

يلزم تكوين أساسي بسرعة 802. 1X لسيناريو المضيف الواحد الذي تم إختباره على المحول Catalyst 3750X مع IOS 15. 2(4)E1. تم إختبار السيناريو باستخدام برنامج Windows Native Plus و 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
```

سيناريو المجالات المتعددة

الرسم التخطيطي للشبكة

التكوينات

تم إختبار سيناريو متعدد المجالات على Catalyst 3850 باستخدام IOS 03.02.03.SE بسبب متطلبات التزويد بالطاقة عبر شبكة إيثرنت (PoE) لهاتف بروتوكول الإنترنت (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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

لأغراض التحقق، أستخدم هذا الأمر لسرد جلسات العمل من جميع المحولات:

```
show access-session
```

أنت يستطيع أيضا شاهدت معلومات تفصيلية حول جلسة من وحيد switchport:

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

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

لاستكشاف أخطاء 802.1X المتعلقة وإصلاحها، يمكنك تمكين تصحيح الأخطاء بنفس الطريقة كما هو الحال بالنسبة لصيغة النمط القديم 802.1X:

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

* إختياريا لتصحيح الأخطاء مسبقا، يمكنك إستخدام الحدث و/أو القاعدة فقط للحد من الإخراج على المعلومات ذات الصلة ب IBNS 2.0.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).