Cryptage de Commutateur-hôte de MACsec avec l'exemple de Cisco AnyConnect et de configuration ISE

ID de document : 117277

Mis à jour : Janv. 31, 2014

Contribué par Michal Garcarz et Machulik romain, ingénieurs TAC Cisco.

Produits connexes

- Sécurité
- 802.1x
- Logiciel Cisco Identity Services Engine

Contenu

Introduction

Ce document fournit un exemple de configuration pour le cryptage de degré de sécurité de Media Access Control (MACsec) entre un suppliant de 802.1x (Mobile Security de Cisco AnyConnect) et un authentificateur (commutateur). Les Logiciels Cisco Identity Services Engine (ISE) est utilisés comme authentification et policy server.

MACsec est normalisé dans 802.1AE et pris en charge sur Cisco 3750X, 3560X, et 4500 Commutateurs SUP7E. 802.1AE définit le chiffrement de voie au-dessus des réseaux câblés qui utilisent des clés hors bande. Ces clés de chiffrement sont étées en pourparlers avec le protocole de l'accord de clé de MACsec (MKA) qui est utilisé après l'authentification réussie de 802.1x. MKA est normalisé dans IEEE 802.1X-2010.

Un paquet est chiffré seulement sur le lien entre le PC et le commutateur (cryptage point par point). Le paquet reçu par le commutateur est déchiffré et envoyé par l'intermédiaire des liaisons ascendantes décryptées. Afin de chiffrer la transmission entre les Commutateurs, le cryptage de commutateur-commutateur est recommandé. Pour ce cryptage, l'association de sécurité Protocol (SAP) est utilisée pour négocier et régénérer des clés. SAP est un protocole d'accord de clé de prénorme développé par Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de configuration de 802.1x
- Connaissance de base de configuration CLI des Commutateurs de Catalyst
- Expérience avec la configuration ISE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Systèmes d'exploitation de Microsoft Windows 7 et de Microsoft Windows XP
- Logiciel de Cisco 3750X, version 15.0 et ultérieures
- Logiciel de Cisco ISE, version 1.1.4 et ultérieures
- Sécurité mobile de Cisco AnyConnect avec l'Access Manager de réseau (NAM), version 3.1 et ultérieures

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Schéma de réseau et circulation

Étape 1. Le suppliant (AnyConnect NAM) commence la session de 802.1x. Le commutateur est l'authentificateur et l'ISE est le serveur d'authentification. Extensible Authentication Protocol au-dessus de protocole du RÉSEAU LOCAL (EAPOL) est utilisé comme transport pour l'EAP entre le suppliant et le commutateur. Le RAYON est utilisé comme protocole de transport pour l'EAP entre le commutateur et l'ISE. La dérivation d'authentification MAC (MAB) ne peut pas être utilisée, parce que des clés EAPOL doivent être retournées d'ISE et être utilisées pour la session de l'accord de clé de MACsec (MKA).

Étape 2. Après que la session de 802.1x soit complète, le commutateur initie une session MKA avec EAPOL comme protocole de transport. Si le suppliant est configuré correctement, les clés pour le cryptage symétrique 128-bit AES-GCM (Galois/mode de compteur) s'assortissent.

Étape 3. Tous les paquets suivants entre le suppliant et le commutateur sont chiffrés (encapsulation 802.1AE).

Configurations

ISE

La configuration ISE implique un scénario typique de 802.1x à une exception au profil d'autorisation qui pourrait inclure des stratégies de chiffrement.

Choisissez la **gestion > les ressources de réseau > les périphériques de réseau** afin d'ajouter le commutateur comme périphérique de réseau. Introduisez une clé pré-partagée de RAYON (secret partagé).

La règle d'authentification par défaut peut être utilisée (pour des utilisateurs définis localement sur ISE).

Choisissez la **gestion > la Gestion de l'identité > les utilisateurs** afin de définir l'utilisateur « Cisco » localement.

Le profil d'autorisation pourrait inclure des stratégies de chiffrement. Suivant les indications de cet exemple, choisissez la **stratégie > les résultats > l'autorisation profile** afin de visualiser les retours de l'information ISE au commutateur que le chiffrement de voie est obligatoire. En outre, le VLAN le numéro (10) a été configuré.

Choisissez la **stratégie > l'autorisation** afin d'utiliser le profil d'autorisation dans la règle d'autorisation. Cet exemple renvoie le profil configuré pour l'utilisateur « Cisco ». Si le 802.1x est réussi, les retours ISE Rayon-reçoivent au commutateur avec le linksec-policy=must-secure de Cisco AVPair. Cet attribut force le commutateur pour initier une session MKA. Si cette session échoue, l'autorisation de 802.1x sur le commutateur échoue également.

Commutateur

Les configurations typiques de port de 802.1x incluent (partie supérieure affichée) :

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius

aaa group server radius ISE
 server name ISE

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order dot1x
 authentication port-control auto
 dot1x pae authenticator

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 timeout 5
 retransmit 2
key cisco
```

La stratégie des gens du pays MKA est créée et appliquée à l'interface. En outre, MACsec est activé sur l'interface.

```
mka policy mka-policy
 replay-protection window-size 5000

interface GigabitEthernet1/0/2
 macsec
 mka policy mka-policy
```

La stratégie des gens du pays MKA te permet pour configurer les paramètres détaillés qui ne peuvent pas être poussés de l'ISE. La stratégie des gens du pays MKA est facultative.

AnyConnect NAM

Le profil pour le suppliant de 802.1x peut être configuré manuellement ou poussé par l'intermédiaire de Cisco ASA. Les étapes suivantes présentent une configuration manuelle.

Afin de gérer des profils NAM :

Ajoutez un nouveau profil de 802.1x avec MACsec. Pour le 802.1x, le Protected Extensible Authentication Protocol (PEAP) est utilisé (utilisateur configuré « Cisco » sur ISE) :

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'AnyConnect NAM configuré pour EAP-PEAP exige les qualifications correctes.

La session sur le commutateur devrait être authentifiée et autorisée. L'état de Sécurité devrait

« être sécurisé » :

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Secured
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D56FD55B3BF
     Acct Session ID:  0x00011CB4
              Handle:  0x97000D57

Runnable methods list:
      Method   State
       dot1x    Authc Success
```

Les statistiques de MACsec sur le commutateur fournissent les détails en vue de le paramètre de la stratégie local, les identifiants de canal de sécuriser (SCI) pour trafic reçu/envoyé, et mettent en communication également des statistiques et des erreurs.

```
bsns-3750-5#show macsec interface g1/0/2
 MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
  Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
  SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 76         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 2441
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
```

```
  Notusing pkts 0              Decrypt bytes 176153
  Ingress miss pkts 2437
```

Sur AnyConnect, les statistiques indiquent l'utilisation de cryptage et les statistiques de paquet.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Debugs pour un scénario fonctionnant

L'enable met au point sur le commutateur (une certaine sortie a été omise pour la clarté).

```
bsns-3750-5#show macsec interface g1/0/2
 MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
  Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
  SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 76         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 2441
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
  Notusing pkts 0              Decrypt bytes 176153
  Ingress miss pkts 2437
```

Après qu'une session de 802.1x soit établie, de plusieurs paquets d'EAP sont permutés au-dessus d'EAPOL. La dernière réponse réussie du rayon-Acccept intérieur porté ISE (succès d'EAP) inclut également plusieurs attributs RADIUS.

```
RADIUS: Received from id 1645/40 10.48.66.74:1645, Access-Accept, len 376
RADIUS:  EAP-Key-Name        [102] 67  *
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "linksec-policy=must-secure"
```

```
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Send-Key   [16]  52  *
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Recv-Key   [17]  52  *
```

L'Eap-Clé-nom est utilisé pour la session MKA. La linksec-stratégie force le commutateur pour utiliser MACsec (l'autorisation échoue si ce n'est pas complète). Ces attributs peuvent être également vérifiés dans les captures de paquet.

L'authentification est réussie.

```
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Le commutateur applique les attributs (ceux-ci incluent un nombre facultatif VLAN qui a été également envoyé).

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

Le commutateur commence alors la session MKA quand il envoie et reçoit des paquets EAPOL.

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

Après que l'échange de 4 paquets sécurisent des identifiants sont créés avec l'association de sécurité de la réception (RX).

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A5020002
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
```

La session est de finition et l'association de sécurité de la transmission (TX) est ajoutée.

```
%MKA-5-SESSION_SECURED: (Gi1/0/2 : 2) MKA Session was secured for
RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D56FD55B3BF,
CKN A2BDC3BE967584515298F3F1B8A9CC13
HULC-MACsec: Process install TxSA request66B4EEC for interface GigabitEthernet1/0/
```

La stratégie « devoir-sécurisée » est appariée et l'autorisation est réussie.

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Tous les paquets de 2 secondes MKA bonjour sont permutés afin de s'assurer que tous les participants sont actifs.

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Debugs pour un scénario manquant

Quand le suppliant n'est pas configuré pour MKA et l'ISE demande le cryptage après une

authentification réussie de 802.1x :

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

Les essais de commutateur pour initier une session MKA quand il envoie 5 paquets EAPOL.

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

Et chronomètre finalement et échoue autorisation.

```
 %MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) Peer has stopped sending MKPDUs for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gi1/0/2 : 2) MKA Session was stopped by MKA and not
secured for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529,
CKN F8288CDF7FA56386524DD17F1B62F3BA
%AUTHMGR-5-FAIL: Authorization failed or unapplied for client (0050.5699.36ce)
on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

La session de 802.1x signale l'authentification réussie, mais l'autorisation défaillante.

```
bsns-3750-5#show authentication sessions int g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Failed
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D55FD4D7529
     Acct Session ID:  0x00011CA0
              Handle:  0xA4000D56

Runnable methods list:
      Method   State
       dot1x    Authc Success
```

Le trafic de données sera bloqué.

Captures de paquet

Quand le trafic est capturé sur les requêtes d'écho/réponses de Protocole ICMP (Internet Control Message Protocol) du site 4 de suppliant sont envoyés et reçu, il y aura :

- 4 requêtes d'écho chiffrées d'ICMP envoyées au commutateur (88e5 est réservé pour 802.1AE)
- 4 ont déchiffré des réponses d'écho d'ICMP reçues

C'est en raison de la façon dont des crochets d'AnyConnect sur Windows API (avant libpcap quand des paquets sont envoyés et avant libpcap quand des paquets sont reçus) :

> **Note**: La capacité de renifler le trafic MKA ou 802.1AE sur le commutateur avec des configurations telles que le Fonction Switched Port Analyzer (SPAN) ou la capture incluse de paquet (CPE) n'est pas prise en charge.

Modes de MACsec et de 802.1x

Non tous les modes de 802.1x sont pris en charge pour MACsec.

Le guide de Comment-Faire du Cisco TrustSec 3.0 : L'introduction à MACsec et à NDAC déclare cela :

- **Mode de seul hôte** : **MACsec est entièrement pris en charge** en mode de seul hôte. En ce mode, seulement un MAC ou une adresse IP simple peut être authentifié et sécurisé avec MACsec. Si une adresse MAC différente est détectée sur le port après qu'un point final ait authentifié, une violation de sécurité sera déclenchée sur le port.
- **Mode de l'authentification de Multi-domaine (MDA)** : En ce mode, un point final peut être sur le domaine de données et un autre point final peut être sur le domaine de Voix. **MACsec est entièrement pris en charge en mode MDA**. Si les deux points finaux sont MACsec-capables, chacun sera sécurisé par sa propre session indépendante de MACsec. Si seulement un point final est MACsec-capable, ce point final peut être sécurisé tandis que l'autre point final envoie le trafic en clair.
- **Mode de Multi-authentification** : En ce mode, un nombre de points finaux pratiquement illimité peut être authentifié à un port de commutateur simple. **MACsec n'est pas pris en charge en ce mode.**
- **Mode de Multi-hôte** : Tandis que l'utilisation de MACsec en ce mode est techniquement possible, **elle n'est pas recommandée**. En mode de Multi-hôte, le premier point final sur le port authentifie, et alors tous les points finaux supplémentaires seront permis sur le réseau par l'intermédiaire de la première autorisation. MACsec fonctionnerait avec le premier hôte connecté, mais aucun autre point final ? le trafic s passerait réellement, puisque ce ne serait pas le trafic chiffré.

Informations connexes

- Guide de configuration de Cisco TrustSec pour 3750
- Guide de configuration de Cisco TrustSec pour ASA 9.1
- Services basés sur identité de réseau : Mac security
- Le nuage de TrustSec avec le 802.1x MACsec sur la gamme du Catalyst 3750X commutent l'exemple de configuration
- L'ASA et les séries du Catalyst 3750X commutent l'exemple de configuration de TrustSec et dépannent le guide

- Déploiement et feuille de route de Cisco TrustSec
- Support et documentation techniques - Cisco Systems

Ce document était-il utile ? Oui aucun

Merci de votre feedback.

Ouvrez une valise de support (exige un contrat de service Cisco.)

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Janv. 31, 2014
ID de document : 117277