Exemple de configuration du chiffrement d'hôte de commutateur MACsec avec Cisco AnyConnect et ISE

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Configuration Diagramme et flux du trafic du réseau Configurations ISE Commutateur NAM AnyConnect Vérification Dépannage Débogues pour un scénario de travail Débogues pour un scénario défaillant Captures de paquets Modes MACsec et 802.1x Informations connexes

Introduction

Ce document fournit un exemple de configuration pour le chiffrement MACsec (Media Access Control Security) entre un demandeur 802.1x (Cisco AnyConnect Mobile Security) et un authentificateur (commutateur). Cisco ISE (Identity Services Engine) est utilisé comme serveur d'authentification et de stratégie.

MACsec est standardisé dans 802.1AE et pris en charge sur les commutateurs Cisco 3750X, 3560X et 4500 SUP7E. 802.1AE définit le chiffrement de liaison sur les réseaux câblés qui utilisent des clés hors bande. Ces clés de chiffrement sont négociées avec le protocole MKA (MACsec Key Agreement) utilisé après une authentification 802.1x réussie. MKA est normalisé dans la norme IEEE 802.1X-2010.

Un paquet est chiffré uniquement sur la liaison entre le PC et le commutateur (chiffrement point à point). Le paquet reçu par le commutateur est déchiffré et envoyé via des liaisons ascendantes non chiffrées. Afin de chiffrer la transmission entre les commutateurs, le chiffrement de commutateur est recommandé. Pour ce chiffrement, le protocole SAP (Security Association Protocol) est utilisé pour négocier et régénérer les clés. SAP est un protocole d'accord clé prénormalisé développé par Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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

- Systèmes d'exploitation Microsoft Windows 7 et Microsoft Windows XP
- Logiciel Cisco 3750X, versions 15.0 et ultérieures
- Logiciel Cisco ISE, versions 1.1.4 et ultérieures
- Cisco AnyConnect Mobile Security avec Network Access Manager (NAM), versions 3.1 et ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Diagramme et flux du trafic du réseau



192.168.1.201

Étape 1. Le demandeur (AnyConnect NAM) démarre la session 802.1x. Le commutateur est l'authentificateur et l'ISE est le serveur d'authentification. Le protocole EAP (Extensible Authentication Protocol over LAN) est utilisé comme transport pour EAP entre le demandeur et le commutateur. RADIUS est utilisé comme protocole de transport pour EAP entre le commutateur et l'ISE. Le contournement d'authentification MAC (MAB) ne peut pas être utilisé, car les clés EAPOL doivent être retournées à partir d'ISE et utilisées pour la session MACsec Key Agreement (MKA).

Étape 2. Une fois la session 802.1x terminée, le commutateur lance une session MKA avec EAPOL comme protocole de transport. Si le demandeur est configuré correctement, les clés de cryptage symétrique AES-GCM 128 bits (mode Galois/Counter) correspondent.

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

Configurations

La configuration ISE implique un scénario type 802.1x, à l'exception du profil d'autorisation qui peut inclure des stratégies de chiffrement.

Choisissez Administration > Network Resources > Network Devices afin d'ajouter le commutateur en tant que périphérique réseau. Saisissez une clé pré-partagée RADIUS (Shared Secret).

alah	
cisco Identity Services Engine	Administration ▼
🔆 System 🧏 Identity Management 🔛	Network Resources 🛃 Web Portal Management 👸 Feed Service
Network Devices Network Device Groups E	xternal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices	Network Devices List > 3750-5 Network Devices * Name 3750-5 Description * IP Address: 10.48.66.109 / 32 Model Name v Software Version v * Network Device Group
	Location All Locations Set To Default Device Type All Device Types Set To Default
	Enable Authentication Settings Protocol RADIUS *Shared Secret Show

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

Choisissez Administration > Identity Management > Users afin de définir l'utilisateur « cisco » localement.

cisco Identity Services Engine	
🔆 System 🏼 🖉 Identity Management	🖥 Network Resources 🛛 🛃 Web Portal Management 🛛 🔂 Feed Service
Identities Groups External Identity Sources	s Identity Source Sequences Settings
Identities Identities Image: state stat	Network Access Users List > New Network Access User ✓ Network Access User *Name cisco Status ✓ Enabled ✓ Email
	Password * Password * Password * Re-Enter Password • • • • • • • • • • • • • • • • •

Le profil d'autorisation peut inclure des stratégies de chiffrement. Comme indiqué dans cet

ISE

exemple, choisissez **Policy > Results > Authorization Profiles** afin d'afficher les informations que ISE renvoie au commutateur que le chiffrement de liaison est obligatoire. En outre, le numéro de VLAN (10) a été configuré.

cisco Identity Services Engine	Administration ▼
Authentication Authorization Results	Profiling Posture Client Provisioning Security Group Access Authorization Profiles > MACSECprofile
	Authorization Profile *Name MACSECprofile Description *Access Type ACCESS_ACCEPT Service Template
 Client Provisioning Security Group Access 	Common Tasks Auto Smart Port Filter-ID Reauthentication
	MACSec Policy must-secure 💌

Choisissez **Policy > Authorization** afin d'utiliser le profil d'autorisation dans la règle d'autorisation. Cet exemple montre comment renvoyer le profil configuré pour l'utilisateur « cisco ». Si la norme 802.1x réussit, ISE renvoie Radius-Accept au commutateur avec Cisco AVPair linksecpolicy=must-secure. Cet attribut force le commutateur à lancer une session MKA. Si cette session échoue, l'autorisation 802.1x sur le commutateur échoue également.

cisco Identity Services Engine	Administration Ad	ration 🔻
🛓 Authentication 🛛 🧕 Authorization 🔀	Profiling 👩 Posture 👦 Client Provisioning 🚍 S	ecurity Group Access 🛛 🐥 Policy Elements
Authorization Policy Define the Authorization Policy by configuring rules ba First Matched Rule Applies	ised on identity groups and/or other conditions. Drag and drop rule	s to change the order.
 Exceptions (0) Standard 		
Status Rule Name	Conditions (identity groups and other conditions)	Permissions
Macsec	if Radius:User-Name EQUALS cisco	then MACSECprofile

Commutateur

Les paramètres de port 802.1x standard sont les suivants (partie supérieure illustrée) :

```
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 MKA locale 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 MKA locale vous permet de configurer des paramètres détaillés qui ne peuvent pas être poussés à partir de l'ISE. La stratégie MKA locale est facultative.

NAM AnyConnect

Le profil du demandeur 802.1x peut être configuré manuellement ou poussé via Cisco ASA. Les étapes suivantes présentent une configuration manuelle.

Afin de gérer les profils NAM :

🕥 Cisco AnyConnect Secure Mobility Client 📃 🖃 💌					
	VPN: You may need to use a browser to gain access.				
Web Authent	Web Authentication Required				
	Network: Connected (10.48.67.84)				
	wired Manage Networks				
	wired	Manage Networks			
T	wired	Manage Networks Connect only to current network			

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

Sisco AnyConnect Secure Mobility Client		
cisco AnyConnec	t Secure Mobility Client	0
Status Overview	Network Access Manager	
VPN	Cisco AnyConnect	
Networks >	Enter information for the connection. Media: O Wi-Fi O Wired Hidden Network	Network Service: Enabled Wi-Fi: No Wi-Fi adapters
	Hidden Network Descriptive Name: macsec SSID: Security: 802.1X (MACsec) 802.1X Configuration password PEAP OK Cancel	Type Privileges Wired Administra

Vérification

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

Le NAM AnyConnect configuré pour EAP-PEAP nécessite des informations d'identification correctes.

Cisco AnyConnect	macsec 💽				
Please enter your username and password for the network: macsec					
Username:	cisco				
Password:	******				
	Show Password				
	OK Cancel				
Sisco AnyConn	ect Secure Mobility Client 🗖 🔲 🖾				
Web Authenticat	PN: ou may need to use a browser to gain access. Connect ion Required				
Web Authenticat	PN: ou may need to use a browser to gain access. Connect ion Required etwork: uthenticating macsec $\sim \sim \sim \sim \sim$				
Web Authenticat	PN: ou may need to use a browser to gain access. Connect ion Required etwork: uthenticating macsec				

La session sur le commutateur doit être authentifiée et autorisée. L'état de sécurité doit 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 MACsec sur le commutateur fournissent les détails relatifs aux paramètres de stratégie locale, aux identificateurs de canaux sécurisés (SIC) pour le trafic reçu/envoyé, ainsi que les statistiques et les erreurs de port.

```
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 pkts0Ingress notag pkts2441Ingress badtag pkts0Ingress unknownSCI pkts0Ingress noSCI pkts0Unused pkts0
 Ingress noSCI pkts 0
  Notusing pkts 0
                               Decrypt bytes 176153
```

Ingress miss pkts 2437

Sur AnyConnect, les statistiques indiquent l'utilisation du chiffrement et les statistiques de paquets.

Notwork Accose M

		^
Subnet Mask (IPV4)	255.255.255.0	
Default Gateway (IPv4)	192.168.1.10	
Bytes		· · · · ·
Sent:	16567	
Received:	5760	
Frames		^
Sent:	115	
Received:	49	
Security Information —		∧
Configuration:	802.1X (MACsec)	_
Encryption:	GCM(Software)	=
EAP Method:	eapPeap(eapMschapv2)	
Server:	ise2.test-cisco.com	
Credential Type:	Username/Password	
		Ŧ

Dépannage

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

Débogues pour un scénario de travail

Activez les débogages sur le commutateur (certains résultats ont été omis pour plus de clarté).

debug macsec event debug macsec error debug epm all debug dot1x all debug radius debug radius verbose

Après l'établissement d'une session 802.1x, plusieurs paquets EAP sont échangés via EAPOL. La dernière réponse réussie d'ISE (EAP Success) transportée à l'intérieur de Radius-Accepcept 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:Vendor, Cisco[20]34RADIUS: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	*

EAP-Key-Name est utilisé pour la session MKA. La stratégie linksec force le commutateur à utiliser MACsec (l'autorisation échoue si ce n'est pas terminé). Ces attributs peuvent également être vérifiés dans les captures de paquets.

18	10.48	.66.7	4 10.48.	66.109	RADIUS	418 Access-Accept(2)	(id=40,]	l=376
Þ	AVP:	l=7	t=User-Name(1):	cisco				
Þ	AVP:	l=40	t=State(24): 52	265617574	46853657373696f6e	3a433041383030303130	30	
Þ	AVP:	l=51	t=Class(25): 43	34143533a	4330413830303031	30303030304435364644	35	
Þ	AVP:	l=6	t=Tunnel-Type(64	 Tag=0; 	(01: VLAN(13)			
Þ	AVP:	l=6	t=Tunnel-Medium	Type (65)) Tag=0x01: IEEE-	802(6)		
Þ	AVP:	l=6	t=EAP-Message(79) Last S	Segment[1]			
Þ	AVP:	l=18	t=Message-Autho	enticator	r(80): 05fc3f0450	d6b4f805644045519929	72	
Þ	AVP:	l=5	t=Tunnel-Private	-Group-J	[d(81) Tag=0x01:	10		
P	AVP:	l=67	t=EAP-Key-Name	(102): \@	031R\315g\206\334	\236\254\344:\333`jH	\355(\353	\343\;
	[Le	ngth:	65]					
	EAP	-Key-	Name: \031R\315g	\206\334	\236\254\344:\33	3`jH\355(\353\343\25	5\004\362H	\376\
Þ	AVP:	l=34	t=Vendor-Speci	fic(26) v	<pre>/=ciscoSystems(9)</pre>			
	► VSA	: l=2	8 t=Cisco-AVPair	(1): lin	ksec-policy=must	-secure		
Þ	AVP:	l=58	t=Vendor-Speci	ic(26) ν	/=Microsoft(311)			
Þ	AVP:	l=58	t=Vendor-Speci	fic(26) v	/=Microsoft(311)			

L'authentification a réussi.

%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 (ils incluent un numéro de VLAN facultatif qui a également été envoyé).

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

Le commutateur démarre ensuite la session MKA lorsqu'il envoie et reçoit des paquets EAPOL.

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A800010000D56FD55B3BF, AuthMgr-Handle 97000D57
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
EAPOL pak dump rx
dot1x-packet(Gi1/0/2): Received an EAPOL frame
dot1x-packet(Gi1/0/2): Received an MKA packet
```

Après avoir créé 4 identificateurs sécurisés d'échange de paquets avec l'association de sécurité Receive (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 terminée et l'association de sécurité Transmit (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 « must-secure » est appariée et l'autorisation est réussie.

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

Toutes les 2 secondes, des paquets Hello MKA sont échangés afin de s'assurer que tous les participants sont vivants.

dot1x-ev(Gi1/0/2): Received TX PDU (5) for the client 0x6E0001EC (0050.5699.36ce)
dot1x-packet(Gi1/0/2): MKA length: 0x0084 data: ^A
dot1x-ev(Gi1/0/2): Sending EAPOL packet to group PAE address
EAPOL pak dump Tx

Débogues pour un scénario défaillant

Lorsque le demandeur n'est pas configuré pour MKA et que l'ISE demande le chiffrement après une authentification 802.1x réussie :

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 C0A800010000D55FD4D7529 Le commutateur tente d'initier une session MKA lorsqu'il envoie 5 paquets EAPOL.

%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000, AuditSessionID COA8000100000D55FD4D7529, AuthMgr-Handle A4000D56 dot1x-ev(Gi1/0/2): Sending out EAPOL packet EAPOL pak dump Tx dot1x-ev(Gi1/0/2): Sending out EAPOL packet EAPOL pak dump Tx dot1x-ev(Gi1/0/2): Sending out EAPOL packet EAPOL pak dump Tx dot1x-ev(Gi1/0/2): Sending out EAPOL packet EAPOL pak dump Tx dot1x-ev(Gi1/0/2): Sending out EAPOL packet EAPOL pak dump Tx

```
Et finalement, l'autorisation expire et échoue.
```

%MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) Peer has stopped sending MKPDUs for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A800010000D55FD4D7529, 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 C0A80010000D55FD4D7529La session 802.1x signale une authentification réussie, mais une autorisation échouée.

```
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: COA8000100000D55FD4D7529
    Acct Session ID: 0x00011CA0
            Handle: 0xA4000D56
Runnable methods list:
    Method State
      dot1x Authc Success
Le trafic de données sera bloqué.
```

Captures de paquets

Lorsque le trafic est capturé sur le site demandeur 4, les demandes/réponses d'écho ICMP (Internet Control Message Protocol) sont envoyées et reçues, il y a :

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

Cela est dû à la façon dont AnyConnect se connecte à l'API Windows (avant libpcap lors de l'envoi de paquets et avant libpcap lors de la réception de paquets) :

Destination	Protocol L	ength Info					
Cisco_25:a5:43	0x88e5	106 Ethernet II					
192.168.1.201	ICMP	74 Echo (ping) reply	id=0x0001, seq=23/5888, ttl=255				
Cisco_25:a5:43	0x88e5	106 Ethernet II					
192.168.1.201	ICMP	74 Echo (ping) reply	id=0x0001, seq=24/6144, ttl=255				
Cisco_25:a5:43	0x88e5	106 Ethernet II					
192.168.1.201	ICMP	74 Echo (ping) reply	id=0x0001, seq=25/6400, ttl=255				
Cisco_25:a5:43	0x88e5	106 Ethernet II					
192.168.1.201	ICMP	74 Echo (ping) reply	id=0x0001, seq=26/6656, ttl=255				
Frame 3: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)							
Ethernet II, Src: Vmware_99:36:ce (00:50:56:99:36:ce), Dst: Cisco_25:a5:43 (bc:16:65:25:a5:43)							
0569936ce0000565d05c	5dfa65d73	45d3					
	Destination Cisco_25:a5:43 192.168.1.201 Cisco_25:a5:43 192.168.1.201 Cisco_25:a5:43 192.168.1.201 Cisco_25:a5:43 192.168.1.201 (ire (848 bits), 106 re_99:36:ce (00:50:5)	Destination Protocol L Cisco_25:a5:43 0x88e5 192.168.1.201 ICMP cire (848 bits), 106 bytes cap 102.168.1.201 ICMP cire (848 bits), 106 bytes cap 102.168.1.201 ICMP	Destination Protocol Length Info Cisco_25:a5:43 0x88e5 106 Ethernet II 192.168.1.201 ICMP 74 Echo (ping) reply Cisco_25:a5:43 0x88e5 106 Ethernet II 192.168.1.201 ICMP 74 Echo (ping) reply Cisco_25:a5:43 0x88e5 106 Ethernet II 192.168.1.201 ICMP 74 Echo (ping) reply Cisco_25:a5:43 0x88e5 106 Ethernet II 192.168.1.201 ICMP 74 Echo (ping) reply Cisco_25:a5:43 0x88e5 106 Ethernet II 192.168.1.201 ICMP 74 Echo (ping) reply Cisco_25:a5:43 0x88e5 106 Ethernet II 192.168.1.201 ICMP 74 Echo (ping) reply cire (848 bits), 106 bytes captured (848 bits) reply reply:36:ce (00:50:56:99:36:ce), Dst: Cisco_25:a5:43 (bits) 0569936ce00000565d05c5dfa65d7345d3				

[Length: 92]

Note: La possibilité de détecter le trafic MKA ou 802.1AE sur le commutateur avec des fonctionnalités telles que SPAN (Switched Port Analyzer) ou EPC (Embedded Packet Capture) n'est pas prise en charge.

Modes MACsec et 802.1x

Tous les modes 802.1x ne sont pas pris en charge pour MACsec.

- Mode hôte unique : MACsec est entièrement pris en charge en mode hôte unique. Dans ce mode, seule une adresse MAC ou IP peut être authentifiée et sécurisée avec MACsec. Si une autre adresse MAC est détectée sur le port après l'authentification d'un point de terminaison, une violation de sécurité est déclenchée sur le port.
- Mode d'authentification multidomaine (MDA) : Dans ce mode, un point de terminaison peut se trouver sur le domaine de données et un autre sur le domaine vocal. MACsec est entièrement pris en charge en mode MDA. Si les deux points de terminaison sont compatibles MACsec, chacun sera sécurisé par sa propre session MACsec indépendante. Si un seul point d'extrémité est compatible MACsec, ce point d'extrémité peut être sécurisé tandis que l'autre point d'extrémité envoie le trafic en clair.
- Mode Multi-Authentification : Dans ce mode, un nombre quasi illimité de terminaux peut être authentifié sur un port de commutateur unique. MACsec n'est pas pris en charge dans ce mode.
- Mode multihôte : Bien que l'utilisation de MACsec dans ce mode soit techniquement possible, elle n'est pas recommandée. En mode multihôte, le premier point de terminaison du port s'authentifie, puis tout point de terminaison supplémentaire sera autorisé sur le réseau via la première autorisation. MACsec fonctionnerait avec le premier hôte connecté, mais aucun autre trafic de point d'extrémité ne passerait, car il ne s'agirait pas de trafic chiffré.

Informations connexes

- Guide de configuration de Cisco TrustSec pour 3750
- Guide de configuration de Cisco TrustSec pour ASA 9.1
- <u>Services réseau basés sur l'identité : Sécurité MAC</u>
- Exemple de configuration du cloud TrustSec avec 802.1x MACsec sur les commutateurs de la gamme Catalyst 3750X
- Exemple de configuration de l'ASA et du commutateur Catalyst de la série 3750X TrustSec et guide de dépannage
- Déploiement et feuille de route de Cisco TrustSec
- Support et documentation techniques Cisco Systems