하위 인터페이스를 사용하여 Catalyst 8500에서 WAN MACsec 구성

목차

소개

이 문서에서는 하위 인터페이스를 사용하여 Cisco Catalyst 8500 플랫폼에서 WAN MACsec(Media Access Control Security)을 구성하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WAN, VLAN, 암호화를 비롯한 고급 네트워킹 개념
- MACsec(IEEE 802.1AE) 및 키 관리(IEEE 802.1X-2010) 이해
- Cisco IOS® XE 명령줄 인터페이스(CLI) 숙지

사용되는 구성 요소

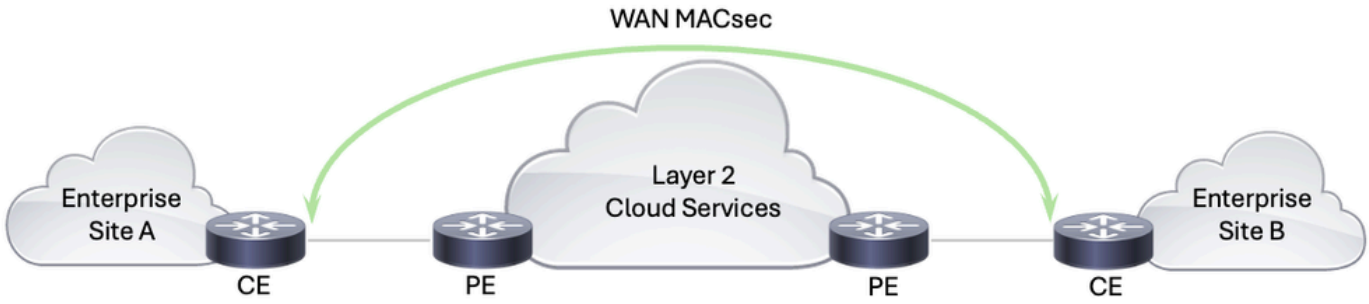
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 8500 Series Edge Platform
- Cisco IOS XE 버전 17.14.01a

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

WAN MACsec은 MACsec의 기능을 활용하여 WAN 네트워크 전체에서 네트워크 트래픽을 보호하도록 설계된 보안 솔루션입니다. 통신 사업자 네트워크를 사용하여 데이터를 교환할 때 변조 방지를 위해 전송 중인 데이터를 암호화하는 것이 중요합니다. WAN MACsec은 구축 및 관리가 용이하여 도청 및 중간자(man-in-the-middle) 공격과 같은 데이터 조작으로부터 네트워크 트래픽을 보호해야 하는 조직에 적합합니다. 또한 끊김 없는 회선 속도(line-rate) 암호화를 제공하여 데이터가 통신 사업자 네트워크, 클라우드 환경, 엔터프라이즈 네트워크 등 다양한 네트워크 인프라를 통과할 때 안전하게 보호되고 손상되지 않도록 보장합니다.



WAN MACsec 솔루션

IEEE 802.1AE 표준에 의해 정의된 MACsec은 약간의 기록을 공유하기 위해 이더넷 프레임에 대한 데이터 기밀성, 무결성 및 원본 신뢰성을 보장함으로써 이더넷 네트워크에서 안전한 통신을 제공합니다. MACsec은 OSI(Open Systems Interconnection) 모델의 데이터 링크 레이어(레이어 2)에서 작동하여 이더넷 프레임을 암호화하고 인증하여 노드 간 통신을 보호합니다. 원래 LAN용으로 설계된 MACsec은 WAN 구축도 지원하도록 발전했습니다. 고속 네트워크에 중요한 라인 레이트 암호화를 통해 지연 시간과 오버헤드를 최소화합니다.

IEEE 802.1X-2010은 포트 기반 네트워크 액세스 제어를 정의하는 원래 IEEE 802.1X 표준의 개정판입니다. 2010 개정판에는 MACsec 구현에서 암호화 키를 관리하는 데 필수적인 MKA(MACsec Key Agreement) 프로토콜이 도입되었습니다. MKA는 MACsec에서 데이터를 암호화 및 암호 해독하는 데 사용하는 암호화 키의 배포 및 관리를 처리합니다. MKA는 MACsec 구축을 위한 멀티벤더 상호운용성에 기여하는 표준으로, 동적 WAN 환경에서 지속적인 보안을 유지하는 데 필수적인 안전한 키 교환 및 키 재설정 메커니즘을 지원합니다.

WAN MACsec 구축에서 IEEE 802.1AE(MACsec)는 데이터 링크 계층에서 기본 암호화 및 보안 메커니즘을 제공하여 모든 이더넷 프레임이 네트워크를 통과할 때 보호되도록 합니다. MKA 프로토콜을 사용하는 IEEE 802.1X-2010은 MACsec이 작동하는 데 필요한 암호화 키를 배포하고 관리하는 중요한 작업을 처리합니다. 이러한 표준은 WAN MACsec이 WAN 네트워크 전반에 걸쳐 강력한 고속 암호화를 제공하여 전송 중인 데이터를 포괄적으로 보호하면서 상호운용성과 관리 용이성을 유지할 수 있도록 합니다.

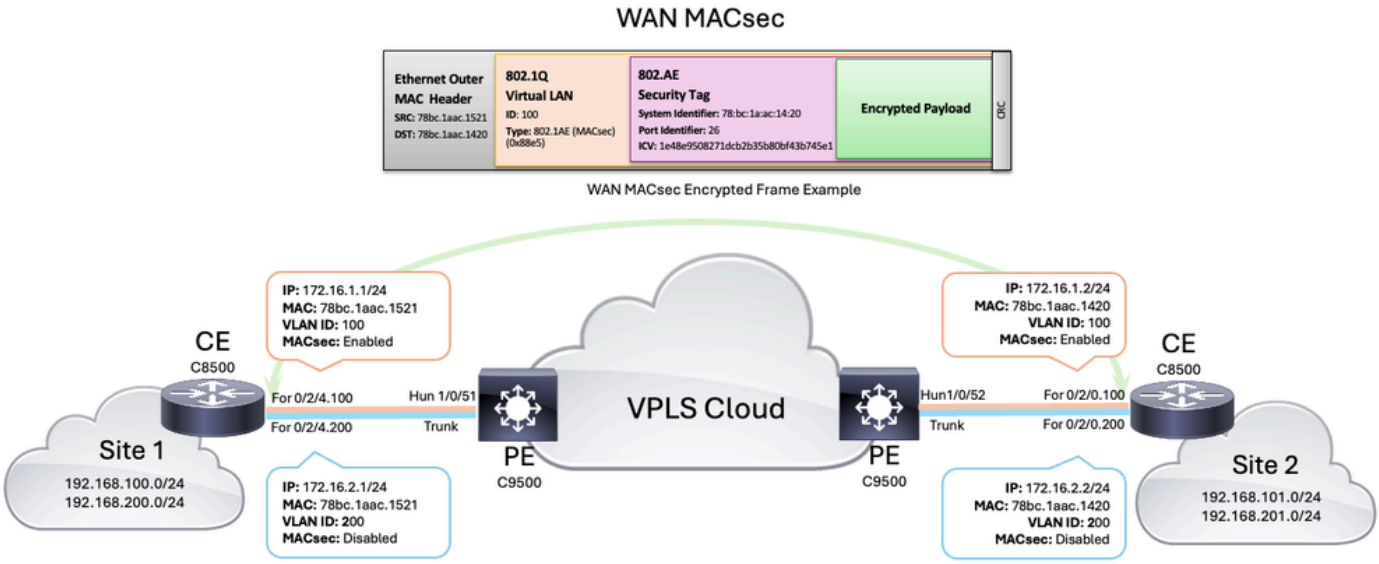
WAN 환경의 고유한 과제를 해결하기 위해 기존 MACsec 구축에서 몇 가지 기능이 개선되었습니다
.

- 802.1Q Tag in the Clear: 이 기능을 사용하면 802.1Q VLAN 태그를 암호화된 MACsec 헤더 외부로 노출할 수 있으므로, 특히 공용 이더넷 전송 환경에서 더욱 유연한 네트워크 설계를 용이하게 합니다. 이 기능은 MACsec을 캐리어 이더넷 서비스와 통합하는 데 필수적입니다. 동일한 네트워크에서 암호화 트래픽과 비암호화 트래픽을 공존시켜 네트워크 아키텍처를 간소화하고 비용을 절감할 수 있기 때문입니다.
- PMC(Public Carrier Ethernet)를 통한 적응성: 최신 WAN MACsec 구현은 PMC(Public Carrier Ethernet) 서비스에 적응할 수 있습니다. 이러한 적응성에는 EAPoL(Ethernet Authentication Protocol over LAN) 대상 주소 및 이더 타입 수정이 포함되며, 이를 통해 MACsec이 캐리어 이더넷 네트워크에서 원활하게 작동하여 이러한 프레임을 사용하거나 차단할 수 있습니다.

WAN MACsec은 이더넷 암호화의 상당한 진보를 나타내며, 고속 보안 WAN 연결에 대한 증가하는 요구를 해결합니다. 또한 유선 속도 암호화, 유연한 네트워크 설계 지원, 공용 캐리어 서비스에 대한 적응성을 제공할 수 있어 최신 네트워크 보안 아키텍처의 중요한 구성 요소가 됩니다. 조직은 WAN MACsec을 활용하여 고속 WAN 링크의 강력한 보안을 달성하는 동시에 네트워크 아키텍처를 간소화하고 운영 복잡성을 줄일 수 있습니다.

구성

네트워크 다이어그램



WAN MACsec 토폴로지

설정

1단계: 기본 디바이스 컨피그레이션

컨피그레이션을 시작하려면 먼저 트래픽 세그멘테이션 및 서비스 공급자와의 연결에 사용할 하위 인터페이스를 정의해야 합니다. 이 시나리오에서는 서브넷 172.16.1.0/24에 연결된 VLAN 100 및 서브넷 172.16.2.0/24에 연결된 VLAN 200에 대해 두 개의 하위 인터페이스가 정의됩니다(나중에 하나의 하위 인터페이스만 MACsec으로 구성됩니다).

CE 8500-1	CE 8500-2

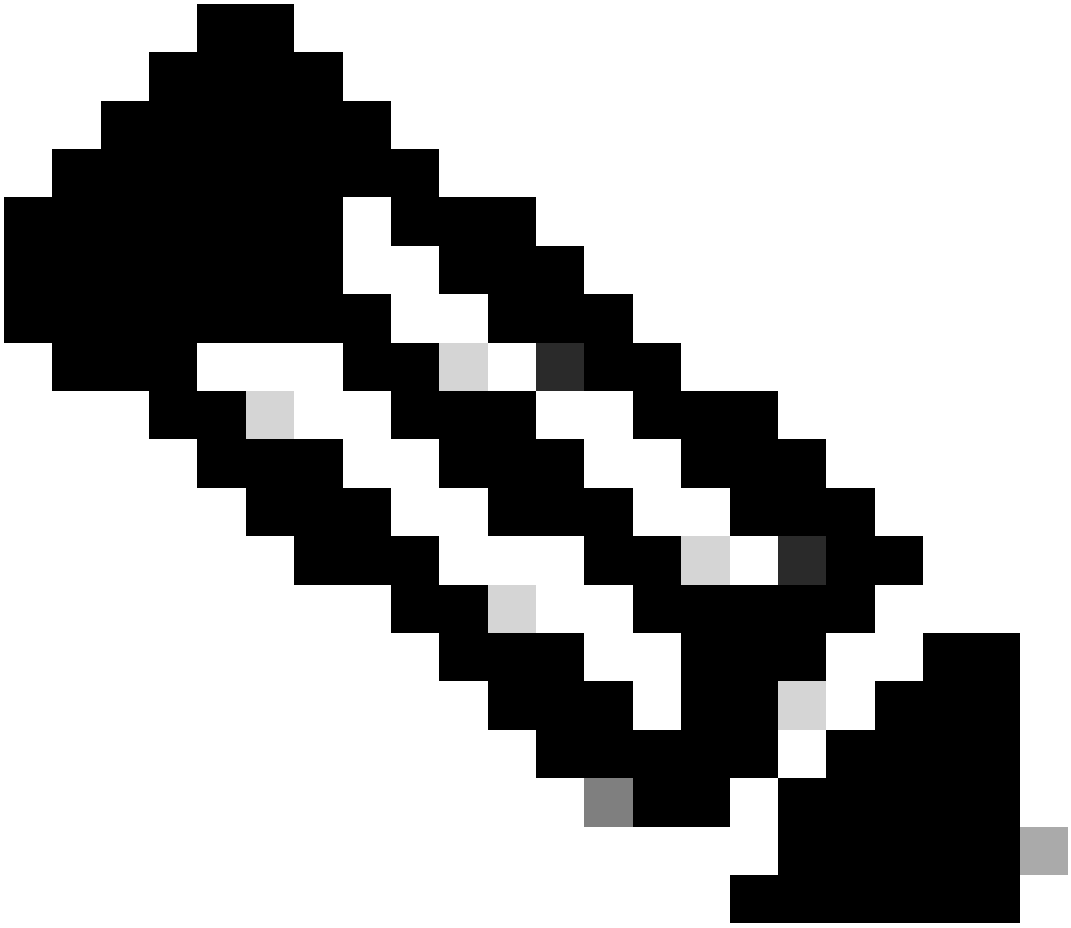
<#root>	<#root>
interface FortyGigabitEthernet0/2/4.100	interface FortyGigabitEthernet0/2/0.100
encapsulation dot1Q 100 ip address 172.16.1.1 255.255.255.0	**encapsulation dot1Q 100 ip address 172.16.**
!	!
interface FortyGigabitEthernet0/2/4.200	interface FortyGigabitEthernet0/2/0.200
encapsulation dot1Q 200 ip address 172.16.2.1 255.255.255.0	**encapsulation dot1Q 200 ip address 172.16.**

2단계: MACsec 키 체인 구성

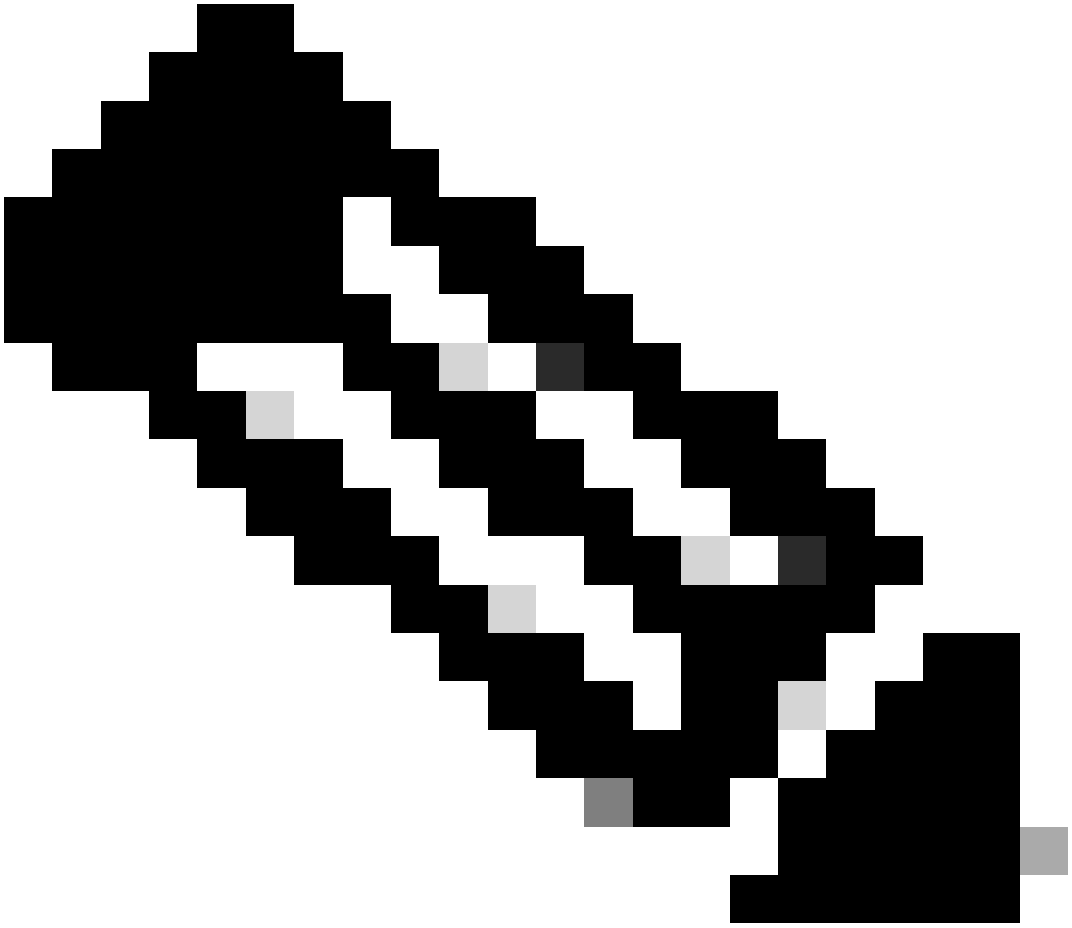
IEEE 802.1X-2010 표준에서는 MACsec 암호화 키를 PSK(Pre-Shared Key)에서 802.1X EAP(Extensible Authentication Protocol)로 파생하거나 MKA 키 서버에서 선택 및 배포할 수 있음을 명시합니다. 이 예에서는 PSK가 사용되고 MACsec 키 체인을 통해 수동으로 구성되며, 이는 MACsec에서 사용되는 다른 모든 암호화 키를 파생시키는 데 사용되는 기본 키인 CAK(Connectivity Association Key)와 동일합니다.

CE 8500-1	
<#root>	<#root>
8500-1#	8500-2#
configure terminal	**configure terminal**
8500-1(config)#	**8500-2(config)#**
key chain keychain_vlan100 macsec	**key chain keychain_vlan100**
8500-1(config-keychain-macsec)#	**8500-2(config-keychain-macs**
key 01	**key 01**
8500-1(config-keychain-macsec-key)#	**8500-2(config-keychain-macs**
cryptographic-algorithm aes-256-cmac	**cryptographic-algorithm aes**
8500-1(config-keychain-macsec-key)#	**8500-2(config-keychain-macs**
key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1	**key-string a5b2df4657bd8c02**
8500-1(config-keychain-macsec-key)#	**8500-2(config-keychain-macs**
lifetime 00:00:00 Jun 1 2024 duration 864000	**lifetime 00:00:00 Jun 1 202**
8500-1(config-keychain-macsec-key)#	**8500-2(config-keychain-macs**
key 02	**key 02**
8500-1(config-keychain-macsec-key)#	**8500-2(config-keychain-macs**
cryptographic-algorithm aes-256-cmac	**cryptographic-algorithm aes**
8500-1(config-keychain-macsec-key)#	**8500-2(config-keychain-macs**
key-string b5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e2	**key-string b5b2df4657bd8c02**

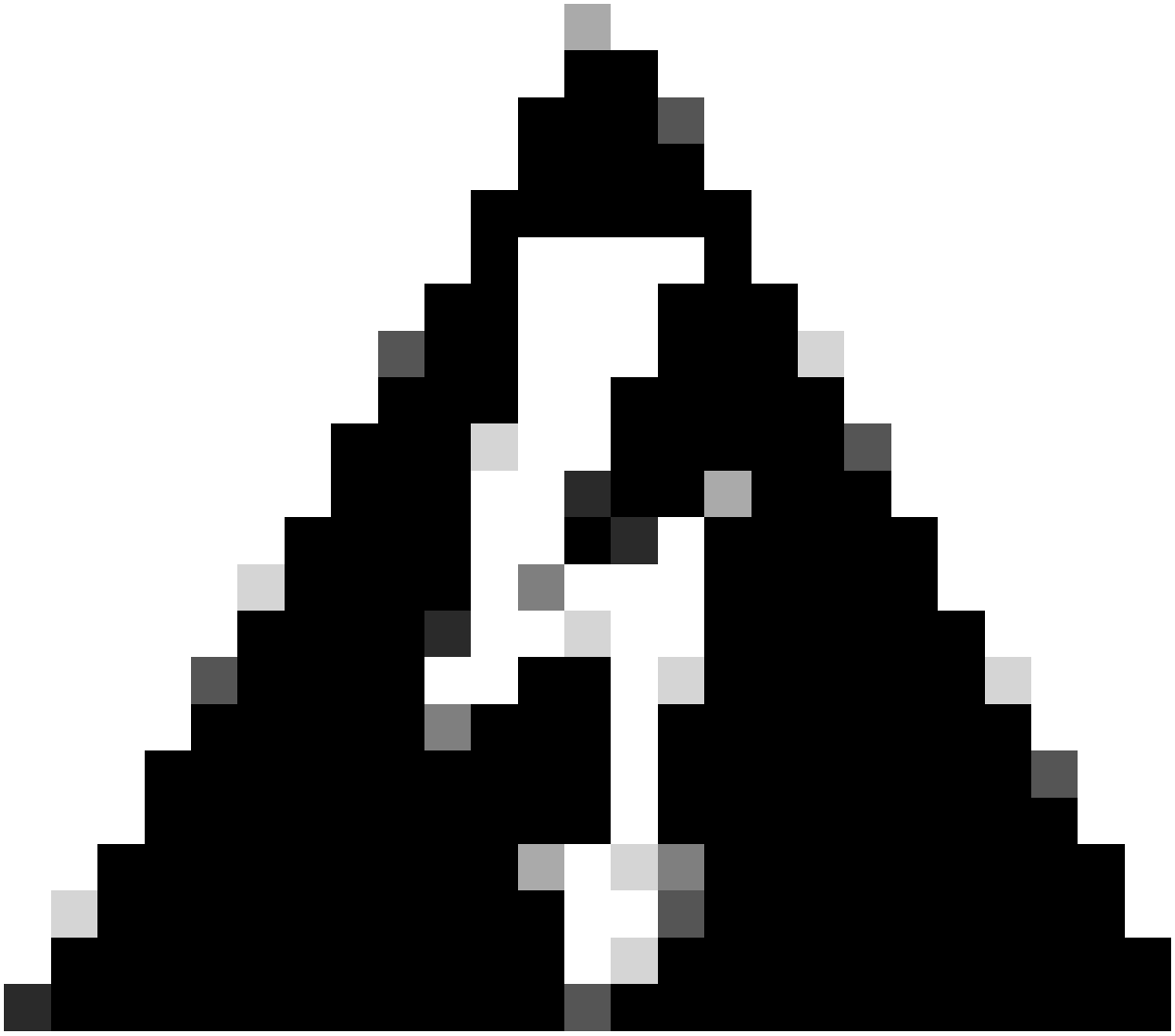
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
lifetime 23:00:00 Jun 1 2024 infinite	lifetime 23:00:00 Jun 1 202
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
exit	exit
8500-1(config-keychain-macsec)#	8500-2(config-keychain-macs
exit	exit



참고: MACsec 키 체인을 구성하는 동안 키 문자열은 16진수로만 구성되어야 하며, aes-128-cmac 암호화 알고리즘에는 32개의 16진수 키가 필요하고 aes-256-cmac 암호화 알고리즘에는 64개의 16진수 키가 필요합니다.



참고: 여러 키를 사용할 경우 지정된 키 수명이 만료된 후 히트리스 키 롤오버를 수행하려면 키 간에 중복되는 기간이 필요합니다.



경고: 두 라우터의 시계가 동기화되어 있는지 확인하는 것이 중요합니다. 따라서 NTP(Network Time Protocol)를 사용하는 것이 좋습니다. 이렇게 하지 않으면 MKA 세션 설정을 방해하거나 향후 실패할 수 있습니다.

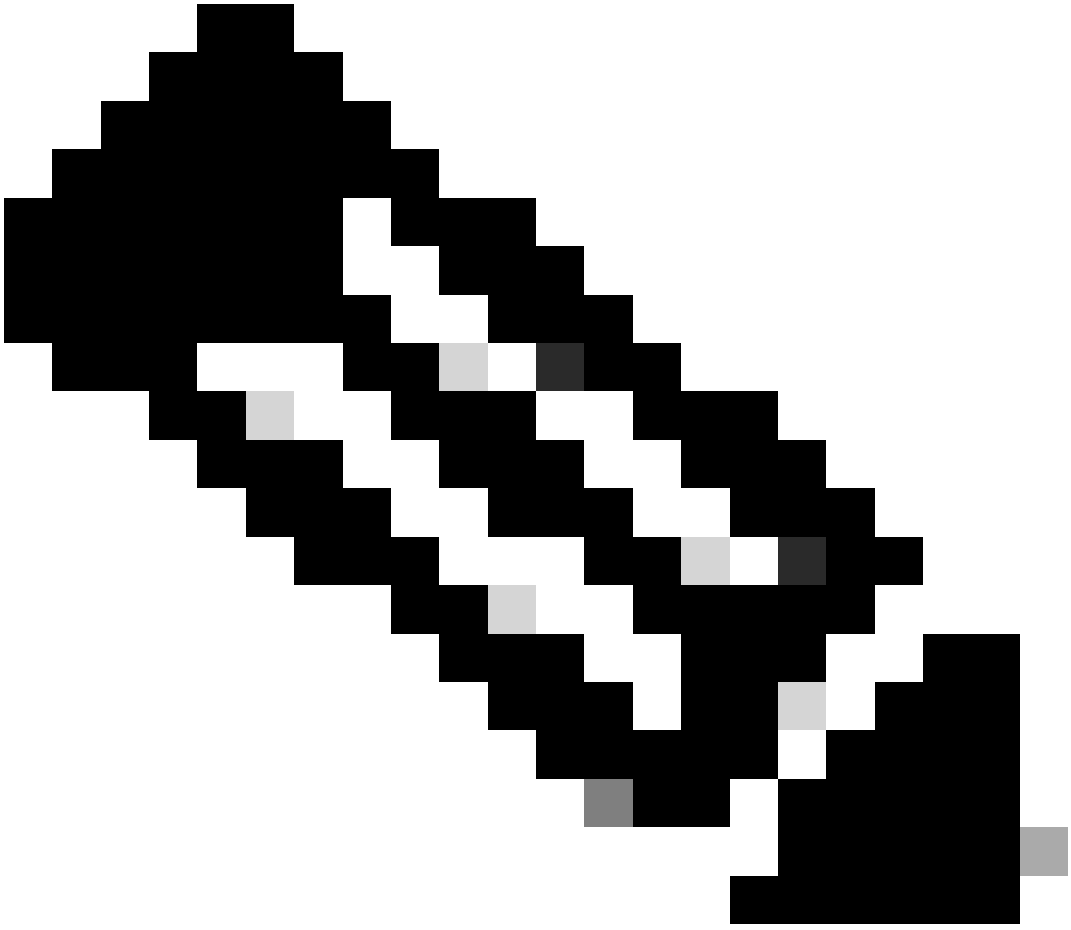
3단계: MKA 정책 구성

기본 MKA 정책은 초기 설정 및 단순 네트워크에 유용할 수 있지만, 일반적으로 특정 보안, 규정준수 및 성능 요구 사항을 충족하기 위해 WAN MACsec에 대한 사용자 지정 MKA 정책을 구성하는 것이 좋습니다. 맞춤형 정책을 통해 유연성과 제어력이 향상되어 네트워크 보안이 견고해지고 요구 사항에 맞게 맞춤화됩니다.

MKA 정책을 구성할 때 키 서버 우선순위, MACsec MKPDU(Key Agreement Packet Data Unit) 지연 보호, 암호 그룹 등 선택할 수 있는 여러 가지 요소가 있습니다. 이 플랫폼 및 소프트웨어 버전에서는 다음 암호를 사용할 수 있습니다.

MACsec 암호	설명
gcm-aes-128	128비트 키를 사용하는 AES(Advanced

	Encryption Standard)를 사용하는 GCM(Galois/Counter Mode)
gcm-aes-256	256비트 키를 사용하는 AES가 포함된 GCM(Galois/Counter Mode)(높은 암호화 강도)
gcm-aes-xpn-128	128비트 키를 사용하는 AES와 XPN(Extended Packet Numbering)을 사용하는 GCM(Galois/Counter Mode)
gcm-aes-xpn-256	256비트 키를 사용하는 AES가 포함된 GCM(Galois/Counter Mode), XPN(높은 암호화 강도)



참고: XPN은 더 긴 패킷 번호 지정을 지원하여 GCM-AES 암호를 개선하며, 이는 매우 긴 세션 또는 높은 처리량의 환경에 대한 보안을 향상시킵니다. 고속 링크(예: 40Gb/s 또는 100Gb/s)를 사용하면 키 롤오버 시간이 매우 짧을 수 있습니다. 일반적으로 전송되는 패킷 수를 기반으로 하는 MACsec 프레임 내의 PN(Packet Number)이 이러한 속도로 빠르게 소진될 수 있기 때문입니다. XPN은 패킷 번호 지정 시퀀스를 확장하므로 대용량 링크에서 발생할 수 있는 SAK(Security Association Key) rekey가 필요하지 않습니다.

이 예에서 MKA 정책에 대해 선택한 암호는 gcm-aes-xpn-256이며, 다른 요소는 기본값을 갖습니다
.

CE 8500-1	CE 8500-2
<#root> 8500-1# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. 8500-1(config)# **mka policy subint100** 8500-1(config-mka-policy)# **macsec-cipher-suite gcm-aes-xpn-256** 8500-1(config-mka-policy)# **end**	<#root> 8500-2# **configure terminal** Enter configuration commands, one per line 8500-2(config)# **mka policy subint100** 8500-2(config-mka-policy)# **macsec-cipher-suite gcm-aes-xpn-256** 8500-2(config-mka-policy)# **end**

4단계: 인터페이스 및 하위 인터페이스 레벨에서 MACsec 구성

이 시나리오에서는 물리적 인터페이스가 IP 주소로 구성되지 않더라도 일부 macsec 명령을 이 수준에서 적용하여 솔루션이 작동해야 합니다. MACsec 정책 및 키 체인은 하위 인터페이스 레벨에서 적용됩니다(컨피그레이션 예 참조).

CE 8500-1	CE 8500-2
<#root> 8500-1# **configure terminal** 8500-1(config)# **interface FortyGigabitEthernet0/2/4** 8500-1(config-if)# **mtu 9216** 8500-1(config-if)# **cdp enable** 8500-1(config-if)# **macsec dot1q-in-clear 1** 8500-1(config-if)# **macsec access-control should-secure** 8500-1(config-if)#	<#root> 8500-2# **configure terminal** 8500-2(config)# **interface FortyGigabitEthernet0/2/0** 8500-2(config-if)# **mtu 9216** 8500-2(config-if)# **cdp enable** 8500-2(config-if)# **macsec dot1q-in-clear 1** 8500-2(config-if)# **macsec access-control should-secure** 8500-2(config-if)#

exit	**exit**
8500-1(config)#	8500-1(config)#
interface FortyGigabitEthernet0/2/4.100	**interface FortyGigabitEthernet0/2/0.100**
8500-1(config-if)#	8500-2(config-if)#
eapol destination-address broadcast-address	**eapol destination-address broadcast-address**
8500-1(config-if)#	8500-2(config-if)#
eapol eth-type 876F	**eapol eth-type 876F**
8500-1(config-if)#	8500-2(config-if)#
mka policy subint100	**mka policy subint100**
8500-1(config-if)#	8500-2(config-if)#
mka pre-shared-key key-chain keychain_vlan100	**mka pre-shared-key key-chain keychain_vlan100**
8500-1(config-if)#	8500-2(config-if)#
macsec	**macsec**
8500-2(config-if)#	8500-2(config-if)#
end	**end**

물리적 인터페이스 레벨에서 적용된 명령

a. 토폴로지에 사용된 통신 사업자가 점보 프레임을 허용하므로 MTU가 9216으로 설정되지만 이는 필수 사항은 아닙니다

b. macsec dot1q-in-clear 명령을 사용하면 VLAN(dot1q) 태그가 암호화되지 않은 암호화되지 않은 암호화되지 않은 암호화되지 않도록 옵션을 사용할 수 있습니다

c. macsec access-control should-secure 명령은 물리적 인터페이스 또는 하위 인터페이스에서 암호화되지 않은 패킷을 보내거나 받을 수 있게 합니다(일부 하위 인터페이스에서는 암호화가 필요하고 다른 인터페이스에서는 필요하지 않은 경우 이 명령은 MACsec이 활성화된 동일한 물리적 인터페이스에서 암호화되지 않은 패킷을 보내거나 받을 수 없도록 하는 기본 MACsec 동작 때문입니다)

하위 인터페이스 레벨에서 적용된 명령

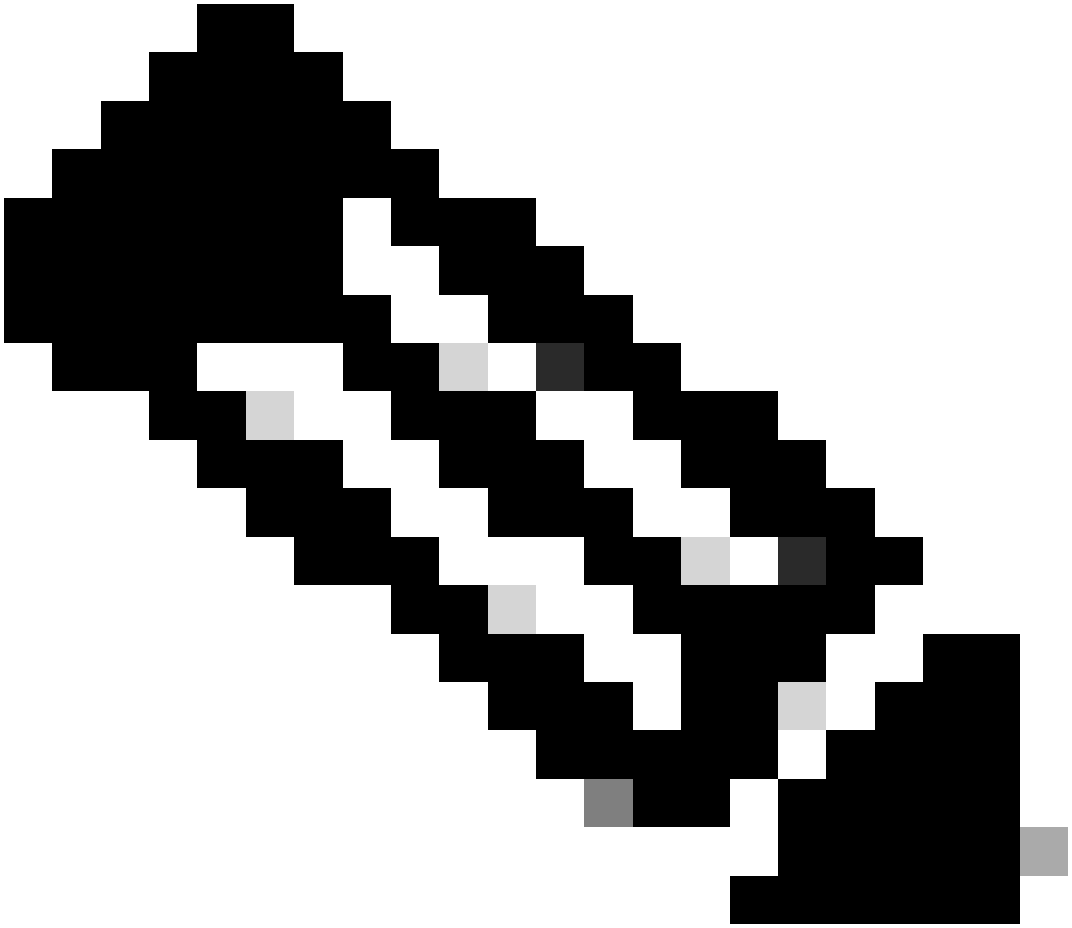
a. 이제 eapol destination-address broadcast-address 명령은 EAPoL 프레임의 대상 MAC 주소(기본적으로 멀티캐스트 MAC 주소 01:80:C2:00:00:03)를 브로드캐스트 MAC 주소로 변경하여 서비스 공급자가 플러딩하고 삭제하거나 소비하지 않도록 해야 합니다.

b. eapol eth-type 876F 명령을 사용하여 EAPoL 프레임의 기본 이더넷 유형(기본적으로 0x888E)을 변경하고 이를 0x876F로 변경합니다. 이는 통신 사업자가 이러한 프레임을 삭제하거나 사용하지 못하도록 하기 위해 다시 필요합니다.

c. mka policy <policy name> 및 mka pre-shared-key key-chain <key chain name> 명령은 사용자 지정 정책 및 키 체인을 하위 인터페이스에 적용하는 데 사용됩니다.

d. 마지막으로 macsec 명령은 하위 인터페이스 레벨에서 MACsec을 활성화합니다.

현재 설정에서는 이전 EAPoL 변경 없이 통신 사업자 측의 9500 스위치가 EAPoL 프레임을 전달하지 않았습니다.



참고: dot1q-in-clear 및 should-secure와 같은 MACsec 명령은 하위 인터페이스에서 상속됩니다. 또한 EAPoL 명령은 물리적 인터페이스 레벨에서 설정할 수 있으며, 이러한 경우 하위 인터페이스에서도 이러한 명령을 상속합니다. 그러나 하위 인터페이스에서 EAPoL 명령을 명시적으로 구성하면 해당 하위 인터페이스에 대한 상속된 값 또는 정책이 재정의됩니다.

다음을 확인합니다.

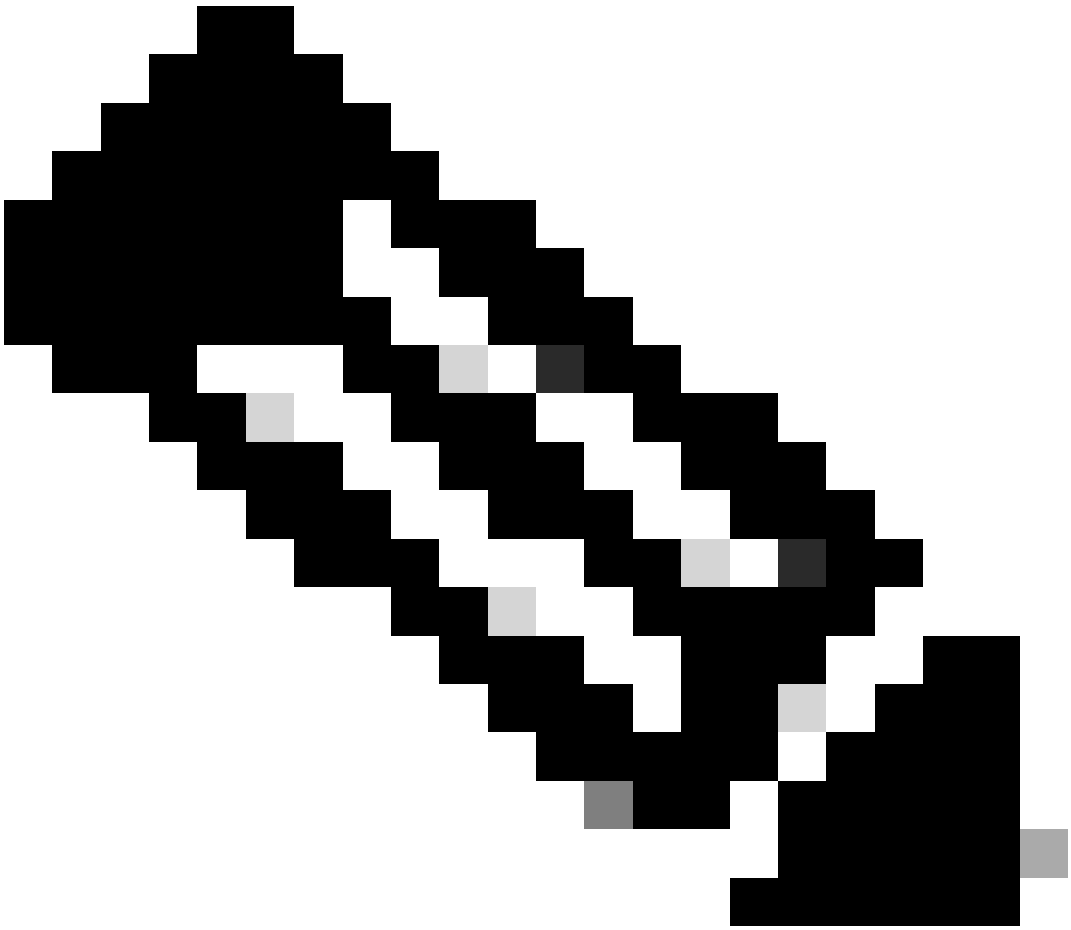
컨피그레이션이 적용되면 다음 출력에서는 각 CE(Customer Edge) C8500 라우터의 관련 실행 중

인 컨피그레이션을 보여줍니다(일부 컨피그레이션은 생략됨).

```
<#root>
8500-1#
show running-config

Building configuration...

Current configuration : 8792 bytes
!
!
version 17.14
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
!
hostname 8500-1
!
boot-start-marker
boot system flash bootflash:c8000aep-universalk9.17.14.01a.SPA.bin
boot-end-marker
!
!
no logging console
no aaa new-model
!
!

key chain keychain_vlan100 macsec key 01 cryptographic-algorithm aes-256-cmac key-string a5b2df4657bd8c

!
!
!
!
!
!
license boot level network-premier addon dna-premier
!
!
spanning-tree extend system-id
!

mka policy subint100 macsec-cipher-suite gcm-aes-xpn-256


!
!
!
!
!
!
cdp run
!
!
!
!
```

```
interface Loopback100
 ip address 192.168.100.10 255.255.255.0
!
interface Loopback200
 ip address 192.168.200.10 255.255.255.0
!
!

interface FortyGigabitEthernet0/2/4

 mtu 9216
 no ip address
 no negotiation auto
 cdp enable

 macsec dot1q-in-clear 1 macsec access-control should-secure

!

interface FortyGigabitEthernet0/2/4.100

 encapsulation dot1Q 100
 ip address 172.16.1.1 255.255.255.0


ip mtu 9184

 eapol destination-address broadcast-address eapol eth-type 876F mka policy subint100 mka pre-shared-ke

!

interface FortyGigabitEthernet0/2/4.200

 encapsulation dot1Q 200
 ip address 172.16.2.1 255.255.255.0
!
!
router eigrp 100
 network 172.16.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip forward-protocol nd
!
!
!
control-plane
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 login
 transport input ssh
!
!
!
!
!
```

```
!
end

8500-1#
```



참고: MACsec을 활성화한 후 macsec 명령을 적용하면 해당 인터페이스의 MTU가 자동으로 조정되고 MACsec 오버헤드를 고려하여 32바이트 감소됩니다.

다음으로 피어 간의 MACsec 상태를 확인하고 확인하는 데 사용할 수 있는 필수 명령 목록을 찾을 수 있습니다. 이 명령은 현재 MACsec 세션, 키 체인, 정책 및 통계에 대한 자세한 정보를 제공합니다.

show mka sessions - 이 명령은 현재 MKA 세션 상태를 표시합니다.

show mka sessions detail - 이 명령은 각 MKA 세션에 대한 자세한 정보를 제공합니다.

show mka keychains - 이 명령은 MACsec 및 할당된 인터페이스에 사용되는 키 체인을 표시합니다
.

show mka policy - 이 명령은 적용된 정책, 사용된 인터페이스 및 암호 그룹을 표시합니다.

show mka summary - 이 명령은 MKA 세션 및 통계의 요약을 제공합니다.

show macsec statistics interface <interface name> - 이 명령은 지정된 인터페이스에 대한 MACsec 통계를 보여주며, 암호화된 트래픽이 송수신되고 있는지를 식별하는 데 도움이 됩니다.

CE 8500-1

```
<#root>
8500-1#
show mka sessions


Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=========================================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server
Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN
=========================================================================================================
Fo0/2/4.100
     78bc.1aac.1521/001a
subint100
         NO                 NO
26
              78bc.1aac.1420/001a  1
Secured
            02


8500-1#
show mka sessions detail


MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

TX-SSCI.................. 2
Local Tx-SCI............. 78bc.1aac.1521/001a
Interface MAC Address.... 78bc.1aac.1521
MKA Port Identifier...... 26
Interface Name........... FortyGigabitEthernet0/2/4.100
Audit Session ID.........
```

```
CAK Name (CKN)..... 02
Member Identifier (MI)... 8387013B6C4D6106D4443285
Message Number (MN)..... 439243
EAP Role..... NA
Key Server..... NO

MKA Cipher Suite..... AES-256-CMAC


Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... F5720CC2E83183F1E673DACD00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)
SAK Rekey Time..... 0s (SAK Rekey interval not applicable)


MKA Policy Name..... subint100

Key Server Priority..... 0
Delay Protection..... NO
Delay Protection Timer..... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility..... 80C201
SAK Rekey On Live Peer Loss..... NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO

SAK Cipher Suite..... 0080C20001000004 (GCM-AES-XPN-256)

MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------
  F5720CC2E83183F1E673DACD  439222      78bc.1aac.1420/001a  0         YES            1

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority

Installed

  ------------------------------------------------------------------------------------

8500-1#

show mka keychains


MKA PSK Keychain(s) Summary...

Keychain         Latest CKN                                                    Interface(s)
Name             Latest CAK                                                    Applied
=============================================================================================
```

```
keychain_vlan100 02 Fo0/2/4.100


                <HIDDEN>

8500-1#
show mka policy


MKA Policy defaults :
         Send-Secure-Announcements: DISABLED

MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
================================================================================
*DEFAULT POLICY*  0    FALSE 0  FALSE TRUE   GCM-AES-128
                                             GCM-AES-256


subint100 0 FALSE 0 FALSE TRUE GCM-AES-XPN-256 Fo0/2/4.100




8500-1#
show mka summary


Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

================================================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server
Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN
================================================================================================================
Fo0/2/4.100     78bc.1aac.1521/001a  subint100         NO                 NO
26              78bc.1aac.1420/001a  1                 Secured            02



MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 14
   Fallback Secured............ 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 13
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0
```

```
SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 2
   SAKs Received............... 18
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics


MKPDUs Validated & Rx...... 737255

      "Distributed SAK"..... 18
      "Distributed CAK"..... 0


MKPDUs Transmitted......... 738485

      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0

MKPDU Failures
   MKPDU Tx............................... 0
   MKPDU Rx ICV Verification.............. 0
   MKPDU Rx Fallback ICV Verification..... 0
   MKPDU Rx Validation.................... 0
   MKPDU Rx Bad Peer MN................... 0
   MKPDU Rx Non-recent Peerlist MN........ 0
SAK USE Failures
   SAK USE Latest KN Mismatch............. 0
   SAK USE Latest AN not in USE........... 0
```

```
8500-1#

show macsec statistics interface Fo0/2/4.100

MACsec Statistics for FortyGigabitEthernet0/2/4.100
 SecY Counters
  Ingress Untag Pkts:       0
  Ingress No Tag Pkts:      0
  Ingress Bad Tag Pkts:     0
  Ingress Unknown SCI Pkts: 0
  Ingress No SCI Pkts:      0
  Ingress Overrun Pkts:     0
  Ingress Validated Octets: 0


Ingress Decrypted Octets: 11853398

  Egress Untag Pkts:        0
  Egress Too Long Pkts:     0
  Egress Protected Octets:  0


Egress Encrypted Octets: 11782598


 Controlled Port Counters
  IF In Octets:             14146226
  IF In Packets:            191065
  IF In Discard:            0
  IF In Errors:             0
  IF Out Octets:            14063174
  IF Out Packets:           190042
  IF Out Errors:            0

 Transmit SC Counters (SCI: 78BC1AAC1521001A)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       190048
 Transmit SA Counters (AN 0)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       190048

 Receive SA Counters (SCI: 78BC1AAC1420001A  AN 0)
  In Pkts Unchecked:        0
  In Pkts Delayed:          0
  In Pkts OK:               191069
  In Pkts Invalid:          0
  In Pkts Not Valid:        0
  In Pkts Not using SA:     0
  In Pkts Unused SA:        0
  In Pkts Late:             0
```

서로 다른 하위 인터페이스에서 성공적으로 연결하고 192.168.0.0/16 서브넷 간의 연결도 성공했습니다. 다음 ping 테스트에서는 성공적인 연결을 보여줍니다.

<#root>

8500-1#

ping 172.16.1.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#
```

ping 172.16.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#
```

ping 192.168.101.10 source 192.168.100.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.10, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#
```

PE(Provider Edge) 디바이스의 ICMP 테스트에서 패킷을 캡처한 후 암호화된 프레임과 암호화되지 않은 프레임을 비교할 수 있습니다. 이더넷 외부 MAC 헤더는 두 프레임에서 동일하며 dot1q 태그가 표시됩니다. 그러나 암호화된 프레임에는 0x88E5(MACsec)의 EtherType이 표시되고, 암호화되지 않은 프레임에는 ICMP 프로토콜 정보와 함께 0x0800(IPv4)의 EtherType이 표시됩니다.

암호화된 프레임 VLAN 100
<#root> F241.03.03-9500-1# **show monitor capture cap buffer detail | begin Frame 80** Frame 80: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface /tmp/epc_ws/wif_to Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe) Interface name: /tmp/epc_ws/wif_to_ts_pipe Encapsulation type: Ethernet (1) Arrival Time: Jul 29, 2024 23:50:16.528191000 UTC [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1722297016.528191000 seconds [Time delta from previous captured frame: 0.224363000 seconds] [Time delta from previous displayed frame: 0.224363000 seconds] [Time since reference or first frame: 21.989269000 seconds] Frame Number: 80 Frame Length: 150 bytes (1200 bits) Capture Length: 150 bytes (1200 bits) [Frame is marked: False] [Frame is ignored: False] **[Protocols in frame: eth:ethertype:vlan:ethertype:macsec:data]** **Ethernet II, Src: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21), Dst: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)** Destination: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)

```
       Address: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Source: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21)
       Address: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Type: 802.1Q Virtual LAN (0x8100) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100

   000. .... .... .... = Priority: Best Effort (default) (0)
   ...0 .... .... .... = DEI: Ineligible
   .... 0000 0110 0100 = ID: 100

Type: 802.1AE (MACsec) (0x88e5) 802.1AE Security tag

   0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
       0... .... = VER: 0x0
       .0.. .... = ES: Not set
       ..1. .... = SC: Set
       ...0 .... = SCB: Not set
       .... 1... = E: Set
       .... .1.. = C: Set
   .... ..00 = AN: 0x0
   Short length: 0

Packet number: 147 System Identifier: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21) Port Identifier: 26 ICV: 2

Data (102 bytes)

0000  99 53 71 3e f6 c7 9b bb 00 21 68 48 d6 ca 26 af   .Sq>.....!hH..&.
0010  80 a5 76 40 19 c9 45 97 b3 5a 48 d3 2d 30 72 a6   ..v@..E..ZH.-0r.
0020  96 47 6e a7 4c 30 90 e5 70 10 80 e8 68 00 5f ad   .Gn.L0..p...h._.
0030  7f dd 4a 70 a8 46 00 ef 7d 56 fe e2 66 ba 6c 1b   ..Jp.F..}V..f.l.
0040  3a 07 44 4e 5e e7 04 cb cb f4 03 71 8d 40 da 55   :.DN^......q.@.U
0050  9f 1b ef a6 3a 1e 42 c7 05 e6 9e d0 39 6e b7 3f   ....:.B.....9n.?
0060  f2 82 cf 66 f2 5b                                 ...f.[
    Data: 9953713ef6c79bbb00216848d6ca26af80a5764019c94597b^@&
    [Length: 102]
```

관련 정보

- WAN MACSEC 및 MKA 지원 개선 사항
- 고속(1-100GE) WAN 구축을 보호하는 혁신적인 이더넷 암호화(802.1AE - MACsec)
- 라우터에서 WAN MACSEC 문제 해결

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.