브리지 보안

목차

소개

이더넷 세그먼트 간에 연결 설정된 무선 링크를 설계할 때 보안은 매우 중요한 고려 사항입니다.이 문서에서는 IPSEC 터널을 사용하여 브리지 무선 링크를 통과하는 트래픽을 보호하는 방법을 설명합니다.

이 예에서는 두 개의 Cisco Aironet 350 Series 브리지가 WEP를 설정합니다.두 라우터가 IPSEC 터널을 설정했습니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 사항을 사용하는 데 익숙해야 합니다.

- Cisco Aironet Bridge 컨피그레이션 인터페이스
- Cisco IOS 명령줄 인터페이스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IOS 버전 12.1을 실행하는 Cisco 2600 Series 라우터
- 펌웨어 버전 11.08T를 실행하는 Cisco Aironet 350 Series 브리지

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 사

용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 이론

Cisco Aironet 340, 350 및 1400 Series 브리지는 최대 128비트 WEP 암호화를 제공합니다.WEP 알고리즘의 보안 및 Cisco Aironet Response to Press - 802.11 Security의 결함에 설명된 대로 WEP 알고리즘의 잘 알려진 문제와 익스플로잇의 용이성 때문에 보안 연결에 의존할 수 없습니다.

무선 브리지 링크를 통해 전달되는 트래픽의 보안을 강화하는 한 가지 방법은 링크를 통과하는 암호화된 라우터-라우터 IPSEC 터널을 생성하는 것입니다.이는 브리지가 OSI 모델의 레이어 2에서 작동하기 때문입니다.브리지 간 연결을 통해 IPSEC 라우터 간 라우터를 실행할 수 있습니다.

무선 링크의 보안이 침해된 경우 포함된 트래픽은 암호화된 상태로 안전합니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

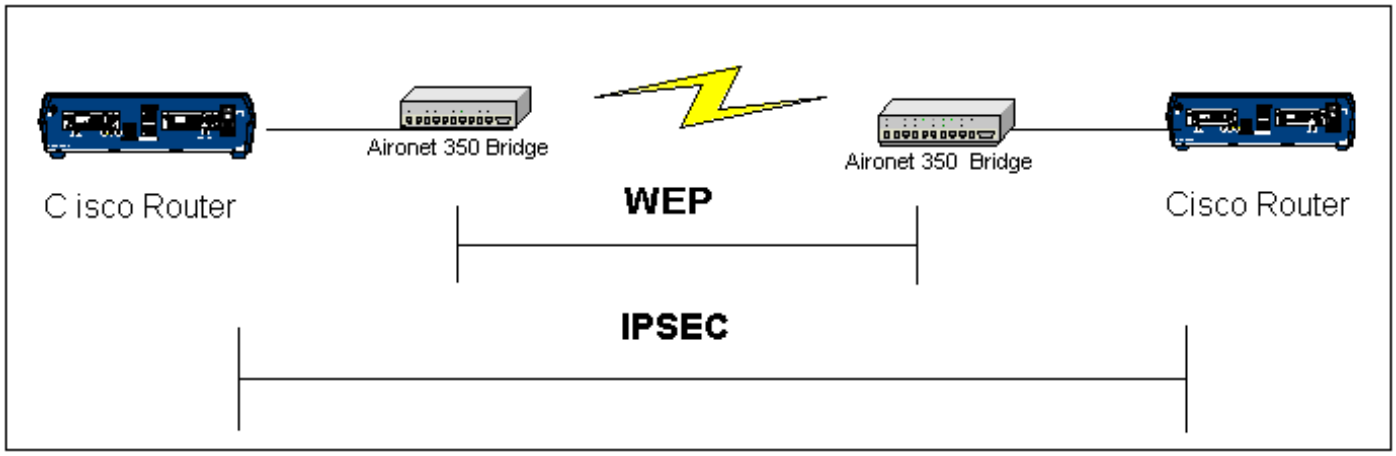
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 방법을 설명합니다.

참고: 이 문서에서 사용되는 명령에 대한 추가 정보를 찾으려면 IOS 명령 조회 도구를 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- 라우터A
- 라우터B
- 브리지 예

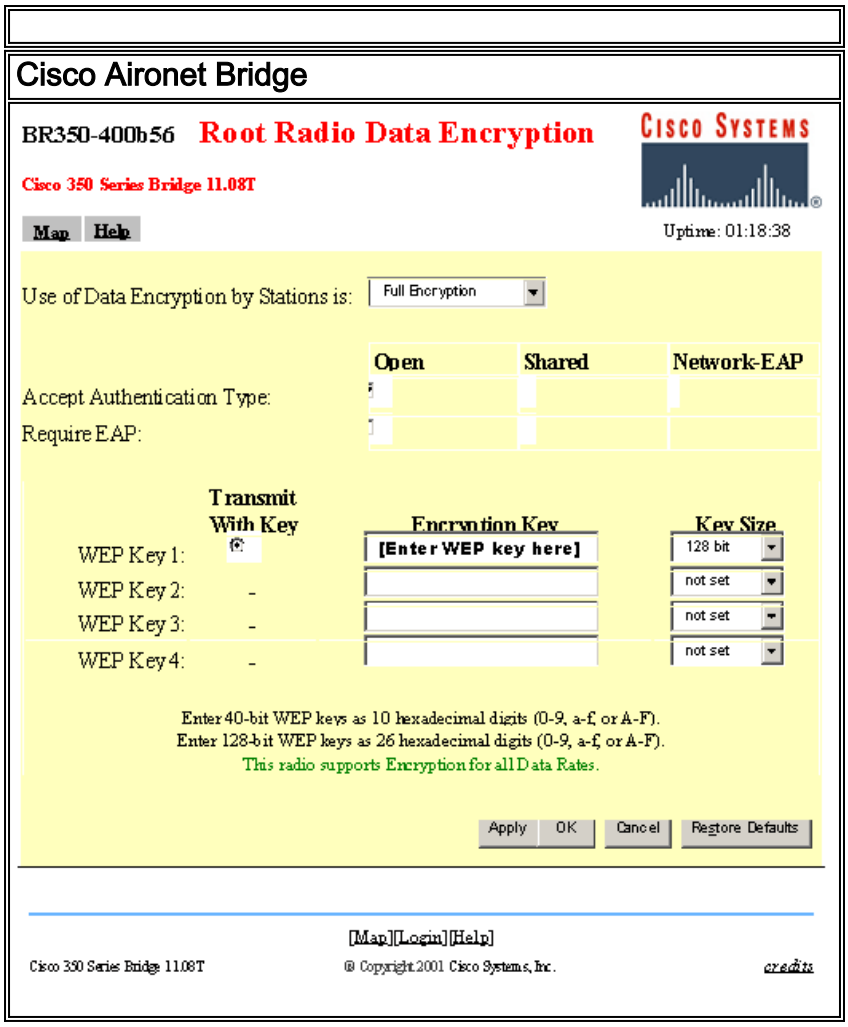
RouterA(Cisco 2600 라우터)

```
RouterA#show running-config
Building configuration...

Current configuration : 1258 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
ip dhcp excluded-address 10.1.1.20
ip dhcp excluded-address 10.1.1.30
!
ip dhcp pool wireless
 network 10.1.1.0 255.255.255.0
!
ip audit notify log
ip audit po max-events 100
call rsvp-sync
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco address 10.1.1.30
!
!
crypto ipsec transform-set set esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.30
set transform-set set
match address 120
!
interface Loopback0
ip address 20.1.1.1 255.255.255.0
!
interface Ethernet0
ip address 10.1.1.20 255.255.255.0
crypto map vpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.30
no ip http server
no ip http cable-monitor
!
access-list 120 permit ip 20.1.1.0 0.0.0.255 30.1.1.0
0.0.0.255
!
!
line con 0
transport input none
line vty 0 4
```

```
!
end
```

RouterB(Cisco 2600 라우터)

```
RouterB#show running-config
Building configuration...

Current configuration : 1177 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
!
ip audit notify log
ip audit po max-events 100
call rsvp-sync
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco address 10.1.1.20
!
!
crypto ipsec transform-set set esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.20
set transform-set set
match address 120
interface Loopback0
ip address 30.1.1.1 255.255.255.0
!
interface Ethernet0
ip address 10.1.1.30 255.255.255.0
no ip mroute-cache
crypto map vpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.20
no ip http server
no ip http cable-monitor
!
access-list 120 permit ip 30.1.1.0 0.0.0.255 20.1.1.0
0.0.0.255
!
!
line con 0
transport input none
line vty 0 4
login
!
end
```



다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show crypto engine connections active** - 이 명령은 현재 활성 암호화 세션 연결을 보는 데 사용됩니다.

```
RouterA#show crypto engine connection active
  ID Interface   IP-Address      State Algorithm              Encrypt Decrypt
   1 Ethernet0   10.1.1.20       set   HMAC_MD5+DES_56_CB           0       0
2002 Ethernet0   10.1.1.20       set   HMAC_MD5+3DES_56_C           0       3
2003 Ethernet0   10.1.1.20       set   HMAC_MD5+3DES_56_C           3       0

RouterB#show crypto engine connection active
  ID Interface    IP-Address      State Algorithm              Encrypt Decrypt
   1  <none>         <none>       set   HMAC_MD5+DES_56_CB           0       0
2000 Ethernet0    10.1.1.30       set   HMAC_MD5+3DES_56_C           0       3
2001 Ethernet0    10.1.1.30       set   HMAC_MD5+3DES_56_C           3       0
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

IPSEC 연결 문제를 해결하려면 다음을 참조하십시오.

- IP 보안 문제 해결 - 디버그 명령 이해 및 사용
- Cisco 네트워크 레이어 암호화 구성 및 문제 해결:IPSec 및 ISAKMP, 1부 및 2부

무선 연결 문제를 해결하려면 다음을 참조하십시오.

- TAC 케이스 수집 툴 - 무선 LAN
- 무선 브리지 네트워크로 일반적인 문제 해결
- 무선 LAN 네트워크에서 연결 문제 해결

관련 정보

- **기술 지원 - 무선 LAN**
- **기술 지원 - IPSec 협상/IKE 프로토콜**
- **Technical Support - Cisco Systems**