VG224 SCCP 보안 암호화 구성

목차

소개

이 문서에서는 보안 암호화 구성에 대해 설명합니다. VG224 아날로그 게이트웨이의 SCCP(Signaling Connection Control Part)

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SCCP
- VG224
- Cisco CUCM(Unified Communications Manager)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- VG224

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

구성

1단계. callmanager.pem 인증서를 VG224에 복사합니다(아래 컨피그레이션에서 SECURE 신뢰 지점으로 참조).

2단계. MAC 주소가 FastEthernet0/0(바인드 인터페이스)인 VG224에 주체 이름으로 마지막 10자리만 사용하는 자체 서명 인증서를 생성합니다.

3단계. vg-cert를 통화 관리자 트러스트로 CUCM에 복사하고 CUCM을 다시 시작합니다.

이 정보는 VG224에 필요한 인증서 구성에 제공됩니다.

```
Router(config)#crypto key generate rsa general-keys label vg modulus 1024
Router(config)#crypto pki trustpoint vg
Router(ca-trustpoint)#enrollment selfsigned
serial-number none
fqdn none
ip-address none
subject-name cn=1A:E2:85:7B:E2  <----- Last 10 DIGITS ONLY of the SCCP bind interface.
Formatting EXACTLY as shown with colons.
rsakeypair vg
crypto pki enroll vg
Router(config)#crypto pki export vg_cert pem terminal
```

팁: 명령 참조 안내서

참고: 주의 사항 CSCti08882 때문에 보안 VG224 아날로그 폰에서 보안 IP 폰으로 전화를 걸 때 잠금 아이콘이 표시되지 않습니다

다음을 확인합니다.

이 정보는 VG224를 성공적으로 등록하기 위한 것입니다.

```
Router#show sccp
SCCP Admin State: UP
Gateway Local Interface: FastEthernet0/0
        IPv4 Address: 14.1.97.95
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 172.18.172.204, Port Number: 2000
        Priority: N/A, Version: 7.0, Identifier: 1
        Trustpoint: N/A
Call Manager: 172.18.172.205, Port Number: 2000
        Priority: N/A, Version: 7.0, Identifier: 2
        Trustpoint: N/A
Call Manager: 172.18.172.206, Port Number: 2000
        Priority: N/A, Version: 7.0, Identifier: 3
        Trustpoint: N/A

AutoCfg_Virtual_Endpoint Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 172.18.172.204, Port Number: 2000
TCP Link Status: CONNECTED, Device Name: AN1AE2857BE2FFF
Reported Max Streams: 0, Reported Max OOS Streams: 0
Supported Codec: g711ulaw, Maximum Packetization Period: 20

Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 172.18.172.204, Port Number: 2443
TCP Link Status: CONNECTED, Device Name: AN1AE2857BE2400
Security
 Signaling Security: ENCRYPTED TLS
Media Security: SRTP
Supported crypto suites :AES_CM_128_HMAC_SHA1_32
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
```

```
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: ilbc, Maximum Packetization Period: 120
TLS : ENABLED
```

이것은 SCCP IOS 컨피그레이션을 사용하는 보안 VG224를 보여줍니다.

```
Building configuration...


Current configuration : 5258 bytes
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system slot0:vg224-i6k9s-mz.151-4.M3
boot-end-marker
!
!
enable secret 5 $1$f99B$PWPClPrUNzgsUZEO8aBYG.
!
no aaa new-model
crypto pki token default removal timeout 0
!
crypto pki trustpoint SECURE
 enrollment terminal
 revocation-check crl
!
crypto pki trustpoint vg
 enrollment selfsigned
 serial-number none
 fqdn none
 ip-address none
 subject-name cn=1A:E2:85:7B:E24       ( instead of this command,  we can use hiddle command
"mac-address Fast Ethernet0/0 as well )
 revocation-check crl
 rsakeypair AN1AE2857BE2400
!
!
crypto pki certificate chain SECURE
 certificate ca 588C9B7C2D4B37F03930E8C926D02A18
   <truncated>
crypto pki certificate chain vg certificate self-signed 03 <truncated> ip source-route ! ip cef
ip name-server 172.18.108.43 ip name-server 172.18.108.34 ! ! no ipv6 cef ! stcapp ccm-group 1
stcapp security trustpoint vg stcapp security mode encrypted stcapp ! stcapp feature access-code
! stcapp feature speed-dial ! ! ! stcapp supplementary-services port 2/0 fallback-dn 862224 ! !
! ! ! ! ! ! ! voice-card 0 ! ! ! ! ! ! ! ! ! ! interface FastEthernet0/0 ip address dhcp duplex
auto speed auto ! interface FastEthernet0/1 no ip address duplex auto speed auto ! ip forward-
protocol nd ! ip http server no ip http secure-server ip route 0.0.0.0 0.0.0.0 14.1.97.1 254 ip
route 0.0.0.0 0.0.0.0 14.1.97.1 254 ! ! ! control-plane ! ! voice-port 2/0 timeouts initial 60
timeouts interdigit 60 timeouts ringing infinity ! voice-port 2/1 ! <truncated>
! voice-port 2/23 ! ccm-manager config server 172.18.172.204 ccm-manager config ccm-manager sccp
local FastEthernet0/0 ccm-manager sccp ! ! mgcp profile default ! sccp local FastEthernet0/0
sccp ccm 172.18.172.204 identifier 1 version 7.0 sccp ccm 172.18.172.205 identifier 2 version
7.0 sccp ccm 172.18.172.206 identifier 3 version 7.0 sccp ! sccp ccm group 1 associate ccm 1
priority 1 associate ccm 2 priority 2 associate ccm 3 priority 3 ! dial-peer voice 999200 pots
service stcapp securiy mode encrypted =====> Required command
 port 2/0
```

```
!
dial-peer voice 99920 pots
! service stcapp

securiy mode encrypted   =====> Required command
 port 2/1
!
!(configure all ports in same secure mode)
!
line con 0
line aux 0
line vty 0 4
 password ww
 login
 transport input all
!
ntp server 172.18.108.15
end
```