

VG224 SCCP-Verschlüsselung konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfung](#)

Einleitung

Dieses Dokument beschreibt die sichere verschlüsselte Konfiguration. SCCP (Signaling Connection Control Part) am analogen VG224-Gateway.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SCCP
- VG 224
- Cisco Unified Communications Manager (CUCM)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- VG 224

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: Kopieren Sie das callmanager.pem-Zertifikat in den VG224 (in der nachfolgenden Konfiguration als SECURE Trustpoint bezeichnet)

Schritt 2: Erstellen Sie auf dem VG224 ein selbstsigniertes Zertifikat mit der MAC-Adresse von FastEthernet0/0 (Bindungsschnittstelle), wobei nur die letzten 10 Ziffern als Bettname verwendet werden.

Schritt 3: Kopieren Sie das vg-cert in CUCM als Call-Manager Trust und starten Sie CUCM neu.

Die Informationen werden für die Konfiguration von Zertifikaten bereitgestellt, die für VG224 erforderlich sind.

```
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.
rsa-keypair vg
crypto pki enroll vg
Router(config)#crypto pki export vg_cert pem terminal
```

Tipp: [Befehlsreferenz](#)

Anmerkung: Wenn Sie von einem sicheren analogen VG224-Telefon an ein sicheres IP-Telefon anrufen, wird aufgrund eines Vorbehalts [CSCti0882](#) kein Sperrsymbol angezeigt.

Überprüfung

Diese Informationen dienen zur Überprüfung der erfolgreichen Registrierung von VG224.

```
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

Dies zeigt, dass das sichere VG224 mit der SCCP-IOS-Konfiguration verwendet wird.

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$PWPC1PrUNzgsUZE08aBYG.  
!  
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
```