Configurar seguro VG224 SCCP cifrado

Índice

Introdução

Este documento descreve a configuração cifrada segura que sinaliza a peça de controle da conexão (SCCP) no gateway analógico VG224.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SCCP
- VG224
- Gerente das comunicações unificadas de Cisco (CUCM)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- VG224

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Configurar

Etapa 1. Copie o certificado callmanager.pem ao VG224 (provido como SE FIXA o ponto confiável na configuração abaixo)

Etapa 2. Crie um certificado assinado do auto no VG224 com o MAC address do FastEthernet0/0 (relação do ligamento) com somente os últimos dígitos 10 como o assunto-nome.

Etapa 3. Copie o vg-CERT a CUCM como uma confiança do gerenciador de chamada e reinicie CUCM.

A informação é fornecida para a configuração dos Certificados que são exigidos para o VG224.

```
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
```

> Dica: Guia de referência de comando

> Nota: Você não verá um ícone do fechamento ao chamar de um telefone analógico VG224 seguro a um telefone IP seguro devido à advertência CSCti08882

Verificar

Esta informação é para a verificação para o registro bem-sucedido do VG224

```
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
```

Isto mostra esse VG224 seguro usando a configuração do IOS SCCP.

```
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
```