Configurez sécurisé du SCCP VG224 chiffré

Contenu

Introduction

Ce document décrit la configuration chiffrée sécurisée signalant la partie commande de connexion (SCCP) sur la passerelle de l'analogue VG224.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- VG224

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Configurez

Étape 1. Copiez le certificat callmanager.pem sur le VG224 (référencé comme SÉCURISENT le point de confiance dans la configuration ci-dessous)

Étape 2. Créez un certificat signé d'individu sur le VG224 avec l'adresse MAC de FastEthernet0/0 (bind interface) avec seulement les 10 derniers chiffres comme subject-name.

Étape 3. Copiez le vg-CERT sur CUCM comme confiance d'appel-gestionnaire et redémarrez CUCM.

Les informations sont données pour la configuration des Certificats qui sont exigés pour 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
```

Conseil : Guide de référence des commandes

Remarque: Vous ne verrez pas une icône de verrouillage quand appelant d'un téléphone analogique VG224 sécurisé à un téléphone IP sécurisé dû à la mise en garde CSCti08882

Vérifiez

Ces informations sont pour la vérification pour l'enregistrement réussi de 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
```

Ceci affiche à cela VG224 sécurisé utilisant la configuration IOS de 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
```