Configurar CGR 1000 com o CGOS para o desenvolvimento zero do toque

Índice

Introdução

Este documento descreve as etapas de configuração exigidas para registrar com sucesso o roteador conectado Cisco 1000 da grade (CGR 1000) com sistema operacional conectado da grade (CGOS) para colocar o diretor da rede (FND) como um dispositivo do campo. Antes que um roteador esteja registrado ao FND, deve encontrar diversas condições prévias que incluem a infraestrutura chave do registro em público (PKI) e a configuração personalizada. Além do que isto, uma configuração de exemplo sanitized será incluída.

Contribuído pelo arqueiro de Ryan, engenheiro de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Server de aplicativo 1.0 ou instalada mais atrasada e ser executado CG-NMS/FND com o acesso da Web UI disponível.
- Servidor proxy do servidor de provisionamento do túnel (TP) instalado e ser executado.
- Server de base de dados Oracle instalado e configurado corretamente.
- setupCgms.sh é executado com sucesso pelo menos uma vez com um db_migrate principiante bem sucedido.
- Server DHCPv4 e DHCPv6 já configurados e disponíveis com os ajustes do proxy salvar no **Admin >** página dos **ajustes do abastecimento da** relação de usuário de web FND (UI).
- O arquivo do dispositivo .csv deve já ter sido importado ao FND e o dispositivo deve estar no estado “inaudito”.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FND 3.0.1-36
- SS com base no software (também 3.0.1-36)
- as cgms-ferramentas empacotam instalado no server de aplicativo (3.0.1-36)
- Todos os servidores Linux que executam RHEL 6.5
- Todos os Windows Server que dirigem a empresa R2 de Windows Server 2008
- CSR 1000v que é executado em um VM como o roteador de extremidade principal
- CGR-1120/K9 usados como o roteador de área de Fied (DISTANTE) com CG-OS 4(3)

Um ambiente de laboratório controlado FND foi usado durante a criação deste documento. Quando outras disposições diferirão, você deve aderir a todos os requisitos mínimos dos Guias de Instalação.

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configuração e registro passo a passo

1. Configurar o hostname do dispositivo.

2. Configurar o Domain Name.

3. Configurar os server DNS.

4. Configurar e verifique time/NTP.

5. Traga acima os cartões e/ou as interfaces Ethernet celulares. Assegure-se de que todas as relações necessárias tenham seu IPs e que o roteador tem um Gateway of Last Resort.
Para que o FND provision com sucesso a relação de Loopback0, deve já ser criado com os endereços. Crie a relação de Loopback0 e verifique que tem endereços do IPv4 e do IPv6. Você pode usar o” IPs descartável porque será substituído após o abastecimento do túnel.

6. Permita estas características: NTP, ike cripto, DHCP, túnel, virtual-túnel cripto do IPsec.

7. Crie seu perfil do registro do ponto confiável (esta é a URL direta para o Web page do registro do protocolo simple certificate enrollment (SCEP) em seu Certificate Authority (CA) RSA. Se você usa uma autoridade de registro, a URL será diferente):

```
Router(config)#crypto ca profile enrollment LDevID_Profile
Router(config-enroll-profile)#enrollment url
http://networkdeviceenrollmentserver.your.domain.com/CertSrv/mscep/mscep.dll
```

8. Crie seu ponto confiável e ligue-lhe o perfil do registro.

```
Router(config)#crypto ca trustpoint LDevID
Router(config-trustpoint)#enrollment profile LDevID_Profile
Router(config-trustpoint)#rsakeypair LDevID_Keypair 2048
Router(config-trustpoint)#revocation-check none
Router(config-trustpoint)#serial-number
Router(config-trustpoint)#fingerprint
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
```

9. Autentique seu ponto confiável com o server SCEP.

```
Router(config)#crypto ca authenticate LDevID
  Trustpoint CA authentication in progress. Please wait for a response...
  2017 Mar  8 19:02:00 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_CA_AUTHENTICATE_OK: Trustpoint
LDevID: CA certificates(s) authenticated.
```

10. Registre sua infraestrutura da chave do ponto confiável em público (PKI).

```
Router(config)#crypto ca enroll LDevID
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Challenge password:
Re-enter challenge password:
The serial number in the certificate will be: PID:CGR1120/K9 SN:JAF#############
Certificate enrollment in progress. Please wait for a response...
2017 Mar  8 19:02:24 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_ENROLL_OK: Trustpoint LDevID:
Device identity certificate successfully enrolled to CA.
```

11. Verifique sua corrente do ceritifcate.

```
Router#show crypto ca certificates
```

12. Configurar os parâmetros de SNMP exigidos para que Callhome trabalhe corretamente.

```
Router(config)#snmp-server contact NAME
Router(config)#snmp-server user admin network-admin
Router(config)#snmp-server community PUBLIC group network-operator
```

13. Configurar estes ajustes pessoais do módulo da rede de área da tecnologia Wireless básica (WPAN).

```
Router(config)#interface wpan 4/1
Router(config-if)#no shutdown
Router(config-if)#panid 5
Router(config-if)#ssid meshssid
Router(config-if)#ipv6 add 2001:db8::1/32
```

14. Como o FND confia em Netconf sobre o HTTPS para controlar FARs, permita e configurar apropriadamente o servidor HTTPS para escutar na porta 8443 e de autenticar conexões com o PKI.

```
Router(config)#ip http secure-server
Router(config)#ip http secure-server trustpoint LDevID
Router(config)#ip http secure-port 8443
```

15. Configurar seu perfil do callhome.

```
Router(config)#callhome
Router(config-callhome)#email-contact email@domain.com
Router(config-callhome)#phone-contact +1-555-555-5555
Router(config-callhome)#streedaddress TEXT
Router(config-callhome)#destination-profile nms
Router(config-callhome)#destination-profile nms format netconf
Router(config-callhome)#destination-profile nms transport-method http
Router(config-callhome)#destination-profile nms http https://tpsproxy.your.domain.com:9120
Router(config-callhome)#enable
```

16. Salve a configuração.

17. Neste momento, tudo que você tem que fazer é recarregar o roteador mas se você quer começar manualmente o registro sem um reload você pode configurar o cgdm:

```
Router(config)#cgdm
Router(config-cgdm)#registration start trustpoint LDevID
```

Configuração de exemplo

Está aqui uma configuração sanitized tomada de um CGR1120 imediatamente antes de ZTD bem sucedido (neste ambiente de laboratório a relação Ethernet2/2 foi usada como a fonte preliminar do túnel de IPsec):

```
version 5.2(1)CG4(3)
logging level feature-mgr 0
hostname YOUR-HOSTNAME
vdc YOUR-HOSTNAME id 1
   limit-resource vlan minimum 16 maximum 4094
   limit-resource vrf minimum 2 maximum 4096
   limit-resource u4route-mem minimum 9 maximum 9
   limit-resource u6route-mem minimum 24 maximum 24
   limit-resource m4route-mem minimum 58 maximum 58
   limit-resource m6route-mem minimum 8 maximum 8
feature ntp
feature crypto ike
feature dhcp
feature tunnel
feature crypto ipsec virtual-tunnel
username admin password YOURPASSWORD role network-admin
username Administrator password YOURPASSWORD role network-admin
ip domain-lookup
ip domain-name your.domain.com
ip name-server x.x.x.x
crypto key param rsa label LDevID_keypair modulus 2048
crypto key param rsa label YOUR-HOSTNAME.your.domain.com modulus 2048
crypto ca trustpoint LDevID
   enrollment profile LDevID_Profile
   rsakeypair LDevID_keypair 2048
   revocation-check none
   serial-number
   fingerprint xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
crypto ca profile enrollment LDevID_Profile
   enrollment url http://x.x.x.x/CertSrv/mscep/mscep.dll
snmp-server contact NAME
snmp-server user Administrator network-admin
snmp-server community public group network-operator
callhome
   email-contact ciscotac@cisco.tac.com
   phone-contact +1-555-555-5555
   streetaddress Here
   destination-profile nms
   destination-profile nms format netconf
   destination-profile nms transport-method http
   destination-profile nms http https://tpsproxy.your.domain.com:9120 trustpoint LDevID
   destination-profile nms alert-group all
   enable
ntp server x.x.x.x
ntp server x.x.x.x
crypto ike domain ipsec
vrf context management
vlan 1
service dhcp
ip dhcp relay
line tty 1
line tty 2
```

```
interface Dialer1
interface Ethernet2/1
interface Ethernet2/2
   ip address x.x.x.x/30
   no shutdown
interface Ethernet2/3
interface Ethernet2/4
interface Ethernet2/5
interface Ethernet2/6
interface Ethernet2/7
interface Ethernet2/8
interface loopback0
   ip address 1.1.1.1/32
   ipv6 address 2001:x:x::80/128
interface Serial1/1
interface Serial1/2
interface Wpan4/1
   no shutdown
   panid 20
   ssid austiniot
   ipv6 address 2001:db8::1/32
interface Wifi2/1
clock timezone CST -6 0
clock summer-time CST 2 Sun Mar 02:00 1 Sun Nov 02:00 60
line console
line vty
boot kickstart bootflash:/cgr1000-uk9-kickstart.5.2.1.CG4.3.SPA.bin
boot system bootflash:/cgr1000-uk9.5.2.1.CG4.3.SPA.bin
ip route 0.0.0.0/0 x.x.x.x
feature scada-gw
scada-gw protocol t101
scada-gw protocol t104
ip http secure-port 8443
ip http secure-server trustpoint LDevID
ip http secure-server
cgdm
   registration start trustpoint LDevID
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.