제로 터치 구축을 위한 CGOS를 사용하여 CGR 1000 구성

목차

소개

이 문서에서는 CGOS(Connected Grid Operating System)에 Cisco CGR 1000(Connected Grid Router 1000)을 FND(Field Network Director)에 필드 디바이스로 성공적으로 등록하는 데 필요한 컨피그레이션 단계를 설명합니다.라우터가 FND에 등록되기 전에 PKI(Public Key Infrastructure) 등록 및 사용자 지정 컨피그레이션을 포함하는 몇 가지 전제 조건을 충족해야 합니다.이 외에도 삭제된 샘플 컨피그레이션이 포함됩니다.

기고자: Cisco TAC 엔지니어 Ryan Bowman

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CG-NMS/FND 애플리케이션 서버 1.0 이상이 설치되어 웹 UI 액세스를 사용하여 실행 중입니다.
- TPS(Tunnel Provisioning Server) 프록시 서버가 설치 및 실행되고 있습니다.
- Oracle 데이터베이스 서버가 설치되고 올바르게 구성되었습니다.
- setupCgms.sh가 첫 번째 db_migrate에 성공하여 한 번 이상 성공적으로 실행되었습니다.
- DHCPv4 및 DHCPv6 서버는 이미 구성되었으며 FND UI(웹 사용자 인터페이스)의 **Admin(관리)** > Provisioning Settings(프로비저닝 설정) 페이지에 저장된 프록시 설정과 함께 사용할 수 있습니다.
- 디바이스 .csv 파일을 FND로 이미 가져와야 하며 디바이스가 'unnoted' 상태여야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FND 3.0.1-36
- 소프트웨어 기반 SSM(3.0.1-36)
- 응용 프로그램 서버에 설치된 cgms-tools 패키지(3.0.1-36)
- RHEL 6.5를 실행하는 모든 Linux 서버
- Windows Server 2008 R2 Enterprise를 실행하는 모든 Windows 서버
- VM에서 헤드 엔드 라우터로 실행되는 CSR 1000v
- CG-OS 4(3)에서 FAR(Fixed Area Router)로 사용되는 CGR-1120/K9

이 문서를 작성하는 동안 제어된 FND 랩 환경이 사용되었습니다.다른 구축은 다르지만 설치 가이드의 최소 요구 사항을 모두 준수해야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

단계별 구성 및 등록

1. 디바이스 호스트 이름을 구성합니다.

2. 도메인 이름을 구성합니다.

3. DNS 서버를 구성합니다.

4. 시간/NTP를 구성하고 확인합니다.

5. 셀룰러 카드 및/또는 이더넷 인터페이스를 불러옵니다.필요한 모든 인터페이스에 해당 IP가 있고 라우터에 마지막 사용 게이트웨이가 있는지 확인합니다.
FND가 루프백 0 인터페이스를 성공적으로 프로비저닝하려면 주소를 사용하여 이 인터페이스를 이미 생성해야 합니다.Loopback 0 인터페이스를 만들고 IPv4 및 IPv6 주소가 있는지 확인합니다.터널 프로비저닝 후 교체되기 때문에 Throwhowway" IP를 사용할 수 있습니다.

6. 다음 기능을 활성화합니다.ntp, crypto ike, dhcp, tunnel, crypto ipsec virtual-tunnel.

7. 신뢰 지점 등록 프로필을 만듭니다(CA(RSA Certificate Authority)에서 SCEP(Simple Certificate Enrollment Protocol) 등록 웹 페이지의 직접 URL입니다. 등록 기관을 사용하는 경우 URL이 달라집니다.

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

8. 신뢰 지점을 생성하고 등록 프로파일을 해당 지점에 바인딩합니다.

```
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. SCEP 서버로 신뢰 지점을 인증합니다.

```
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. PKI(Public Key Infrastructure)에 신뢰 지점을 등록합니다.

```
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. 인증서 체인을 확인합니다.

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

12. Callhome이 올바르게 작동하려면 필요한 SNMP 매개변수를 구성합니다.

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

13. 이러한 기본 WPAN(Wireless Personal Area Network) 모듈 설정을 구성합니다.

```
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. FND는 HTTPS를 통한 Netconf를 사용하여 FAR을 관리하고, 포트 8443에서 수신 대기하며 PKI와의 연결을 인증하도록 HTTPS 서버를 활성화 및 적절히 구성합니다.

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

15. callhome 프로필을 구성합니다.

```
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. 구성을 저장합니다.

17. 이 시점에서는 라우터를 다시 로드하기만 하면 되지만 다시 로드 없이 수동으로 등록을 시작하려면 cgdm을 구성할 수 있습니다.

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

샘플 컨피그레이션

다음은 ZTD가 성공하기 직전에 CGR1120에서 가져온 무결성 컨피그레이션입니다(이 랩 환경에서는 Ethernet2/2 인터페이스가 기본 IPSec 터널 소스로 사용됨).

```
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
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.