Configurez CGR 1000 avec CGOS pour le déploiement nul de toucher

Contenu

Introduction

Ce document décrit l'étape nécessaire de configuration pour enregistrer avec succès le routeur 1000 (CGR 1000) de grille connecté par Cisco avec le système d'exploitation connecté de grille (CGOS) pour mettre en place le directeur de réseau (FND) comme périphérique de champ. Avant qu'un routeur soit enregistré au FND, il doit rencontrer plusieurs conditions préalables qui incluent l'inscription en Infrastructure à clés publiques (PKI) et configuration personnalisée. En plus de ceci, une configuration d'échantillon assainie sera incluse.

Contribué par l'archer de Ryan, ingénieur TAC Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveur d'applications 1.0 ou installé postérieur et s'exécuter CG-NMS/FND avec l'accès du Web UI disponible.
- Percez un tunnel le serveur proxy du serveur de mise en service (TPS) installé et s'exécuter.
- Serveur de base de données d'Oracle installé et correctement configuré.
- setupCgms.sh fonctionnent avec succès au moins une fois avec un db_migrate pour la première fois réussi.
- Serveurs DHCPv4 et DHCPv6 déjà configurés et disponibles avec des paramètres de proxy enregistrés sur la **page Settings d'admin > de ravitaillement de l'**interface utilisateur d'utilisateur web FND (UI).
- Le fichier du périphérique .csv devrait avoir été déjà importé au FND et le périphérique devrait être dans l'état « inentendu ».

Composants utilisés

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

- FND 3.0.1-36
- SSM articulé autour d'un logiciel (aussi 3.0.1-36)
- les cgms-outils empaquettent installé dans le serveur d'applications (3.0.1-36)
- Tous les serveurs Linux exécutant RHEL 6.5
- Tous les Windows Server exécutant l'entreprise R2 des Windows Server 2008
- Exécution CSR 1000v sur une VM comme routeur de tête de réseau
- CGR-1120/K9 utilisés en tant que routeur de région de Fied (LOINTAIN) avec CG-OS 4(3)

Un environnement de travaux pratiques commandé FND a été utilisé pendant la création de ce document. Tandis que d'autres déploiements différeront, vous devriez adhérer à toutes les conditions requises minimum des guides d'installation.

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configuration et inscription pas à pas

1. Configurez l'adresse Internet de périphérique.

2. Configurez le domain-name.

3. Configurez les serveurs de DN.

4. Configurez et vérifiez time/NTP.

5. Évoquez les cartes et/ou les interfaces Ethernet cellulaires. Assurez-vous que toutes les interfaces requises ont leur IPS et que le routeur a une passerelle de dernier recours.
Pour que le FND provision avec succès le bouclage 0 interfaces, il doit déjà être créé avec des adresses. Créez le bouclage 0 interfaces et le vérifiez qu'elle a des adresses d'ipv4 et d'IPv6. Vous pouvez utiliser le » IPS jetable parce qu'ils seront remplacés après ravitaillement de tunnel.

6. Activez ces caractéristiques : ntp, crypto IKE, DHCP, tunnel, crypto virtuel-tunnel d'ipsec.

7. Créez votre profil d'inscription de point de confiance (c'est l'URL direct pour la page Web simple d'inscription de Protocol d'inscription de certificat (SCEP) sur votre Autorité de certification (CA) RSA. Si vous utilisez une autorité d'enregistrement, l'URL sera différent) :

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

8. Créez votre point de confiance et liez le profil d'inscription à lui.

```
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. Authentifiez votre point de confiance avec le serveur 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. Inscrivez-vous votre point de confiance dans l'Infrastructure à clés publiques (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. Vérifiez votre chaîne de ceritifcate.

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

12. Configurez les paramètres SNMP requis pour que le callhome fonctionne correctement.

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

13. Configurez ces configurations de base de module du réseau personnel sans fil (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. Comme le FND se fonde sur Netconf au-dessus de HTTPS pour gérer FARs, enable et pour configurer convenablement le serveur HTTPS pour écouter sur le port 8443 et pour authentifier des connexions avec le PKI.

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

15. Configurez votre profil de 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. Enregistrez la configuration.

17. En ce moment, tout que vous devez faire est de recharger le routeur mais si vous voulez commencer manuellement l'enregistrement sans recharge vous peut configurer le cgdm :

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

Exemple de configuration

Voici une configuration assainie prise d'un CGR1120 juste avant ZTD réussi (dans cet environnement de travaux pratiques l'interface Ethernet2/2 a été utilisée comme source du tunnel primaire d'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
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.