

نود نم رشنلل CGOS عم CGR 1000 نيوكت سمل

تايوتحملا

[عمدقملا](#)
[قيساسالا تابلطتلا](#)
[تابلطتلا](#)
[عمدختسملا تانوكملا](#)
[قوخطب قوخط ليچستلاو نيوكتلا](#)
[نيوكتلا نم قنيغ](#)
[قحصللا نم ققحتلا](#)
[احال صلاو عاخطالا فاشكتسا](#)

عمدقملا

1000 قلاصتلا عكبشلا هجوم ليچستلا قبولطملا نيوكتلا تاوخط دنتسملا اذه فصلي عكبشلا ريديملا (CGOS) قلاصتلا عكبشلا ليغشت ماطن عم حاجنب Cisco نم (CGR 1000) نأ بجي، قلاصتلا قودنصللا هجوملا ليچست لبقي. لقح زاحك (FND) قيناديلا قيساسالا قينبلا في ليچستلا نمضتت يتلا قيساسالا تابلطتلا نم ديدعل يبللي مت جذومن نيومتيتي، كلذل قلاصتلا ابو. صصخملا نيوكتلاو (PKI) ماعلا حاتفملا هريهطت.

Cisco نم TAC سندنهم، ناموب نياري لبقي نم قماسملا تمت.

قيساسالا تابلطتلا

تابلطتلا

قيلاتلا عيضاوملاب قفرعم كيديل نوكت نأ Cisco قيصوت

- لوصوللا عم ليغشتلا ديقتو تبثم ثدحأ رادصا وأ CG-NMS/FND 1.0 قيبطت مداخل رفوتي ببوللا مدختسم قهجاو لا.
- هليغشتو Tunnel Provisioning Server (TPS) ليكو مداخل تبثت مت.
- قححص لكشب هنيوكتو Oracle تانايب قداق مداخل تبثت مت.
- قرملا حاجنب db_migrate عم لقالا قلع قداقو قرم حاجنب setupCgms.sh ليغشت متي قلاو.
- ليكولا تاداعلا عم لقلااب ارفوتمو DHCPv4 و DHCPv6 (مداوخ) مداخل نيوكت مت.
- FND ب قلاصلا بيومدختسم قهجاو قحفضي قرفوتلا تاداعلا Admin > قلع قظوفحملا (UI).
- زاوجللا نوكتي نأ بجي و FND قلاو لقلااب هداريتسا مت دق زاوجللا csv. فلم نوكتي نأ بجي

"عومسم ريغ" ةلاح يف

ةمدختسملا تانوكملا

ةيالاتلا ةيداملا تانوكملا وجوماربلا تارادصا ىلإ دنتسمل اذه يف ةدراول تامولعمل دنتست

• 3,0,1-36 ت.د

• (3.0.1-36 اضيأ) جوماربلا ىلإ ةدنتسمل SSM

• (3.0.1-36) تاقبطل مداخل يف ةتبثمل CGMS تاودأ ةمزنح

• 6.5 رادصا RHEL مازنب لمعت يتلا Linux مداوخ عيمج

• Windows Server 2008 R2 Enterprise ليغشتلا مازنب لمعت يتلا Windows مداوخ ةفاك

• يئاهن هجومي VM زاهج ىلع لمعت CSR 1000V

• CG-OS 4(3) عم (FAR) ةجدم ةقطنم هجومي CGR-1120/K9 مدختس

نأ نم مغرلا ىلع. دنتسمل اذه عاشنإ ءانثأ اهب مكحتمل FND ربتخم ةئيبي مادختسا مت نم ايندلا تابلطتملا عيمجب مازتلالا كيلىل بجي هنأ الا، فلتختس ىرخألا رشنلا تايلىم عتبتلا ةلدأ

ةصاخ ةيلىم عم ةئيبي يف ةدوجوملا ةزهجألا نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضارتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسُملا ةزهجألا عيمج تادب رما يأل لمحتمل ريثأتلل كمهف نم دكأتف، ةرشابم كتكبش

ةوطخب ةوطخ ليچستلا ونيوكتلا

1. زاهجال فيضم مسا نيوكتب مق

2. domain-name نيوكتب مق

3. DNS (مداوخ) مداخل نيوكتب مق

4. هنم ققحتلا و NTP/تقولا نيوكت

5. ةرورضل تاهجاو عيمج نأ نم دكأت. تنرتي تاهجاو وأ/و ةيولخل فاتاوהל تاقاطب بلج. ةريخألا ةلواحمل ةباب هيدل هجومل نأ وهب ةصاخلا IP نيوانع ىلع يوتحت مق. نيوانعل مادختساب لعفلاب اهؤاشنإ بجي، 0 عاچرتسالا ةهجاو حانج نب FND رفوت نأ لجا نم مادختسا كنكمي IPv4 و IPv6 نيوانع ىلع يوتحت اهنأ نم ققحت و 0 عاچرتسالا ةهجاو عاشنإب قفنلا ديوزت دعبل اهلادبتسا متيس هنأل "ةلجترملا" IP نيوانع

6. ntp, crypto ike, dhcp, tunnel, crypto ipSec virtual-tunnel: تازيمل هذه نيكمتب مق

7. بيولا ءحفصل رشابم URL ناوئع وه اذه) ةقثل ةطقن ليچست فيرعت فلم عاشنإب مق. (CA) RSA ةداهش عجرم ىلع (SCEP) طيسبلل ةداهشل ليچست لوكتورب ليچستب ةصاخلا (افلتخم URL نوكتيسف، "ليچست عجرم" مدختست تنك اذا)

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

8. اهب ليچستال فيرعت فلم طبروكب ةصاخال ةقثال ةطقن ءاشناب مق.

```
Router(config)#crypto ca trustpoint LDevID
Router(config-trustpoint)#enrollment profile LDevID_Profile
Router(config-trustpoint)#rsa keypair 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:xx:xx
```

9. SCEP مادخ م ادختساب كب ةصاخال TrustedPoint ةقداصم.

```
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: C
```

10. (PKI) ماعال حات فملل ةيساسال ةينبالا في كب ةصاخال ةقثال ةطقن ليچست.

```
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 ident
```

11. تاتيبيسلال ةلسلس نم ققحت.

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

12. حيحص لكشب لمعلل CallHome ل ةبولطمال SNMP تاملعم نيوكتب مق.

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

13. هذو (WPAN) ةيكل سلال ةي صخش ل ةكبش ل ةي طمن ل ةدحول ادادع ني وكتب مق 13.

```
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. ةدي عبل لوصول طاقن ةرادال HTTPS ربع NetConf ل ع دمت عي قودنصل نأ ل ارظنو - 14 امك ، بسانم لكش ب هني وكتو 8443 ذفنم ل ل ع عامت سلال نم HTTPS م داخ نكمي هناف PKI. عم تالاصتال ةقداصم ل ع دمت عي

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

15. يسيئرل اءاعدت سلال في رعت فلم ني وكتب مق 15.

```
Router(config)#callhome
Router(config-callhome)#email-contact email@domain.com
Router(config-callhome)#phone-contact +1-555-555-5555
Router(config-callhome)#streetaddress 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. ني وكتل ظفح 16.

17. ادب ديرت تنك اذ نكلو هجوم ل لي محت ةداع وه ب مايقل ل ك ل ع ام لك ، ةطقنل هذو دن ع 17. CGDM: ني وكت كنكمي ف ، لي محت ةداع نود ايودي لي جستال

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

ني وكتل نم ةني ع

ربتخم ل ةئي ب ي ف) ةرشابم حج انل ZTD ل بق CGR1120 نم ذوخأم ل طعم ني وكت ي لي امي ف

(يېسىسأل IPsec قفن ردىصمك Ethernet2/2 ةهچاومادختسإ مت ،هذه

```
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
rsa-keypair 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: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 austinot
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

```

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل عاجا ايلاح دجوي ال

اهحالصا و عاطاخا ل فاشكتسا

نيوكتلا اذهل اهلحالصا و عاطاخا ل فاشكتسا ل ةدحتم تامولعم ايلاح رفوتت ال

ةمچرتل هذه ل و ح

ةيلآل تاي نقتل ن م ة و م ج م م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا