Elabore los archivos del .csv (Comma Separated Value) para importar los nuevos dispositivos en FND

Contenido

Introducción

Este documento describe los pasos para elaborar el archivo del .csv para el director de la red del campo (FND). Para proporcionar la Administración de redes segura, el FND no proporciona la detección y el registro automáticos o dinámicos del activo. Antes de que un nuevo dispositivo se pueda agregar a un despliegue FND una entrada de la base de datos única se debe crear para ella importando un archivo de encargo del .csv vía la interfaz del Web User (UI).

Este artículo proporciona las plantillas del .csv que se pueden utilizar y personalizar para agregar los nuevos puntos finales, routeres de área del campo o routeres de centro distribuidor a una solución existente. Además de esto, cada campo de la base de datos (DB) será definido y explicado para ayudar con el diseño y la implementación de los nuevos dispositivos.

> Nota: Antes de que esta guía pueda ser utilizada, usted debe tener una solución conectada de configuración completa y instalada del sistema de administración de red de la rejilla (CG-NMS) /FND.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidor de aplicaciones 1.0 o haber instalado posterior y el ejecutarse CG-NMS/FND con el acceso de la red UI disponible.

- Servidor proxy del servidor de aprovisionamiento del túnel (TP) instalado y el ejecutarse.
- Servidor de base de datos Oracle instalado y configurado correctamente.
- setupCgms.sh se ejecuta con éxito por lo menos una vez con un db_migrate por primera vez acertado.
- Usted puede todavía utilizar esta guía si usted todavía no ha instalado y ha configurado sus servidores del DHCP pero se aconseja fuertemente que antes de que usted utilice este documento su organización ha planeado completamente hacia fuera los esquemas de direccionamiento del IPv4 y del IPv6 para el despliegue. Esto incluye las longitudes del prefijo y los rangos para los túneles IPsec del IPv4, los túneles del Generic Routing Encapsulation (GRE) del IPv6 y se dobla stack que dirige en los loopback conectados del router de la rejilla (CGR).
- También fuertemente se aconseja que usted ha comprado o está planeando ya comprar por lo menos a 1 router de centro distribuidor, por lo menos 1 router de área del campo y por lo menos 1 punto final/contador.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FND 3.0.1-36
- SS basado en software (también 3.0.1-36)
- las cgms-herramientas empaquetan instalado en el servidor de aplicaciones (3.0.1-36)
- Todos los servidores Linux que ejecutan RHEL 6.5
- Todos los Servidores Windows que dirigen la empresa 2008 del r2 del Servidor Windows
- La nube de Cisco mantiene al router (CSR) 1000v que se ejecuta en un VM como router de centro distribuidor
- CGR-1120/K9 usados como router de área del campo (LEJANO) con CG-OS 4(3)

Un ambiente de laboratorio controlado FND fue utilizado durante la creación de este documento. Mientras que diferenciarán otras implementaciones, usted debe adherirse a todos los requerimientos mínimos de las guías de instalación.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

archivos del .csv para agregar los dispositivos en FND

LEJOS

Esta plantilla se puede utilizar para LEJOS que se introducen a la solución por primera vez. Esto será situada en los **dispositivos > la** página de los **dispositivos del campo**. En el campo los dispositivos paginan, hacen clic en el menú dropdown de la **importación global** y selecto **agregue los dispositivos**.

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunne
lDestAddr1,adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhc
```

pV4TunnelLink,dhcpV6TunnelLink,dhcpV4LoopbackLink,dhcpV6LoopbackLink

Identificador del elemento (eid) - Esto es un Identificador único usado para identificar el dispositivo en los mensajes del registro así como el GUI. Para prevenir la confusión, se recomienda que su organización desarrolla un esquema EID. El esquema recomendado es utilizar el número de serie de IDevID CGR como el EID. En este Routers, el número de serie utilizará esta fórmula: PID+SN. Por ejemplo: .

deviceType - Esto se utiliza para identificar la plataforma de hardware o la serie. Para 1120 y 1240 modelos, el valor del deviceType debe ser cgr1000.

tunnelHerEid - Debido al hecho de que el FND no prohiba a uso de 2 el suyo que se ejecuta en los pares HA o independiente, el campo del tunnelHerEid se utiliza para identificar al cual ELLA los túneles VPN en este CGR terminará. Este valor será simplemente el EID del apropiado ELLA.

certIssuerCommonName - Este campo es un requisito del despliegue cero del tacto (ZTD) y es generalmente lo mismo que el nombre DNS de su Certificate Authority de la raíz RSA. Si usted no conoce el Common Name, usted puede encontrarlo y funcionar con el comando show crypto ca certificates. En el encadenamiento para el trustpoint de LDevID, usted ve el Common Name del emisor de la raíz en el asunto del 'certificado de CA 0'. Alternativamente, usted puede acceder simplemente la página de los Certificados del FND y mirar el certificado raíz.

meshPrefixConfig - Este valor se asigna a la interfaz de módulo WPAN. Todo el CGEs que forman un árbol del lenguaje del política de ruteo (RPL) con este router recibe una dirección IP vía el DHCP (el relé DHCP asumido se configura apropiadamente) con este valor como el Prefijo de red.

tunnelSrcInterface1 - Para las implementaciones que utilizan los túneles IPsec primarios y secundarios, este valor es el nombre de la interfaz del origen de túnel para sus túneles primarios (tales como cellular4/1). Si hay un túnel de reserva entonces usted asignará la interfaz de origen agregando un valor para tunnelSrcInterface2. Si usted tiene solamente 1 conexión WAN entonces usted utilizará solamente el campo tunnelSrcInterface1.

ipsecTunnelDestAddr1 - Este valor es la dirección de destino del túnel del IPv4 para el túnel IPsec primario con la interfaz de origen asignada a tunnelSrcInterface1.

adminUsername - Éste es el nombre de usuario que el FND utilizará cuando usted abre el HTTPS y las sesiones de Netconf en LEJOS. Se requiere que el AAA da los permisos completos o está configurado este usuario localmente con el papel red-admin.

adminPassword - La contraseña para la cuenta del adminUsername. Usted puede ver este nombre de usuario en el GUI y navegar a la lengueta de las propiedades de los Config de la página del dispositivo y mirar “nombre de usuario del administrador” en “la sección de las credenciales del router”. Para evitar los errores, esta contraseña se debe primero cifrar con el Signature_Tool del paquete de las cgms-herramientas RPM. Esta herramienta cifra cualquier cosa

en el sólo texto usando la Cadena de certificados en el cgms_keystore. Para utilizar la herramienta de la firma, cambie el directorio a /opt/cgms-tools/bin/ en el servidor de aplicaciones FND. Después, cree un nuevo archivo de .txt del sólo texto que contenga el adminPassword. Una vez que usted tiene el archivo de texto, funcione con este comando:

```
./signature-tool encrypt /opt/cgms/server/cgms/conf/cgms_keystore password-file.txt
```

Copia/goma la salida cifrada en el campo del adminPassword de su archivo del .csv. Es una buena idea borrar con seguridad el archivo de contraseña del sólo texto cuando usted acaba para utilizar la herramienta de la firma.

cgrusername1 - Esta cuenta de usuario no se requiere, pero si configuran a los usuarios múltiples con diversos papeles en el CGR, usted puede agregar otra cuenta de usuario aquí. Es importante saber que solamente el adminUsername y el adminPassword serán utilizados para la Administración del dispositivo. En esta configuración de laboratorio, utilice las mismas credenciales que el adminUsername.

cgrpassword1 - La contraseña para el usuario cgrusername1.

IP - Éste es el IP de administración primario. Cuando los ping o las trazas se ejecutan del FND utilizarán este IP. Enviarán las sesiones HTTP para el administrador de dispositivo conectado de la rejilla (CGDM) a este IP también. En una instalación típica, ésta será la dirección IP asignada a su interfaz tunnelSrcInterface1.

meshPanidConfig - La CACEROLA ID asignada a la interfaz WPAN de este CGR.

wifiSsid - El SSID configurado en la interfaz WPAN.

dhcpV4TunnelLink - El direccionamiento del IPv4 que el FND utilizará en su petición del proxy al servidor DHCP. En este ambiente de laboratorio, el servidor DHCP es Cisco Network Registrar (CNR) y el pool del IPSec DHCPv4 se configura para arrendar las subredes de /31. Si usted utiliza el primer IP en una subred disponible de /31 para su valor dhcpv4TunnelLink entonces el FND provision automáticamente los IP de la subred de punto a punto al tunnel0 CGR y el túnel correspondiente HER.

dhcpV6TunnelLink - El direccionamiento del IPv6 que el FND utiliza en su petición del proxy al servidor DHCP para el túnel del Generic Routing Encapsulation (GRE) del IPv6. En este ambiente de laboratorio, el CNR se configura para arrendar los direccionamientos con el uso de los prefijos de /127. Apenas como el dhcpV4TunnelLink, el FND provision automáticamente el 2do IP de la subred de punto a punto al ELLA cuando usted configura su túnel GRE.

dhcpV4LoopbackLink - El direccionamiento del IPv4 que el FND utilizará en sus peticiones del proxy al servidor DHCP al configurar la interfaz del loopback0 del CGR. En este ambiente de laboratorio, configuraron al agrupamiento DHCP correspondiente en el CNR para arrendar las subredes de /32.

dhcpV6LoopbackLink - El direccionamiento del IPv6 que el FND utilizará en sus peticiones del proxy al servidor DHCP cuando usted configura la interfaz del loopback0 del CGR. En este ambiente de laboratorio, el pool correspondiente fue configurado para arrendar las subredes de /128.

Router de centro distribuidor (ELLA)

Cuando usted agrega a un router de centro distribuidor por primera vez, esta plantilla puede ser utilizada:

```
eid,deviceType,name,status,lastHeard,runningFirmwareVersion,ip,netconfUsername,netconfPassword
```

deviceType - Cuando usted introduce un ASR o un CSR, el valor 'asr1000 se debe utilizar en este campo.

estatus - Los valores de estado validados son inauditos, abajo y suben. Utilice inaudito si es una nueva importación.

lastheard - Si esto es un nuevo dispositivo, este campo se puede dejar en blanco.

runningFirmwareVersion - Este valor se puede dejar en blanco también pero si usted quiere importar la versión, utiliza el número de la versión de la línea muy superior de la **demostración version output**. Por ejemplo, en esta salida, la cadena '03.16.04b.S debe ser utilizada:

```
Router#show version
Cisco IOS XE Software, Version 03.16.04b.S - Extended Support Release
```

netconfUsername - El nombre de usuario del usuario configurado para tener acceso completo Netconf/SSH al ELLA.

netconfPassword - La contraseña para el usuario especificada en el campo del netconfUsername.

Punto final conectado de la rejilla (CGE)

Para agregar un nuevo punto final de la malla al DB es muy simple. Esta plantilla puede ser utilizada:

```
EID,deviceType,lat,lng
```

deviceType - En este ambiente de laboratorio, el “cgmesh” fue utilizado para agregar un contador elegante como CGE.

lat - El coordenada de la latitud de GPS donde el CGE será instalado.

gasero - La longitud de GPS.

Ejemplos

Adición LEJANA:

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunne
lDestAddr1,
adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhcpV4TunnelLi
nk,
dhcpV6TunnelLink,dhcpV4LoopbackLink,dhcpV6LoopbackLink CGR1120/K9+JAF########,cgr1000,ASR1006-
X+JAB##########,root-ca-common-name,2001:db8::/32,cellular3/1,
192.0.2.1,Administrator,ajfiea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl,Administrator,
ajfiea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl,198.51.100.1,5,meshssid,203.0.113.1,2001:d
b8::1,
209.165.200.225,2001:db8::90FE
```

SU adición:

```
eid,deviceType,name,status,lastHeard,runningFirmwareVersion,ip,netconfUsername,netconfPassword
ASR1006-X+JAB##########,CSR1000V+JAB########,asr1000,CSR1000V+JAB########,unheard,,,192.0.2.1,
Administrator,ofhel35s804502gagh=
```

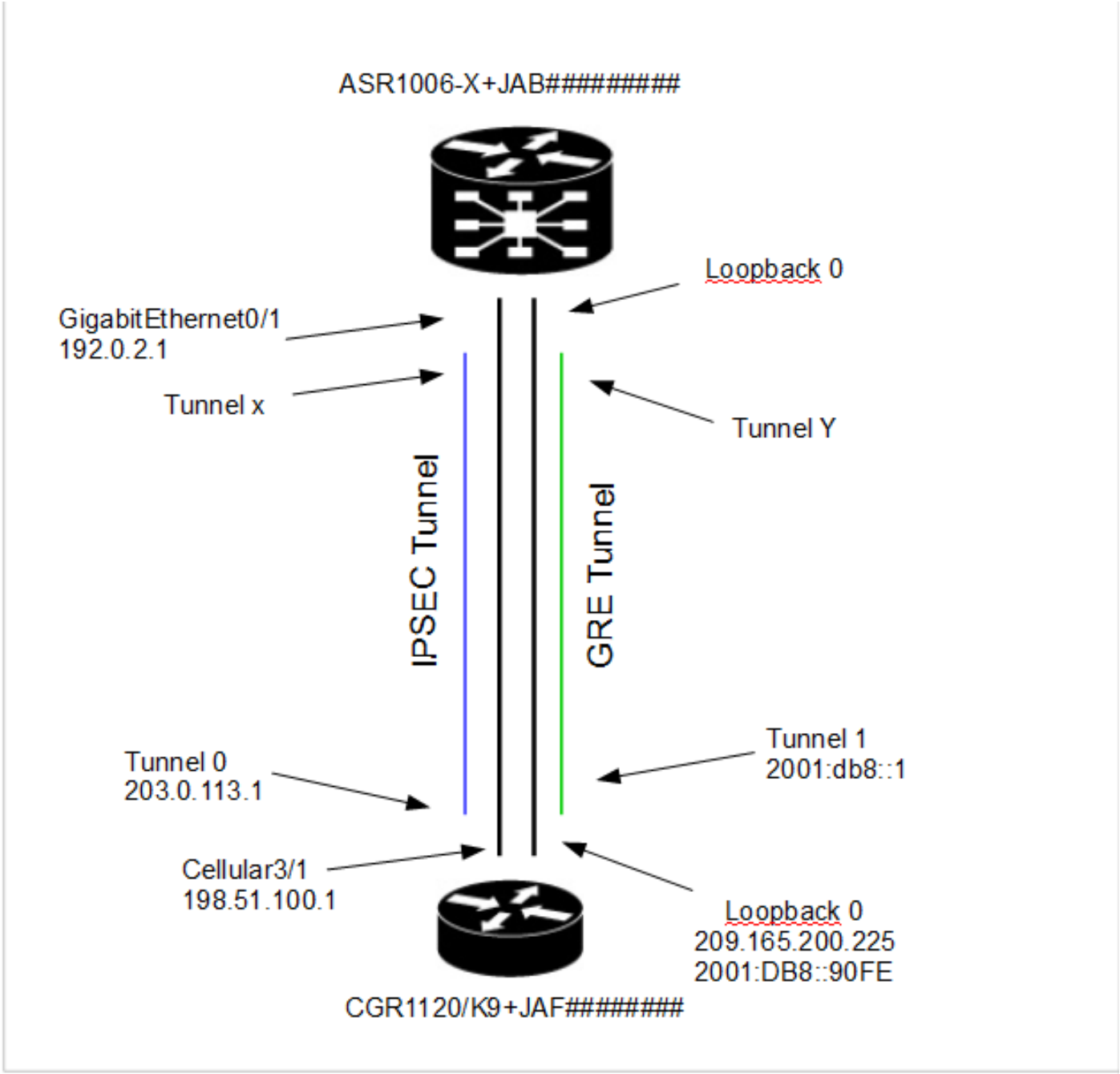
Adición CGE:

```
EID,deviceType,lat,lng
###############,cgmesh,64.434562,-102.750984
```

Diagrama de la red

> Nota: Trabajos del aprovisionamiento del túnel basados diferentemente encendido si a LEJOS está ejecutando CG-OS o el IOS. CG-OS: Una nueva interfaz del túnel IPsec será configurada en LEJOS y ELLA. El FND enviará una petición del proxy al servidor DHCP para 2 IP por el túnel y configurará el 2do IP automáticamente en la interfaz del túnel correspondiente. IOS: ELLA utilizará una plantilla Flexión-VPN que utilice un túnel IPsec de la punta a de múltiples puntos. Con esta configuración, solamente el FARs recibe las nuevas interfaces del túnel.

En este Diagrama de topología “túnel x” refiere a la interfaz relativa del túnel IPsec en ELLA mientras que el “túnel Y” corresponde con el túnel GRE construido apagado del Loopback Interface en ELLA. Además, los IP y las interfaces en el diagrama corresponden directamente a los ejemplos de configuración en las plantillas del .csv.


ASR1006-X+JAB########
Loopback 0
GigabitEthernet0/1
192.0.2.1
Tunnel x
Tunnel Y
IPSEC Tunnel
GRE Tunnel
Tunnel 0
203.0.113.1
Tunnel 1
2001:db8::1
Cellular3/1
198.51.100.1
Loopback 0
209.165.200.225
2001:DB8::90FE
CGR1120/K9+JAF########