Fortinet Security Fabric

Con Fortinet Security Fabric nos permite interconectar nuestros equipos para reunir, analizar y responder a eventos de seguridad que ocurran en nuestra red en tiempo real.

Configuración

Hay que habilitar FortiTelemetry en todos los interfaces que conecten con otros dispositivos fortinet y en el interfaz de la central que conecta a internet

Para habilitar la sincronización en el fortigate destino

```
config sys csf
  set configuration-sync default
end
```



si tenemos problemas de sincronización de objetos deberemos de poner set configuratio-sync local. Renombrar objetos y volver a activar set configuration-sync default

Manualmente poner los valores del Security Fabric de una oficina remota

Si queremos que una oficina no tome automaticamente los valores, sino configurarlos manualmente ejecutaremos

```
config system csf
    set configuration-sync local
end
```

Para configurar los valores iremos a **Security Fabric > Settings** y podremos elegir manualmente dichos parámetros

Conexión Security Fabric mediante túnel ipsec

https://fortixpert.blogspot.com/2019/05/fortios-62-security-fabric-over-ipsec.html

Hay que asignarles una ip a los extremos del túnel ipsec, activar el security fabric en los interfaces del túnel y permitir el tráfico desde las ip de origen del túnel ipsec al fortianalyzer .



Esas ips que ponemos en la interfaz del túnel es la que va a usar para conectarse al fortigate raíz

Tenemos que tener en cuenta que como ip de origen va a usar la que tenga el túnel ipsec

Debug

```
diag debug reset
diag debug app csf -1
diag debug enable
```

Problemas con los logs

Si tenemos varios equipos en el Security Fabric y vemos que un equipo no está enviando los logs al fortianalyzer, debemos de ejecutar en el fortigate que no los envía los siguientes comandos, para desactivar y volver a activar la sincronización

```
    config system csf
        set configuration-sync local
    end
```

Esperamos a que se sincronice el cluster y volvemos a poner la conexión por defecto

```
    config system csf
        set configuration-sync default
    end
```

Referencias

- https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/629879/system-csf
- https://cookbook.fortinet.com/category/collections/security-fabric/
- https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/327890/deploying-security-fabric
- https://fortixpert.blogspot.com/2019/05/fortios-62-security-fabric-over-ipsec.html
- https://fortixpert.blogspot.com/2020/05/sincronizacion-de-objetos-en-security.html
- https://kb.fortinet.com/kb/documentLink.do?externalID=FD49192
- https://community.fortinet.com/t5/FortiGate/Technical-Tip-Disable-re-enable-automatic-synchronization-of-the/ta-p/191082

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=hardware:fortigate:fabric

Last update: **092023/05/ 09:45**