fortigate, faq

FAQ

Campo Action

Cuando estamos mirando los logs de un fortigate, en las columnas aparece denominado **Acción (Action)**, que indica que acción ha tomado el cortafuegos. Las acciones pueden ser :

- **DENY** . El firewall ha bloqueado este tráfico por una política de seguridad
- **START** Si hemos activado la opción de registrar todas las sesiones en la política de seguridad se generará un log en el inicio de su procesamiento, que implica además que el trafico está permitido.

Aparecerán dos logs para cada sesión, uno será el de start y otro con una acción permitida

- **ACCEPT** Conexión establecida correctamente.
- **DNS** Host desconocido.
- **IP-CONN** El host remoto no es alcanzable o no responde.
- **TIMEOUT** La conexión ha finalizado de forma anómala, porque ha sido reseteada o ha llegado al timeout.
- **CLOSE** Conexión finalizada

- https://docs.fortinet.com/uploaded/files/2050/FortiOS_LogReference_v5.2.1.pdf
- https://fortixpert.blogspot.com/2015/09/campo-action-de-los-logs-de-fortigate.html

Ver la configuración

```
show
```

Ver las ips asignadas por DHCP

Abrimos la consola CLI

```
config system interface
edit ?
```

Reiniciar

```
execute reboot
```

Si queremos buscar algo en la configuración usuaríamos **show | grep f texto_a_buscar**. Por ejemplo

```
show | grep -f interface
```

Recuperar contraseña

En caso de que necesitemos poner una nueva contraseña en nuestro fortigate:

- Accedemos físicamente desde la consola del propio aparato
- Nada más salir el login poner user: maintainer y password: bcpb<nºde serie>
- Ya estaremos en modo admin FORTIGATE#

https://cookbook.fortinet.com/resetting-a-lost-admin-password/

Cambiar velocidad de un interfaz

Para saber a que velocidad está trabajando un interfaz

```
get system interface physical
```

Para forzar una velocidad

```
config system interface
edit "WAN1"
set speed 1000full
end
```

Autenticación

Se deben de poner las políticas de red por enciama de las de Grupos de Usuarios

Tracear una política determinada

Muchas veces queremos ver que tráfico pasa por una regla determinada para ello hacemos lo siguiente:

1. Vamoas a Policy y editamos la regla que queremos tracear y habilitamos la opción **log all sessions** y guardamos los cambios.
2. Pinchamos con el botón derecho del ratón sobre la fila de descripción de cada columna
3. En column Settings seleccionamos ID para saber el id de esa política
4. Una vez habilitada dicha opción para esa regla vamos a Log&Report→ Traffic Log→ Forward Traffic
5. Pinchamos con el botón derecho del ratón sobre la fila de descripción de cada columna
6. En column Settings seleccionamos Policy ID

7. Ahora al pinchar sobre la columna Policy Id ponemos como valor el número de la política que queremos tracear

Vdom

Entrar en la vdom correcta antes de efecturar algún cambio

```
config global
config vdom
edit <nombre_vdom>
```

VPN

Comandos para mostrar las conexiones de VPN

```
get vpn ike gateway <name>
get vpn ipsec tunnel name <name>
get vpn ipsec tunnel details
diagnose vpn tunnel list
diagnose vpn ipsec status
get router info routing-table all
```

Para resetear una conexión

```
diag vpn tunnel reset <nombre fase1>
```

Comandos de debug para VPN

```
diagnose debug reset
diagnose vpn ike log-filter clear
diagnose vpn ike log-filter ?
diagnose vpn ike log-filter dst-addr4 xxx.xxx.xxx.xxx
diagnose debug app ike 255          #muestra la salida de la fase1 y fase2
diagnose debug enable
```

Para deshabilitar el debug

```
diagnose debug disable
```

Sflow

http://www.soportejm.com.sv/kb/index.php/article/como-configurar-sflow-en-un-fortigate

Certificados con dispositivos IOS

http://docs.fortinet.com/uploaded/files/1023/provision-certificates-to-ios-devices-technical-note.pdf

Factory Reset

```
exec factoryreset
```

- https://kb.fortinet.com/kb/documentLink.do?externalID=FD37052

Desde la versión 6.0 tenemos un nuevo comando **factoryreset2**

Resetea la configuración a los valores por defecto exceptuando los valores de VDOM, interfaces, y las rutas estáticas

```
execute factoryreset2
```

Log

En los nuevos modelos de fortigate que no tienen el disco duro, no se puede ver ciertos logs relaciones con denegaciones de políticas. Esto es debido a que por defecto el nivel mínimo de aviso está configurado como **warning**. Si queremos ver en el propio fortigate esos logs de avisos sobre accesos denegados debemos de cambiar el nivel de log a **information** para ello:

```
config log memory filter
set severity information
end
```

```
execute log filter reset
execute log filter category event
execute log filter field            #presionar enter para ver opciones
execute log filter field dstport 8001
execute log filter view-lines 1000
execute log filter start-line 1
execute log display
```

Referencias

- https://blog.webernetz.net/cli-commands-for-troubleshooting-fortigate-firewalls/