fortigate

Fortigate

Demos de los programas : https://www.fortianalyzer.com , www.fortimanager.com, www.fortigate.com
user→demo
contraseña: nombre del producto

Comandos

Ver la configuración de red

```
show system interface
```

Rutas

```
get route info routing
show route static
```

Rendimiento

Para ver el rendimiento

```
CLI# diagnose sys top
```

Si el equipo está usando más del 80% de la memoria puede que el equipo entre en modo conservador. Para comprobarlo ejecutamos

```
diag hardware sysinfo shm
```

```
SHM counter:     14690663
SHM allocated:  158756864
SHM total:     7609556992
conservemode:           0
shm last entered:     n/a
system last entered:  n/a
SHM FS total:  7768129536
SHM FS free:   7602745344
SHM FS avail:  7602745344
SHM FS alloc:   165384192
```

Si como es el caso conservemode=0 es que no está en dicho modo.

Si conservemode fuera igual a 1 habría que matar algunos proceso o esperar a que terminen.

Ping extendido

Internal: 192.168.42.1
DMZ: 192.168.100.1
WAN1: 10.10.100.254
WAN2: 172.15.30.1

```
# exec ping-options source 192.168.100.1
(Con este comando elegimos el interface origen desde donde hacemos el ping)

# exec ping 172.15.30.1
```

Habilitar o deshabilitar debug

```
diagnose debug enable
diagnose debug disable
```

Captura de paquetes

Uso

```
diag sniffer packet <interface> <'filter'> <verbose> <count>
```

donde

- <interface> el nombre de un interface o “any” para todos los Interfaces.
- <'filter'> filtro a aplicar en la captura.**none** para no utilizar ninguno
- <verbose> nivel de información que queremos
- <count> número de paquetes a capturar

Hay varios niveles para Verbose:

- 1→muestra las cabeceras “header” de los paquetes
- 2→muestra la cabecera y los datos de los paquetes IP
- 3→ muestra la cabecera y los datos de los paquetes Ethernet

El nivel Verbose 1 es el que da menos información y el 3 el que más.

Ejemplos

- Ejemplo de captura de paquetes SYN solamente

```
diag sniffer packet interface1 'tcp[13] == 2'
```

Este comando puede ser útil para detectar actividad sospechosa en la red.

- `diagnose sniffer packet port1 'TCP AND HOST 192.168.1.4 AND PORT 80' 6`
- `diagnose sniffer packet internal 'port 25'`
- Captura el tráfico entres dos equipos

```
diag sniffer packet internal 'src host 192.168.2.1 and dst host
192.168.0.1' 1
```

- Captura todo el trafico tcp(peticiones dns, icmp, etc) entre dos equipos

```
diag sniffer packet internal 'src host 192.168.2.1 and dst host
192.168.0.1 and tcp' 1
```

- `diag sniffer packet internal 'host 192.168.2.1 and (icmp or tcp)' 1`
- `diag sniffer packet internal 'host 192.168.2.1 or host 192.168.0.1 and tcp port 80' 1`

Referencias

http://kb.fortinet.com/kb/viewContent.do?externalId=11186&sliceId=1

Guardar la configuración

```
exec cfg save
```

Copiar la configuración a otro equipo

http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=10063

Crear un switch

```
config system switch-interface
edit nombre_switch <- nombre que nosotros queramos poner
set member internal wlan <-puertos a añadir
end
```

Una de las cosas que suelen preguntar en los exámenes son las opciones de las configuraciones por defecto

Aumentar tiempos de sesion

Puede ocurrirnos que si tenemos una conexión iniciada y durante un tiempo no exista actividad en dicha sesión, el cortafuegos acabe, pasado un tiempo, cerrándonos dicha sesión por falta de actividad.

Si queremos aumentar el tiempo que esa sesión está activa antes de cerrarla tenemos que modificar el parámetro ttl (time to live o timeout) de la sesión

Esto aumenta el consumo de recursos del sistemas (especialmente la RAM)

Por ejemplo para poner por defecto un timeout de 3000sg para todo los servicios excepto para el ssh que vmos a poner 6000 segundos.

```
config system session-ttl
set default 3000
config port
edit 22
set timeout 6000
next
end
end
```

Limpiar reglas sin usar

Este truco te permite saber que reglas están siendo utilizadas y cuales no se usan, para ello tenemos que ir a Firewall→Política→Opciones de Columna→Añadir el campo **Conteo** (Count si lo tienes en inglés)

Ahora en la lista de políticas aparece una columna que indica las veces que una política ha sido llamada y el número de bytes transferidos.

Ahora basta con mirar las reglas con el contador 0/0 para comprobar si son necesarias.

Reiniciar una aplicación

```
diagnose test application <aplicacion> <opciones>
```

Si como opción al final ponemos 99, le decimos al Fortigate que reinicie el proceso

Por ejemplo para reiniciar el motor IPS

```
diag test application ipsengine 99
```

Servidor Correo

Si tenemos un servidor de correos en nuestra red en vez de crear una ip virtual hay que crear un ip pool para que haga bien el NAT http://kc.forticare.com/default.asp?SID=&Lang=1&id=1969

Para ver las source-ip definidas a nivel global

```
get system source-ip status
```

para cambiarlas

```
service=NTP source-ip=<loopback-address>
service=DNS source-ip=<loopback-address>
service=Fortiguard source-ip=<loopback-address>
service=Syslog #2 source-ip=<loopback-address>
service=Alert Email source-ip=<loopback-address>
```

Referencias

- http://pub.kb.fortinet.com/index/
- http://firewallguru.blogspot.com
- Ejemplos http://docs.fortinet.com/cb/html/index.html#page/FOS_Cookbook/Install_advanced/cb_install-advanced.html#
- Tutoriales http://www.maya.com.sv/kb/index.php/category/fortigates
- http://firewallguru.blogspot.com
- http://www.soportejm.com.sv/kb/index.php/article/radius-fortigate autentificación mediante radius
- http://www.soportejm.com.sv/kb/index.php/article/control-application
- http://www.lebleuet.net/how-to-run-a-debug-on-a-fortinet-firewall?lang=en
- http://www.ipspace.eu/fortinet/fortigate-tutorial-logging-and-alerts/
- http://www.ipspace.eu/fortinet/fortigate/fortigate-conserve-mode-how-to-stop-it-and-what-it-means/
- http://www.soportejm.com.sv/kb/index.php/category/fortigates
- http://www.hackplayers.com/2016/01/backdoor-ssh-en-fortigate-4-a-5.0.7.html