fortigate

Fortigate

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

Comandos

Rutas

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

Para ver el rendimiento

```
CLI# diagnose sys top
```

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
```

Captura de paquetes

- Ejemplo de captura de paquetes SYN solamente

```
diag sniffer packet internal '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'`

Guardar la configuración

```
exec cfg save
```

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.

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

Referencias

http://firewallguru.blogspot.com
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