

## **Determinar el cuadro de pesos relativos y la tabla de valoración de atributos para evaluar la selección a partir de las siguientes especificaciones técnicas**

### **Generales**

- Se requiere una solución de appliance físico.
- Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual.
- La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
- Debe tener consola gráfica de administración y reporting.

### **Rendimiento**

- Throughput capa 4 como mínimo de 8 Gbps.
- Throughput capa 7 (HTTP 64K) como mínimo de 8 Gbps
- Throughput Inspección SSL, mínimo 4 Gbps
- Throughput IPS, mínimo 4 Gbps
- Sesiones concurrentes (TCP), mínimo 10 Millones.
- Sesiones por segundo (TCP), mínimo 290.000
- Usuarios SSL-VPN concurrentes, mínimo 2000

### **Funciones requeridas**

- Filtrado de paquetes por direccionamiento y puerto
- Soporte de IPv4
- Soporte de Trafico Multicast
- Soporte de VPN
- Soporte Traffic Shaping
- Inspección de paquetes con estado desde capa 2 a capa 7 encriptados o no.
- Función de IPS

### **Otras características valoradas**

- Permitir la configuración de túnel IPSEC Site-to-Site
- Identificar la aplicación (capa 7 del modelo OSI), independientemente del puerto lógico utilizado, encriptación utilizada (SSL o SSH) o cualquier técnica evasiva utilizada.
- Permitir categorizar aplicaciones no identificadas para aplicar políticas de control de la solución, o soluciones forenses anti amenazas.
- Permitir bloquear amenazas conocidas, exploits informáticos, malware, spyware a través de todos los puertos, independientemente de la utilización de tácticas evasivas utilizadas.