Administración de rendimiento.

Para la administración de rendimiento es importante contar con las sondas RMON ya que estas nos permitirán capturar el trafico de la red, si se usan routers de Cisco existe una característica llamada Netflow que sirve para detallar información del tráfico como lo son:

* Direcciones IP de origen y destino.
* Interfaces de entrada y salida.
* Puertos de origen y destino UDP/TCP.
* Número de bytes y paquetes en el flujo.
* Números del sistema autónomo de origen y destino.
* Tipo de servicio.

Los datos de NetFlow recopilados en los dispositivos de red se exportan a una máquina del colector. El colector realiza las funciones tales como reducción del volumen de datos (filtración y agregación), del almacenamiento de datos jerárquico, y de la Administración de sistema de archivos.

Una vez obtenidos estos datos, para almacenarlos se puede usar el software SAS, este al ser un software estadístico nos permitirá guardar una gran cantidad de información además de poder manipularla.

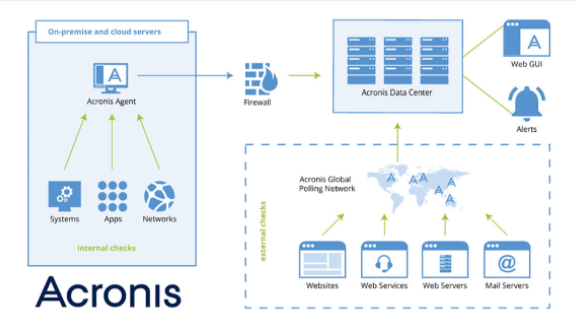
Otros puntos para considerar son que la CPU debe constar de un buen backplane para tener un mejor procesamiento de tráfico, el tamaño de la interfaz y el tubo deben ser amplios para tener una mayor cantidad de datos a enviar de manera simultánea.

Administración de la seguridad.

Para la parte de seguridad de manera preferente se usarán routers Cisco, ya que estos nos permiten usar el protocolo TACACS pero mejorado por ellos mismos con el fin de tener un control más fino, esta mejora la han llamado TACACS+, que al igual que su base cumple con la arquitectura de las AAA, además se puede usar el modo sin privilegios o privilegiado, se pueden configurar para la tolerancia a incidentes, además que una vez que TACACS+ ha sido iniciado se puede pedir el usuario y contraseña para una sesión o para comandos individuales incluyendo la autenticación y la autorización que entre más privilegios tenga más fuerte será.

Además, para la contabilidad el uso de TACACS+ permite usar comandos para administrar la autenticación, autorización y contabilidad.

Para monitorear la red, el servidor o cortafuegos se puede usar un programa llamado “Acronis Monitoring System”.



Esta herramienta tiene la capacidad de para monitorizar todos los elementos: redes, rendimiento de los servidores y sistema operativo, aplicaciones y servicios y comprobaciones web sintéticas, además Acronis es compatible tanto para comprobaciones externas como para internas. La monitorización externa recurre a agentes públicos de Acronis que comprueban la red remotamente a través de la red mundial de sondeos. Así determina la disponibilidad y la actividad en los servicios web, cuando se accede a ellos desde el exterior, desde diversas ubicaciones. Cuando se quiere comprobar los sistemas, la aplicación y los parámetros de red en la infraestructura TIC, la monitorización interna recurre a agentes privados instalados en un servidor basado en la nube o in-situ, ambos disponibles tras un cortafuegos.

Investigar syslog, TACACS, RADIUS, CERT, PSIRT, conmutador de catalizador