

La sala de comunicaciones del Centro Regional de Chiriquí cuenta con dos racks principales: uno pertenece al Grupo de Investigación en Tecnologías Computacionales Emergentes (GITCE), y el otro alberga los componentes esenciales de la red institucional de la UTP. En este laboratorio nos vamos a centrar en el rack institucional, que da servicio a la red principal de la UTP en ese centro regional.

Elementos del sistema:

1. Firewall Fortinet:

El firewall de Fortinet es el primer dispositivo de seguridad perimetral de la red. Sus funciones incluyen:

- Filtrado de tráfico entrante y saliente basado en reglas de seguridad (p. ej. direcciones IP origen/destino, puertos, protocolos).
- Prevención de intrusiones (IPS), detección y bloqueo de amenazas, malware, protección avanzada contra nuevas amenazas mediante inteligencia de amenazas.
- Gestión de conexiones VPN para interconectar sedes remotas o usuarios remotos de forma segura.
- Aplicación de política de seguridad, calidad de servicio (QoS), control de acceso a aplicaciones, filtrado de URLs, DNS, etc.
- Sistema operativo interno (como FortiOS) que permite actualizaciones, administración de logs, reportes, etc. Versiones modernas como FortiOS 7.6 ofrecen mejoras en visibilidad, gestión unificada, IA, respuesta ante incidentes en tiempo real.

2. Arquitectura de Red: Núcleo, Distribución y Acceso:

La red institucional está organizada por capas, siguiendo el modelo jerárquico de redes (tres capas): acceso, distribución, y núcleo (core). Las marcas Cisco y Huawei proporcionan los switches y routers que cumplen estas funciones.

- Capa de acceso: es donde los dispositivos finales (PCs, estaciones de trabajo, impresoras, puntos de acceso inalámbricos, etc.) se conectan. Aquí están los switches de acceso que pueden manejar VLANs, seguridad local, autenticación de puerto, etc.
- Capa de distribución: conecta los switches de acceso entre sí y con el núcleo, aplica políticas de red (enrutamiento interno, ACLs, QoS, agregación de enlaces, redundancia). Es el punto donde se segmenta la red (VLANs), se filtra tráfico, se realiza balanceo de carga, se controlan las áreas de fallo, etc.
- Capa de núcleo: backbone de la red. Proporciona conectividad de alta velocidad entre los distintos puntos de la red, interconexión con otras sedes o centros regionales, enlace con Internet y servicios centrales. Su objetivo es que el tráfico se transporte rápidamente, con baja latencia y alta disponibilidad.

En la UTP, además, esta arquitectura permite la interconexión entre centros regionales y la sede central mediante el proveedor.

3. Servidor con sistema operativo Citrix:

Se refiere a un servidor que proporciona servicios de virtualización, aplicaciones remotas o escritorios virtuales usando la tecnología de Citrix (por ejemplo Citrix Virtual Apps and Desktops). Esto permite que los usuarios finales accedan remotamente a aplicaciones y escritorios alojados en servidor. Puede ser usado para que estudiantes/docentes accedan a software especializado sin necesidad de instalarlo localmente, con acceso desde diferentes sedes, dispositivos o ubicaciones.

Componentes típicos de un entorno Citrix: hipervisor (VMware, Hyper-V u otro), controladores de entrega (“Delivery Controllers”), StoreFront, Citrix Gateway, Director, etc.

Bibliografía:

¿Qué es un firewall? Definición y tipos de firewall | Fortinet. (2023). Fortinet.
<https://www.fortinet.com/lat/resources/cyberglossary/firewall?>

Campus. / Cisco. (2014)
https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Información técnica general | Citrix Virtual Apps and Desktops 7 2303. (2024). Citrix.com.
<https://docs.citrix.com/es-es/citrix-virtual-apps-desktops/2303/technical-overview.html>