

SOFTWARE

RouterOS es un software de enrutamiento que permite realizar las siguientes operaciones: Enrutamiento OSI7, MPLS, Firewall, Enlaces Inalámbricos punto a punto tipo carrier a grandes distancias, Enlaces inalámbricos Punto Multipunto TDMA, Controller de WiFi- CAPS MAN

Características de Ruteo

· Políticas de enrutamiento. Ruteo estático o dinámico. · Bridging, protocolo spanning tree, interfaces multiples bridge, firewall en el bridge. 9 · Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP. · Cache: web-proxy, DNS. · Gateway de HotSpot. · Lenguaje interno de scripts.

Características del RouterOS

· Filtrado de paquetes por: · Origen, IP de destino. · Protocolos, puertos. · Contenidos (seguimiento de conexiones P2P). · Puede detectar ataques de denegación de servicio (DoS) · Permite solamente cierto número de paquetes por periodo de tiempo. Calidad de servicio (QoS) Tipos de colas · RED · BFIFO · PFIFO · PCQ Colas simples · Por origen/destino de red. · Dirección IP de cliente. · Interfase Árboles de colas · Por protocolo. · Por puerto. 10 · Por tipo de conexión.

Interfases del RouterOS

· Ethernet 10/100/1000 Mbit. · Inalámbrica (Atheros, Prism, CISCO/Aironet) · Punto de acceso o modo estación/cliente, WDS. · Síncronas: V35, E1, Frame Relay. · Asíncronas: Onboard serial, 8-port PCI. · ISDN · xDSL · Virtual LAN (VLAN)

Herramientas de manejo de red

· Ping, traceroute. · Medidor de ancho de banda. · Contabilización de tráfico. · SNMP. · Torch. · Sniffer de paquetes.

SOFTWARE

CAPsMAN El AP Controller de Mikrotik/RouterOS. MikroTik CAPSMAN, es un administrador de WiFi controlado. Esta es una característica de RouterOS, que permite manejar dispositivos de Punto de Acceso, sin la necesidad de unirse a cada uno de ellos. El CAPsMAN funciona en cualquier RouterBOARD y permite el despliegue de sistemas masivos de WiFi, siendo los parámetros de procesador y memoria RAM los que se deben revisar para el desarrollo sano de los proyectos. El CAPsMAN funciona con Capa 2 y Capa 3 y tiene como valor agregado administrar la configuración de los puntos de acceso y, opcionalmente también puede gestionar toda la configuración de APS.

CAPsMAN viene con todas las funcionalidades para gestión de tráfico y permite administrar de forma centralizada puntos de acceso de la misma marca, definiendo las redes Wifi, contraseñas; todo esto con la opción de decidir dónde se gestiona el tráfico, si en el manager, o en el punto de acceso.

Características básicas

- RADIUS MAC authentication
 - WPA/WPA2 security
 - TBA
 - Unlimited CAPs (access points) supported by CAPsMAN
 - 32 Radios per CAP
 - 32 Virtual interfaces per master radio interface
- CAPsMAN: También llamado “Manager” es un equipo con o sin interfaces inalámbricas que tiene la capacidad de administrar interfaces de otros dispositivos (llamados CAP). El Manager opcionalmente puede hacer reenvío de tráfico (es decir puede ser Manager y Router de Borde al mismo tiempo).
- CAP: son equipos con interfaces inalámbricas que proveen conexión a usuarios finales. Estas interfaces no se configuran localmente sino a través del Manager El CAPsMAN tiene los perfiles o configuraciones de redes inalámbricas que serán luego configuradas de forma automática en cada CAP. Los CAP sólo se encargan de proveer conectividad inalámbrica a los equipos finales.

SOFTWARE

FIREWALL El Firewall de WiCorp potencializa el RouterOS y sus funcionalidades de capa 7 (Listas Dinámicas, Scripting y Tarping) al conectar el router Mikrotik a una plataforma de defensa polimórfica que actualiza en tiempo real las reglas de seguridad y elimina de forma inteligente las amenazas a su red. En conclusión, se entrega un sistema que funciona como un departamento de ciberseguridad en línea que actualiza permanentemente las listas de acceso del firewall.

La plataforma utilizada por Wi-Corp revisa y actualiza continuamente (24*7) herramientas de protección contra amenazas abiertas o encubiertas usando listas de acceso a la red (ACL), Listas Dinámicas, Filtrado en capa 7, ataques DDoS y de otros caracteres, para dar a nuestros clientes seguridad de carácter superior.

¿COMO FUNCIONA?

El sistema usa big data analytics y machine learning para identificar origen y destino de datos tales como IP addresses, routing information, packet contents, headers, con estos puntos se logran identificar amenazas, para luego crear bloqueos a las mismas. Algunas de las acciones de bloqueo que se realizan son:

- No se permite el acceso de Port Scanners
- Protección ante spam bots
- Vía capa 7 se bloquean Ransomware y Malwares del tipo torrenting
- Via Tarpit, manipulando la conexión de paquetes, se reducen ataques del tipo DDoS
- Eliminando: Requerimientos externos de DNS, Bogons y paquetes malformados
- Usando listas dinámicas con cronómetros
- Instalando comandos en el firewall para defender su red de servidores, IP Botnets y dominios usados por los sitios del tipo ransomware.

Se actualizan aproximadamente 350,000 amenazas por día y el firewall se revisa unas 150 veces al día mediante procesos que no afectan el performance del hardware.

SOFTWARE

PORTAL CAPTIVO- HOT SPOT: Un hotspot ofrece acceso a Internet a través de una red (generalmente) inalámbrica y un enrutador conectado a un proveedor de servicios de Internet. Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, escuelas, etcétera. Este servicio se puede cubrir mediante wifi y permite mantenerse conectado a Internet en lugares públicos. Puede brindarse de manera gratuita o cobrando una suma que depende del proveedor.

Los dispositivos compatibles con wifi y acceso inalámbrico permiten conectar PDA, ordenadores, teléfonos móviles y routers, entre otros.

Por norma general, un Hotspot presenta al usuario una pantalla de bienvenida donde se tiene que hacer login con un usuario de forma gratuita, pagando o usando una cuenta temporal. Una vez realizado este paso y en función de la configuración del Hotspot, el usuario podrá acceder a Internet.

Características del Hotspot de Mikrotik:

Diferentes métodos de autenticación de clientes usando una base de datos interna en el router ó un servidor RADIUS remoto

Almacenar los usuarios en base de datos local o en el servidor RADIUS externo

Walled-garden. Acceso a algunas páginas sin necesidad de autenticación

Gestión de ancho de banda por perfiles o usuarios individuales

Modificación de la pantalla principal de Login, donde podremos poner los datos que necesitemos

Cambio automático de la dirección IP de los clientes para el correcto funcionamiento de la pantalla de login, tiempos de expiración, límite de ancho de banda, etc...

SOFTWARE

THE DUDE, es un software de gestión de red que funciona bajo Windows y permite la gestión y monitoreo de redes de alta densidad

The Dude permite el seguimiento de todos los datos que se envían en la red; administrar todas las conexiones a la red y controlar el uso de cada dispositivo.

The Dude permite crear un mapa de la red y controlar cada servicio.

The Dude asignará automáticamente la red y creará una alerta en caso de detectar un error en la red

La interfaz gráfica THE DUDE permite el uso de pantallas LED de gran formato para instalarlas en el Data Center con el objeto de tener una interfaz visual que facilite el seguimiento de equipos en la red.