

Las mejores soluciones **UTM** para redes incluyen las siguientes funciones de seguridad centrales en sus arsenales:

Cortafuegos de red que realice una inspección de paquetes con estado.

IPS detecta y bloquea intrusiones y ciertos ataques.

El control de la aplicación proporciona visibilidad y control del comportamiento y contenido de la aplicación..

VPN permite el acceso remoto seguro a las redes.

El filtrado de contenido detiene el acceso a sitios web maliciosos, inapropiados o cuestionables y contenidos en línea.

La compatibilidad con IPv6 en todas las funciones de seguridad de red protege las redes a medida que migran de IPv4 a IPv6.

Admite entornos virtualizados, tanto dominios virtuales como dispositivos virtuales. También incluye tecnologías de seguridad adicionales que las organizaciones pueden elegir implementar..

Prevención de pérdida de datos que bloquea la pérdida accidental o intencional de propiedad confidencial datos regulados o cautelares.

Protección antivirus / antispam que evita que cargas maliciosas o mensajes no deseados ingresen a las redes.

Control de punto final que hace cumplir las políticas de seguridad corporativas con usuarios y dispositivos remotos.

Controlador LAN inalámbrico (WLAN) integrado para consolidar todo el tráfico cableado e inalámbrico a través de un solo dispositivo, para simplificar la creación y el cumplimiento de políticas mientras se reduce la complejidad de la red.

Sin embargo, hay mucho más en los dispositivos UTM modernos que una larga lista de funciones