UTM, Unified Threat Management, gestión unificada de amenazas

¿Qué es UTM en seguridad informática? ¿Para qué se usa? ¿De qué se compone? ¿Cuáles son sus características? Si sigue nuestro blog verá la continuidad temática de las últimas semanas en este sitio. Todo horma, encaja dentro de la concientización que queremos hacer respecto a la seguridad informática.

En los últimos años, las estrategias de seguridad únicas se han vuelto incapaces de mantener a las empresas completamente protegidas contra las amenazas, lo que las obliga a requerir una defensa de múltiples capas que integre varias tecnologías en una estrategia de seguridad de TI.

¿Qué es entonces?

La gestión unificada de amenazas (UTM) ha surgido en respuesta a esta necesidad y se ha convertido en la solución predeterminada para muchos integradores de tecnología de la información y proveedores de servicios gestionados (MSP).

La administración unificada de amenazas o los dispositivos UTM brindan la capacidad de realizar numerosas funciones de seguridad dentro de un solo dispositivo o dispositivo de red. Estos dispositivos incluyen la funcionalidad de múltiples dispositivos especializados,tales como, firewalls de red, sistemas de prevención de intrusiones en la red, sistemas antivirus y antispam de puerta de enlace, concentradores de redes privadas virtuales, filtrado de contenido, equilibrio de carga y prevención de pérdida de datos.

All in One

La solución todo en uno es mucho más fácil de administrar para una organización que varias soluciones de seguridad diferentes, lo que reduce la complejidad. Esto es más popular entre las pequeñas empresas porque proporciona una alternativa asequible a la compra de cada solución de seguridad por separado.

¿Dónde se usan?

Los UTM se utilizan comúnmente en sucursales, oficinas en el hogar, banca, minoristas y empresas medianas.

Características de las soluciones UTM

Casi todas las aplicaciones de gestión de amenazas unificadas incluyen las mismas siete funciones. Algunas aplicaciones también pueden incluir características adicionales para atraer a ciertos clientes.

- Antivirus
- Antimalware
- Cortafuegos
- Prevención de intrusiones
- Red privada virtual (VPN)
- Filtrado web
- Prevención de pérdida de datos

Funciones de seguridad UTM

En el nivel más básico, un dispositivo de seguridad UTM actúa como un firewall de hardware con estado de red estándar para restringir el acceso a su red. Por lo general, otras funciones de seguridad se pueden activar como opciones si es necesario.

Las funciones de seguridad típicas que ofrece un dispositivo de seguridad UTM incluyen: El acceso remoto y de sitio a sitio de red privada virtual (VPN) de apoyo; Funcionalidad de puerta de enlace web segura (incluido el análisis antimalware y el filtrado de URL y contenido); Un sistema de prevención de intrusiones en la red centrado en bloquear ataques contra PC y servidores con Windows sin parches.

Otras características de seguridad UTM que a veces se ofrecen:

- Control de aplicaciones
- Firewall de aplicaciones web
- Gestión del ancho de banda prevención de pérdida de datos (DLP)
- Control de acceso basado en identidad balanceo de carga
- Protección DDoS
- Gestión de acceso inalámbrico seguridad del correo electrónico

Pros

Los dispositivos de gestión de amenazas unificados tienen muchos beneficios. Por ejemplo, reducir la cantidad de dispositivos diferentes que los técnicos necesitan aprender, operar y mantener. Esto puede ayudar a disminuir el costo total de proporcionar estas protecciones, pero los UTM tienen algunos inconvenientes.

Las ventajas incluyen menores costos iniciales, mantenimiento y consumo de energía, ya que todas estas funciones residen dentro de un solo dispositivo montado en un bastidor, también son más fáciles de instalar y configurar que múltiples dispositivos individuales y se pueden integrar completamente.

Contras

El mayor problema con estos dispositivos es que se convierten en un único punto de falla. Si el dispositivo falla, por ejemplo, no solo pierde su firewall o su capacidad antivirus, sino que pierde casi toda su pila de seguridad a la vez. Esto significa que cualquier entidad maliciosa o ignorante solo tendría que interrumpir el UTM para derribar todo el sistema de seguridad.

Las empresas que utilizan un dispositivo UTM corren el riesgo de poner todos sus ‘huevos’ de seguridad en una canasta. Este riesgo debe tomarse en serio y, sopesarse con los posibles beneficios de un UTM al analizar las soluciones de seguridad. Otra de sus posibles debilidades es que carecen de la cantidad de detalles que proporciona un dispositivo especializado y que su rendimiento puede ser menos eficiente que el de un dispositivo de una sola función.

En definitiva, su organización debe considerar tanto las ventajas como las desventajas de la administración unificada de amenazas antes de decidir implementarla dentro de su

arquitectura. Si su organización decide utilizar un dispositivo de administración de amenazas unificado, debe colocarlo entre su LAN y la conexión a Internet, como si fuera un firewall.

¿Cuál es la diferencia entre un firewall y un sistema de gestión unificada de amenazas?

Un firewall es una pieza de software que verifica los paquetes de datos antes de que entren o salgan de la red o la máquina en la que está instalado. Compara el contenido del paquete con un conjunto de reglas y luego determina si el contenido es seguro. Si no es así, el paquete se descarta y no ingresa al dispositivo.

Un sistema UTM también hace esto, pero también realiza más tareas de detección y prevención. En lugar de solo monitorear el flujo de paquetes, también puede administrar el equilibrio de carga de la red, el filtrado web y puede proporcionar una descripción general de la red para la resolución de problemas.

La mayoría de los sistemas UTM incluyen un firewall como una de sus características de seguridad. Por lo que proporciona automáticamente una mejor defensa.

Incluso cuando se compara con un firewall de próxima generación (NGFW) que incluye prevención de intrusiones, un sistema UTM aún lo supera, ya que contiene las características del NGFW y más.

Firewall de próxima generación vs UTM

Algunas fuentes dicen que los UTM y los firewalls de próxima generación (NGFW) son sinónimos. Es cierto que algunas

capacidades de los NGFW se superponen con las de los UTM. Sin embargo, los UTM incluyen funciones de seguridad adicionales como el antivirus de puerta de enlace y el filtrado de contenido que no están cubiertos por los NGFW.

Los NGFW son firewalls que incluyen sistemas de prevención de intrusiones e inteligencia de aplicaciones. Originalmente fueron diseñados para llenar el agujero de seguridad dejado por los firewalls tradicionales. Los dispositivos UTM ofrecen siete capas de seguridad, siendo NGFW una de esas capas. Es importante tener en cuenta que cada solución se utiliza por diferentes razones y ninguna es superior a otra.

¿Cómo funciona la Gestión unificada de amenazas?

La mayoría de los sistemas UTM funcionan mediante inspección para detectar actividad maliciosa. Esto generalmente se incluye en una de dos categorías.

1. Inspección de flujo

Al igual que el funcionamiento de un firewall, las muestras de datos que se envían a la red se analizan con algoritmos coincidentes para determinar si son maliciosos. Si lo están, se les impide ingresar a la red. Este método es más rápido.

2. Inspección por poder

Inspección basada en proxy , que reconstruye el contenido que ingresa a un dispositivo UTM y realiza una inspección completa del contenido en busca de posibles amenazas a la seguridad. Si el contenido parece limpio, el dispositivo envía el contenido al usuario final. Si se detecta un virus u otro problema de seguridad, el dispositivo elimina el contenido problemático antes de enviar el archivo o la página web al usuario. Este método es más lento pero más preciso.

Planificación de la capacidad de la red

Un desafío operativo clave es proporcionar un rendimiento adecuado mientras su organización se amplía y sus necesidades de seguridad cambian. Esto se debe a que una organización con una conexión de red de 1 Gbps puede verse tentada a comprar un UTM con una capacidad de estas mismas condiciones, pero tan pronto como se active cualquier opción de seguridad más allá de las capacidades simples de firewall de hardware, el rendimiento disminuirá drásticamente.

Otro desafío operativo clave es cómo tratar con las sucursales. Algunas organizaciones optan por enrutar todo el tráfico de su red a través de una única puerta de enlace de Internet, pero otra opción es proteger cada sucursal con su propio UTM en el perímetro de su red. Cuando este es el caso, los UTM de las sucursales son fáciles de ignorar y difíciles de monitorear, por lo que es vital considerar elegir un UTM con un sistema de administración que permita que los cambios de configuración se envíen a cada dispositivo de la sucursal.

Conclusión

Las organizaciones de hoy no pueden ser demasiado cuidadosas cuando se trata de la seguridad de la red y la TI, especialmente cuando los datos del cliente y el cumplimiento normativo están en riesgo.

Ahora se requieren múltiples capas de seguridad para mantener alejados a los atacantes y proteger los datos confidenciales. Al mismo tiempo, las organizaciones continúan enfrentándose al desafío de administrar la seguridad internamente, debido a la gran carga de los requisitos de administración diarios y al aumento de los costos. Sin embargo, aquí es donde la asociación con un proveedor de servicios gestionados resulta

más beneficiosa. Cuando los MSP incluyen la gestión unificada de amenazas en su pila de tecnología, les proporciona a los clientes una solución integral de seguridad de TI. Además, UTM es altamente compatible con la mayoría de las soluciones y servicios que los MSP ya tienen en su cartera.

Leer también: ¿Qué es un sistema de prevención de intrusiones, IPS?