



Seis consejos para elegir una solución UTM

Por **Angelo Comazzetto**, Senior Product Manager

A medida que la seguridad de redes se hace más compleja, las empresas demandan la sencillez de las soluciones Unified Threat Management (UTM). Empresas como la suya están sustituyendo varios dispositivos costosos y obsoletos de diferentes proveedores por una única solución UTM fiable. Las mejores soluciones ofrecen una forma más potente de gestionar la seguridad de redes hoy y en el futuro. Las soluciones UTM también prometen reducir drásticamente sus esfuerzos en materia de gestión de seguridad de redes y sus costes de hardware.

Este monográfico le ofrece recomendaciones detalladas sobre cómo elegir la completa solución Unified Threat Management (UTM) que mejor se adapte a su empresa.

Ventajas de las soluciones UTM

Con una solución UTM, no tendrá que gestionar y actualizar varias soluciones de protección de diferentes proveedores. Las soluciones UTM simplifican la configuración, la resolución de problemas y la completa gestión de amenazas al tiempo que reducen los costes de gestión. IT puede adoptar rápidamente un sistema familiar. Y con las soluciones UTM gestiona un proveedor, no diez.

Por eso, elegir la plataforma UTM adecuada le ayuda a simplificar de forma significativa la gestión de seguridad de redes.

Cómo elegir la solución UTM adecuada

Las soluciones UTM actuales pueden parecer similares, pero existen importantes diferencias en lo que se refiere a gestión y profundidad de campo. La profundidad de campo se refiere al número de funciones incluidas, pero se centra en la riqueza y eficacia de cada función al resolver problemas específicos. Por supuesto, criterios adicionales como la flexibilidad, las licencias, la sencillez de uso y el rendimiento también influyen en su decisión de compra.

Estos son los seis criterios principales que debería evaluar:

1. Gestión unificada

Elija un producto UTM que le resulte sencillo utilizar. Debe ser fácil de comprender, ofrecer una buena integración y permitirle resolver rápidamente problemas de seguridad. El tiempo necesario para familiarizarse con un producto UTM y alcanzar los objetivos depende de cada persona. Las mejores soluciones ofrecen un entorno y un conjunto de procedimientos que le permiten gestionar con eficiencia los problemas. Cuidado con las soluciones que ofrecen agregar en vez de integrar. Estas soluciones han demostrado ser muy complejas y dificultan su trabajo diario en vez de ahorrarle tiempo. También debe tener en cuenta que algunos productos consiguen una interfaz muy sencilla a expensas de la profundidad: prescinden de muchas opciones y funciones para centrarse en su "sencillo" uso.

2. Profundidad de campo

Revise cuidadosamente la profundidad de las funciones y la calidad de los componentes que necesita de verdad. Las soluciones pueden comercializarse como si fuesen completas cuando, en realidad, pueden dejarle vulnerable a ataques. Por ejemplo, aunque la lista de funciones de una solución UTM incluya filtro de spam o análisis de correo electrónico, es posible que no esté completamente protegido. Existen tecnologías antispam basadas en listas estáticas u orígenes de correo electrónico no fiables que no tienen en cuenta el comportamiento del spammer. Pueden parecer impresionantes. Pero quizá no funcionen.

Lo mismo se aplica al filtrado de URL, que puede ofrecerse de una gran cantidad de maneras. Muchos proveedores comercializan filtros de URL o webs que tienen en cuenta la política de navegación. Algunos ofrecen las funciones mínimas, mientras otros son tan complejos que necesitan demasiada formación o una importante reestructuración de las redes.

De modo que no debería centrarse únicamente en un despliegue que permita marcar la casilla de verificación de una función en una tabla de requisitos o de comparación. Tómese el tiempo necesario para evaluar detenidamente sus requisitos, qué funciones son importantes y cómo deberían desplegarse.

3. Capacidad de adaptación a nuevas demandas

Las mejores soluciones UTM pueden adaptarse. Deben adaptarse de forma flexible a las necesidades de su empresa, ahora y en el futuro. Cuando aparezcan nuevas amenazas de seguridad, nuevas herramientas, versiones, actualizaciones, tecnologías y plataformas completas deben responder. La capacidad de añadir o quitar usuarios también es fundamental.

Por último, debe poder integrar dispositivos adicionales en una única consola de gestión. Esto le permite crear una instalación más potente que funcione como un todo. Cuando dispone de diferentes opciones de expansión, puede ahorrar tiempo y dinero.

4. Opciones de licencia

Las opciones de licencia de los productos UTM pueden ser tan diversas como complejas. Muchos fabricantes dicen que sus dispositivos de hardware son escalables, pero la mayoría presentan importantes limitaciones.

De acuerdo con Frost & Sullivan, analistas del sector, se espera que el mercado de las soluciones UTM supere los 4000 millones de dólares en 2012.

Trampas habituales en lo que se refiere a licencias:

1. "Número ilimitado de usuarios"

Algunos proveedores cobran por usuario teniendo en cuenta las direcciones IP, las direcciones MAC y otros factores que no son evidentes. Un proveedor puede anunciar un número ilimitado de usuarios y, sin embargo, limitar el número de conexiones que puedan estar activas al mismo tiempo. Esto es un límite eficaz que no impide anunciar un número ilimitado de usuarios.

2. Límites de ancho de banda

Otras empresas limitan eficazmente la cantidad máxima de rendimiento de un dispositivo limitando el ancho de banda, por ejemplo limitando la velocidad de subida (WAN) a 1 megabit por segundo.

3. Funciones repartidas entre productos

A veces los proveedores reparten funciones muy demandadas entre distintos productos. Por ejemplo, si se ofrece la solución UTM modelo 1000 a un precio determinado, asegúrese de que para resolver los problemas del modelo 1000 no sea necesario comprar el modelo 1000C o el modelo 300.

Comprender cómo funcionan las licencias de los productos aumenta la probabilidad de elegir la solución adecuada para su empresa. Asegúrese de leer la letra pequeña.

5. Facilidad de uso

Muchos proveedores hablan sobre la facilidad de uso. La interfaz gráfica de usuario (GUI) debe ser intuitiva. No obstante, prácticamente todos los proveedores afirman que la facilidad de uso de su producto es mayor que la de los productos de los demás. Puede comprobar si un producto está bien diseñado viendo unas cuantas capturas de pantalla o dedicando unos minutos a conocer una demostración online o una plataforma de pruebas.

Las mejores soluciones le permiten moverse fácilmente por el producto y efectuar cambios sin tener que convertirse en un experto en tecnología. No elija soluciones UTM que aún presenten configuración de la línea de comandos, programas de gestión de clientes extra o incluso entornos de GUI completamente independientes. Un producto bien diseñado tiene en cuenta al usuario, y no solo a la tecnología que se está configurando.

Al evaluar soluciones UTM, es importante tomarse el tiempo necesarios para asistir a un webcast, ver la interfaz en acción o solicitar un paquete de evaluación. Para hacer la mejor compra, debe probar la GUI personalmente.

Seis consejos para elegir una solución UTM

Asegúrese de verificar la configuración predeterminada. Si un producto requiere inmediatamente invertir una importante cantidad de tiempo en su configuración para cumplir su política de seguridad, existen más puntos de posibles fallos de configuración que en un producto totalmente bloqueado de forma predeterminada. Pruebe el producto durante el proceso de compra: puede ahorrarle muchas horas en el momento del despliegue.

6. Datos de rendimiento

Todos los proveedores ofrecen datos de rendimiento, pero pueden ser confusos. Cuando evalúe una solución UTM, debe tener en cuenta la calidad de los datos y cómo se han recopilado.

Es imposible evaluar un producto UTM por una sola cifra. Si una hoja de configuración indica un rendimiento de correo SMTP de 120 000 mensajes por hora, debe conocer los factores que influyen en esta cifra, incluido el tamaño de cada mensaje analizado, el intervalo de tiempo durante el que se envían y reciben los mensajes y en qué punto del filtrado se rechazan o aceptan los mensajes. Los métodos antispam sofisticados rechazan muchos mensajes de correo que son spam incluso antes de que lleguen a los analizadores de contenido del correo, por lo que el número de mensajes de correo que pasen por todos los componentes de filtrado puede reducirse a una fracción de todos los mensajes de correo "vistos" por el dispositivo UTM. Esto significa que el rendimiento anunciado puede ser muy diferente.

Por otra parte, dos casos de prueba de la misma solución pueden mostrar rendimientos muy distintos si el primer caso prueba el filtrado de correo electrónico con todas las opciones de análisis habilitadas y el segundo solo tiene una opción activada. Diferentes combinaciones de configuraciones con funciones concretas, como VPN o filtrado web, pueden causar numerosas variaciones en los datos de rendimiento.

Criterios de evaluación al elegir una nueva solución UTM

1. Gestión unificada
2. Profundidad de campo
3. Capacidad de adaptación a nuevas demandas
4. Opciones de licencia
5. Facilidad de uso
6. Datos de rendimiento

Seis consejos para elegir una solución UTM



Acerca de la solución Sophos UTM

Hemos ilustrado el gran número de posibilidades que se presentarán ante usted cuando elija un producto UTM. En Sophos, nos dedicamos a facilitarle la selección de una solución UTM.

La solución Sophos UTM ofrece una serie de funciones que atiende todas sus necesidades de seguridad de redes. Ofrecemos todas las funciones en todas las plataformas y, lejos de contar con un solo modelo, proporcionamos un número de licencias realmente ilimitado en la totalidad del hardware, el software y los dispositivos virtuales. Eso significa que puede desplegar un dispositivo de Sophos en cualquier red, y cambiar su función cuando aumenten sus requisitos o cuando sustituya otras soluciones por las funciones de Sophos UTM.

Diseñamos el producto de principio a fin pensando en los usuarios. Al iniciar sesión por primera vez, la elegante y moderna GUI basada en navegador presenta directamente al administrador las funciones esenciales, y para utilizar las funciones y características necesarias bastan unos conocimientos mínimos sobre seguridad.

Estamos permanentemente en contacto con nuestros partners y clientes, y mejoramos nuestras soluciones teniendo en cuenta su opinión. Los administradores que utilicen nuestras soluciones podrán desplegar potentes funciones con solo unos clics, de verdad, sin pasar semanas aprendiendo cómo utilizarlas.

Más información

esp.sophos.com