SOPHOS

Guía para la adquisición de soluciones de UTM y protección de redes

El uso de soluciones de UTM para proteger las redes solía ser una medida parcial: aunque se conseguían ahorros de recursos y facilidad de uso, había que renunciar a ciertas capacidades de protección. Hoy en día, proteger las redes con soluciones de UTM es todo ventajas. Además de disfrutar de los estándares de seguridad más altos, es posible integrar multitud de funciones de protección en una sola plataforma y añadir otras cuando sean necesarias.

Esta guía está diseñada para ayudarle a elegir la solución más adecuada para su empresa. En ella se analizan los factores a tener en cuenta a la hora de evaluar soluciones para conseguir la protección y las funciones necesarias, tanto ahora como a medida que el negocio evolucione.

Cómo utilizar esta guía

En esta guía se enumeran las funciones que deben proporcionar las soluciones de seguridad, divididas en áreas de protección independientes (redes, Internet, correo electrónico, etc.) para facilitar su uso. También incluye preguntas que puede hacer a los proveedores para encontrar la solución que mejor se ajuste a sus necesidades.

Al final del documento encontrará un lista para comparar los productos. Utilice los datos ya proporcionados o añada requisitos adicionales que puedan ser necesarios para su empresa.

Qué es UTM

Las soluciones de gestión unificada de amenazas, o UTM, son suites de programas de seguridad integrados en una sola plataforma que proporcionan protección y políticas de seguridad uniformes a las empresas en su totalidad. Usted elige los elementos de seguridad que desea utilizar y todos ellos se administran mediante una sola plataforma con una consola centralizada.

Según Gartner*, las soluciones UTM deben proporcionar, como mínimo, las siguientes funciones:

- Funciones de cortafuegos dinámico de red estándar
- Acceso remoto y compatibilidad con redes privadas virtuales (VPN) de sitio a sitio
- Puertas de enlace web seguras (filtrado del contenido, direcciones web y programas maliciosos)
- Prevención de intrusiones en la red centrada en el bloqueo de ataques contra servidores y ordenadores de Windows en los que faltan parches

A la hora de evaluar soluciones de UTM, es necesario tener en cuenta dos cosas: las ventajas generales que ofrece la solución de UTM y la conveniencia de cada función de seguridad individual para los requisitos específicos.

Cortafuegos de última generación

Ahora mismo, los cortafuegos de última generación están de moda y cada proveedor describe los constituyentes básicos de forma diferente. Sin embargo, casi todos coinciden en que los cortafuegos de última generación van más allá de los cortafuegos tradicionales y protegen mejor a las empresas en un mundo tan centrado en Internet como el actual.

Las cuatro características fundamentales de los cortafuegos de última generación son:

1. Visibilidad y control de aplicaciones
2. Optimización del uso de las conexiones a Internet
3. Sistemas de prevención de intrusiones (IPS) comprensibles y claros
4. Redes VPN sencillas para la conexión con sucursales y el acceso remoto de usuarios

Muchas soluciones de UTM ofrecen funciones de cortafuegos de última generación. Para poder evaluar las soluciones en función de los requisitos, es importante comprender bien qué se necesita.

* Cuadrante mágico de Gartner de gestión unificada de amenazas (2012)

Evaluación de soluciones: funciones de seguridad

Protección de redes

Para evitar ser detectados, los ciberdelincuentes transforman constantemente los métodos de ataque. La mejor forma de proteger la red contra las amenazas nuevas más recientes es a través de varias capas de defensa.

Incluso antes de añadir suscripciones o licencias de protección, el producto de UTM debe proporcionar una base de seguridad sólida. En su nivel más básico, la solución de UTM debe incluir enrutamiento estático, servicios de servidores proxy de DNS, opciones de servidor DHCP, funciones NTP, cortafuegos dinámico, traducción de direcciones de red, VPN de acceso remoto básico, autenticación local de usuarios, registros locales, informes diarios y funciones de gestión básicas.

Debe proporcionar	Descripción	Preguntas para los proveedores
Sistema de prevención de intrusiones (IPS)	Analiza el tráfico aprobado para detectar paquetes maliciosos y reforzar la política de seguridad del cortafuegos. Puede eliminar paquetes que coincidan con alguna firma de la lista de patrones de amenazas.	‣ ¿Qué tipo de experiencia es necesaria para utilizar correctamente el sistema? ‣ ¿Cómo se distribuyen y configuran las reglas?
Control del ancho de banda y calidad del servicio	Otorga prioridad al tráfico según las reglas configuradas y permite controlar el uso de determinados recursos en diferentes condiciones.	‣ ¿Cuántas conexiones inalámbricas son posibles con un solo dispositivo? ‣ ¿Resulta fácil identificar y controlar el ancho de banda que utilizan las aplicaciones?
Opciones de VPN site-to-site	Vincula las oficinas remotas con la oficina principal para permitir que los usuarios envíen y reciban información a través de una conexión segura. Además, permite que los empleados utilicen dispositivos como servidores de archivos o impresoras de otras oficinas.	‣ ¿Con qué protocolos es compatible la VPN? ‣ ¿Qué experiencia o conocimientos son necesarios para configurar una VPN?
Opciones de acceso remoto	Permite que los usuarios se conecten de forma segura al dispositivo UTM desde cualquier ubicación.	‣ ¿Ofrece varias opciones de acceso remoto como, por ejemplo, a través de VPN sin cliente? ‣ ¿Es compatible el acceso remoto con cualquier sistema operativo y dispositivo? ‣ Los dispositivos de los usuarios, ¿deben disponer de aplicaciones especiales para utilizar la VPN? ‣ ¿Son necesarias licencias adicionales?
Compatibilidad con oficinas remotas	Conecta las redes de las oficinas remotas con el dispositivo de UTM para protegerlas con las mismas políticas y funciones.	‣ ¿Es fácil conectar las oficinas remotas? ‣ ¿Es necesario un técnico? ‣ ¿Se pueden administrar de forma centralizada las oficinas remotas? ‣ ¿Son necesarias licencias o suscripciones adicionales?
Informes detallados	Ofrece estadísticas e informes detallados en tiempo real e históricos sobre el uso de la red o el ancho de banda, la seguridad, etc.	‣ ¿Cuenta con un disco duro incorporado? ‣ ¿Qué tipos de informes están disponibles sin una aplicación diferente?

Protección web

Puede que ya utilice un filtro web para impedir el acceso a direcciones peligrosas, pero muchos de ellos examinan el tráfico desde el exterior y apenas detectan programas maliciosos.

La protección web debe permitir aplicar términos y condiciones respecto a los sitios de Internet que pueden visitar los usuarios y cómo pueden utilizarlos, además de bloquear programas espía y virus antes de que entren en la red. Los informes detallados deben indicar la eficacia de las políticas para poder hacer ajustes.

Debe proporcionar	Descripción	Preguntas para los proveedores
Filtrado de direcciones web	Controla el uso de Internet por parte de los empleados para evitar navegaciones informales, así como la entrada de contenido inadecuado y programas maliciosos en la red.	‣ ¿Están disponibles actualizaciones en directo? ‣ ¿Cuántos perfiles de navegación se pueden crear y utilizar?
Protección contra programas espía	Evita que los programas maliciosos se instalen en los equipos de los empleados, consuman ancho de banda y envíen datos delicados al exterior.	‣ ¿Están disponibles actualizaciones en directo?
Escaneado antivirus	Escanea el contenido antes de que entre en la red para evitar infecciones de los equipos con virus, gusanos y otros programas maliciosos.	‣ ¿Están disponibles actualizaciones en directo?
Escaneado de HTTPS	Permite ver el tráfico web cifrado para proteger la red contra amenazas que pueden transmitirse a través de HTTPS.	‣ ¿Es posible analizar el tráfico HTTPS y compararlo con las políticas?
Restricción de aplicaciones	Permite ver para qué utilizan Internet los empleados, y controla las aplicaciones que se pueden utilizar y de qué forma.	‣ ¿Están disponibles actualizaciones en directo?
Informes web interactivos	Ofrece funciones flexibles para la creación de informes con las que los administradores pueden crear informes propios.	‣ ¿Están disponibles informes sobre el uso en tiempo real e históricos? ‣ ¿Se puede programar la entrega de los informes? ‣ ¿Es necesaria alguna aplicación de creación de informes de terceros?

Protección de cortafuegos de última generación

La evolución de la protección tradicional basada en puertos utilizada en la mayoría de soluciones de seguridad para redes ha dado lugar a los cortafuegos de última generación. En lugar de simplemente permitir el tráfico a través de puertos como HTTP o HTTPS, los cortafuegos de última generación disponen de firmas que pueden identificar el tráfico de forma mucho más detallada. Por ejemplo, los administradores pueden bloquear las funciones de mensajería de Facebook pero permitir que los usuarios accedan a la red social.

Los cortafuegos de última generación también inspeccionan paquetes en detalle a alta velocidad para identificar y bloquear exploits, programas maliciosos y otras amenazas con gran precisión. Puesto que hoy en día muchos ataques están basados en Internet, el filtrado por puertos de los cortafuegos tradicionales tiene una eficacia limitada a la hora de proteger las infraestructuras contra dichas amenazas.

Gracias a los cortafuegos de última generación, las empresas también pueden establecer prioridades en el uso de la red de forma más estratégica mediante reglas de ajuste de gran potencia. Por ejemplo, pueden permitir llamadas telefónicas de VoIP o dar prioridad al tráfico de Salesforce.com, pero limitar el rendimiento o simplemente bloquear aplicaciones como Bittorrent.

Debe proporcionar	Descripción	Preguntas para los proveedores
Visibilidad y control de aplicaciones	Al poder ver las aplicaciones que se utilizan, es posible tomar decisiones bien fundadas sobre cuáles permitir, bloquear o priorizar para emplear el ancho de banda de la forma más eficaz posible y no perder tiempo bloqueando aplicaciones que no causan ningún problema.	‣ ¿Puede establecer prioridades, controlar el acceso a las aplicaciones y ver en tiempo real quién está utilizando la conexión a Internet y de qué manera? ‣ ¿Le resulta fácil configurar políticas a partir de vistas en tiempo real de las actividades en curso?
Optimización del uso de las conexiones a Internet	El ancho de banda es un artículo de lujo y es necesario asegurarse de que se aprovecha al máximo, por ejemplo, para que las aplicaciones vitales para la empresa como salesforce.com tengan prioridad.	‣ ¿Le resulta fácil gestionar el ancho de banda? ‣ ¿Dispone de un kit de herramientas de calidad del servicio?
IPS comprensible y claro	Ahora, muchos ataques por Internet son capaces de disfrazarse de tráfico legítimo. Los sistemas de prevención de intrusiones eficaces permiten ver no solo el tipo de tráfico web, sino también su comportamiento.	‣ ¿Le resulta fácil gestionar el IPS? ‣ ¿Qué nivel de dominio es necesario? Por ejemplo, ¿es necesario comprender los diferentes tipos de amenazas?
VPN sencilla para conexiones remotas	El teletrabajo es cada vez más habitual. Las empresas necesitan redes VPN seguras, sencillas y rápidas para que los usuarios puedan conectarse a la red y ser productivos desde cualquier lugar.	‣ ¿Le resulta fácil configurar redes VPN cliente para los trabajadores remotos? ‣ ¿Qué dispositivos puede utilizar para conectarse a la red? ‣ ¿Ofrece una solución de HTML5 sin cliente?

Protección del correo electrónico

La protección del correo electrónico contra virus y correo no deseado no es un problema nuevo, pero las amenazas para la seguridad distribuidas por e-mail evolucionan constantemente, lo que hace que la protección se convierta en un trabajo interminable a tiempo completo. Aún así, el correo electrónico debe estar protegido para que problemas habituales como el correo no deseado, los virus y las filtraciones de información confidencial no afecten al negocio.

Debe proporcionar	Descripción	Preguntas para los proveedores
Anti-spam	Impide la entrega de spam y otros tipos de correo electrónico no deseado a los buzones de los empleados.	‣ ¿Qué tasas de detección de spam y falsos positivos ofrece? ‣ ¿Qué técnicas utiliza para la identificación de correo no deseado?
Escaneado antivirus	Detecta y bloquea contenido malicioso en la puerta de enlace para impedir infecciones de virus y otros programas maliciosos en los equipos.	‣ ¿Cuántos motores antivirus utiliza la solución? ‣ ¿Con qué frecuencia escanea el contenido?
Cifrado del correo electrónico	Impide la lectura del correo electrónico para evitar espionajes y la obtención de información delicada y confidencial por parte de destinatarios no intencionados.	‣ ¿Qué tienen que hacer los usuarios para cifrar y descifrar el correo electrónico? ‣ ¿Cómo se administra el cifrado?
Portal para usuarios	Permite que los empleados controlen sus cuentas de correo electrónico, incluidas la cuarentena de correo no deseado y las actividades de los mensajes.	‣ ¿Pueden ocuparse los usuarios de su propia cuarentena del correo electrónico?

Protección de servidores web

Al conectar los servidores a Internet, se desvela cualquier punto débil presente en las aplicaciones web. Y proteger todas las líneas de código y configuraciones es prácticamente imposible.

La protección de servidores web impide que los ciberdelincuentes utilicen ataques como la inyección de SQL o las secuencias de comandos entre sitios para robar información delicada como datos sanitarios o de tarjetas de crédito. Además, debe ayudar a cumplir las normativas cuando es necesario un cortafuegos de aplicaciones web.

Los cortafuegos de aplicaciones web escanean las actividades y detectan intentos de aprovechamiento de las aplicaciones para evitar sondeos y ataques en la red.

Debe proporcionar	Descripción	Preguntas para los proveedores
Refuerzo de formularios	Analiza y verifica la información enviada a través de formularios por los usuarios que visitan los sitios web. Evita daños y aprovechamientos del servidor al procesar datos no válidos.	‣ ¿Se realiza un análisis completo de los formularios? ‣ ¿Es posible detectar formularios manipulados?
Escaneado antivirus	Detecta y bloquea contenido malicioso en la puerta de enlace para impedir infecciones de virus y otros programas maliciosos en los equipos.	‣ ¿Cuántos motores antivirus utiliza la solución? ‣ ¿Con qué frecuencia escanea el contenido?
Refuerzo de direcciones web	Impide que los usuarios que visitan el sitio web accedan a contenido no permitido.	‣ ¿Es necesario introducir la estructura del sitio web de forma manual o puede hacerse de forma automática mediante actualizaciones dinámicas?
Protección de cookies	Evita la manipulación de las cookies proporcionadas a los usuarios que visitan el sitio web.	‣ ¿Protege sitios de comercio electrónico contra manipulaciones de los precios de los productos?

Protección de redes inalámbricas

Las redes inalámbricas necesitan las mismas políticas de seguridad y la misma protección que la red corporativa principal. Por desgracia, los administradores de redes suelen tratarlas como dos redes independientes. La protección inalámbrica del proveedor de UTM elegido debe eliminar, o al menos reducir, el problema de imponer políticas de seguridad uniformes en toda la empresa.

La protección inalámbrica debe ampliar las funciones de seguridad de la solución de UTM a las redes inalámbricas. Además, debería proporcionar funciones para la administración centralizada de las mismas. Proteja de manera uniforme todas las redes y todos los datos, tanto si los empleados acceden a la red a través de cables como de forma inalámbrica.

Debe proporcionar	Descripción	Preguntas para los proveedores
Despliegue "enchufar y listo"	Permite realizar la configuración rápida y fácilmente ya que no es necesario configurar los puntos de acceso.	‣ ¿Cuánto se tarda en configurar y desplegar los puntos de acceso y las políticas?
Administración central	Simplifica la administración de la red inalámbrica gracias a la configuración centralizada, los registros y la solución de problemas desde una misma consola.	‣ ¿Es necesario configurar los puntos de acceso uno por uno en la interfaz local o desde la línea de comandos?
Seguridad integrada	Ofrece protección instantánea para todos los clientes inalámbricos a través de la seguridad de UTM completa.	‣ ¿Se puede reenviar todo el tráfico inalámbrico directamente a la puerta de enlace segura?
Opciones de cifrado WPA/WPA 2	Cifrado de nivel empresarial que impide la lectura de los datos por parte de usuarios no autorizados para evitar fugas y robos de datos.	‣ ¿Es compatible con varios métodos de autenticación y cifrado? ‣ ¿Está disponible alguna interfaz de acceso a servidores RADIUS?
Acceso a Internet para invitados	Protege varias zonas inalámbricas con configuraciones diferentes de la autenticación y la privacidad. Es compatible con puntos de acceso inalámbricos.	‣ ¿Cuántas zonas inalámbricas diferentes se pueden utilizar? ‣ ¿Qué tipo de puntos de acceso son compatibles? ☐ aceptación de las condiciones de uso ☐ contraseña diaria ☐ basado en vales
Informes detallados	Ofrece información sobre los clientes inalámbricos conectados y el uso de la red.	‣ ¿Cuenta con funciones integradas de creación de informes? ‣ ¿Es necesaria una herramienta diferente para los informes?

Protección de estaciones de trabajo

Las redes corporativas crecen y cambian cada vez que se conecta un portátil o un dispositivo móvil. Para que la red esté segura, es necesario proteger las estaciones de trabajo con una solución que compruebe si los dispositivos están actualizados y cumplen las políticas de seguridad.

La protección de estaciones debe proteger también los dispositivos propiedad de la empresa dentro y fuera de la red. Integre las estaciones directamente en el dispositivo de UTM para reducir las tareas de administración y ahorrar dinero. La ejecución de motores antivirus diferentes en la puerta de enlace y en las estaciones de trabajo puede contribuir también a cumplir las normativas.

Debe proporcionar	Descripción	Preguntas para los proveedores
Despliegue sencillo	Permite desplegar y gestionar fácilmente las estaciones de trabajo de las empresas para evitar programas maliciosos y fugas de datos.	‣ ¿Cómo se implementa el cliente para estaciones de trabajo?
Escaneado antivirus	Detecta virus y otros programas maliciosos en las estaciones de trabajo para impedir que entren en la red.	‣ ¿Cuántos motores antivirus diferentes se utilizan? ‣ ¿Ofrece actualizaciones en directo a través de la nube?
Control de dispositivos	Permite impedir el uso de modems, Bluetooth, puertos USB, unidades de CD-ROM y DVD, etc. en la empresa.	‣ ¿Qué dispositivos se pueden controlar con la solución? ‣ ¿Funciona la protección solamente si las estaciones de trabajo se encuentran en el dominio o si están conectadas a través de un túnel VPN?
Informes en tiempo real	Ofrece información sobre las estaciones de trabajo mediante estadísticas actualizadas.	‣ ¿Cuenta con funciones integradas de creación de informes en tiempo real?

Comparación de soluciones de UTM

A la hora de comparar soluciones de UTM, además de las funciones de seguridad independientes, es necesario tener en cuenta una serie de factores.

Necesidades específicas de la empresa

Como mínimo, los productos de UTM deben ofrecer funciones de cortafuegos dinámico, compatibilidad con redes VPN (tanto de sitio a sitio como para usuarios remotos), protección web (filtrado del contenido y protección contra programas maliciosos) y prevención de intrusiones en la red (IPS).

Tenga en cuenta también cualquier requisito de seguridad específico de su empresa. Si tiene oficinas remotas, plantéese cómo puede conectarlas de forma segura. Y si el rendimiento y la recuperación de errores son factores importantes, busque una solución que permita utilizar clústeres activo-activo.

Facilidad de uso

Por su propia naturaleza, las soluciones de UTM ayudan a reducir el tiempo y el esfuerzo dedicados a diario a la administración informática. Sin embargo, el nivel de ahorro de recursos conseguido varía dependiendo de la facilidad de uso de la solución. Tenga en cuenta tanto el período inicial como las actividades habituales que los equipos informáticos y su personal deberán realizar.

Seguridad preparada para el futuro

Al evaluar soluciones, debería tener en cuenta también los cambios que pueden experimentar las necesidades de su empresa en el futuro. Aunque no quiera utilizar todas las opciones de protección disponibles en un principio, puede que necesite funciones adicionales a medida que evolucionen el negocio y los requisitos de seguridad. Si no sabe qué funciones necesitará más adelante, es aconsejable elegir una solución de UTM cuyos modelos incluyan el mismo grupo de funciones.

Tenga en cuenta también los modelos de implementación. Un dispositivo de hardware puede ser la opción más adecuada para su empresa hoy en día pero dejar de serlo si amplía las infraestructuras a la nube. Si tiene intención de utilizar tecnologías de virtualización e informática en la nube en la actualidad o en el futuro, no olvide tenerlo en cuenta.

Comparación punto por punto

Utilice la lista de comparación de productos de la página siguiente para ver qué solución se ajusta mejor a sus necesidades específicas.

Conclusión

Utilice las listas incluidas en esta guía y colabore de forma estrecha con su proveedor para encontrar un producto de UTM que le ofrezca la protección que necesite ahora y en el futuro, y estar protegido contra las amenazas con menos esfuerzo, menos complicaciones y menos dinero.

Sophos UTM

Pruébelo gratis hoy mismo en sophos.com/es-es/try-utm.

Ventas en el Reino Unido e internacionales:
Teléfono: +44 8447 671131
Correo electrónico: sales@sophos.com

Ventas en España:
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Boston (EE. UU.) | Oxford (Reino Unido)

bg.04.13V2

Lista de comparación de productos

Utilice esta tabla para evaluar las diferentes soluciones. Algunos datos están ya incluidos, pero también puede añadir otros requisitos adicionales que puedan ser necesarios para satisfacer las exigencias específicas de su empresa. Después, utilice las preguntas anteriores para encontrar más fácilmente la solución adecuada.

Función	SOPHOS UTM	SONICWALL NSA	WATCH GUARD XTM	FORTINET Fortigate	CHECK POINT UTM-1
SEGURIDAD BÁSICA					
Cortafuegos	✓	✓	✓	✓	✓
Motores antivirus simultáneos e independientes	2	1	1	1	1
Protección integrada de estaciones	✓	Limitado	Limitado	✓	Limitado
TECNOLOGÍAS DE PROTECCIÓN DE ÚLTIMA GENERACIÓN					
Cortafuegos de aplicaciones web	✓				✓
Control de aplicaciones web	✓	✓	Modelos más grandes	✓	✓
Sistema de prevención de intrusiones	✓	✓	✓	✓	✓
Filtrado de datos HTTPS	✓	Limitado	Modelos más grandes	Limitado	
CONEXIÓN DE USUARIOS Y OFICINAS REMOTAS					
VPN IPSec y SSL	✓	✓	Limitado	Limitado	✓
Portal VPN HTML5	✓				
Redes de malla inalámbrica	✓			✓	✓
Portal de autoservicio para usuarios	✓				
Protección de oficinas remotas lista para usar (RED)	✓				
FACILIDAD DE USO E IMPLEMENTACIÓN					
Soluciones de hardware, de software, virtuales o en la nube disponibles	✓				✓
Creación predeterminada de informes, para la revisión diaria del rendimiento	Miles	Pocos	Pocos	Pocos	Pocos
Versión de software ejecutable en hardware estándar de Intel	✓				✓
Dispositivo de hardware de alta disponibilidad sin necesidad de configuración	✓				
Gestor central de UTM gratis (para la administración centralizada de varios dispositivos)	✓				
Clúster activo-activo con equilibrio integrado de cargas	✓	✓	Limitado	Modelos más grandes	✓
Cuadrante mágico de Gartner de soluciones de UTM	Líder	Líder	Líder	Líder	Líder
LICENCIAS Y SOPORTE					
Conjunto uniforme de funciones en todos los modelos	✓				
Posibilidad de añadir módulos de licencias adicionales según las necesidades	✓	✓	✓	Modelos más grandes	Modelos más grandes
Varias opciones de soporte técnico	✓	✓	✓	✓	✓
REQUISITOS ADICIONALES					