SOPHOS

simple + secure

Simplificación de la seguridad para sucursales

De **Udo Kerst,** Director Product Management Network Security

Proteger su red empresarial es más importante que nunca. Malware, botnets y otros programas maliciosos son una amenaza para su red, tanto para sus oficinas centrales como para sus sucursales. Sin embargo, ofrecer una seguridad de red constante en toda su empresa puede ser todo un reto, especialmente para aquellas personas que cuentan con sucursales con pocos usuarios y sin experiencia en sistemas informáticos.

Este documento presenta un nuevo estándar: una solución innovadora, unificada y rentable para gestionar la seguridad de las sucursales, con informes centralizados y un proceso bien definido para lograr rentabilidad de la inversión (ROI).

Seguridad para sucursales: ¿cuáles son los verdaderos problemas?

La cada vez mayor movilidad y las funciones siempre disponibles de hoy en día pueden ofrecer a su empresa una ventaja con respecto a la competencia. Sin embargo, la transmisión de datos confidenciales a través de las redes empresariales e Internet debe realizarse de forma segura. Las amenazas de hackers y el malware pueden detectar cualquier vulnerabilidad de su empresa.

Su sucursal debe contar con protección de cortafuegos, protección para conexiones VPN a recursos corporativos, un sistema de prevención de intrusos, seguridad web y de correo electrónico, al igual que su oficina central.

Tres puntos esenciales a la hora de gestionar la seguridad para sucursales:

1. Implementación de dispositivos de seguridad

De hecho, si su oficina es pequeña puede que no cuente con expertos en informática en sus instalaciones. Incluso muchas empresas no pueden permitirse el lujo de enviar sus equipos de TI para configurar nuevas oficinas en distintas ubicaciones. Algunas empresas configuran previamente cada dispositivo en la oficina central, pero con frecuencia tienen que realizar ajustes finales en las propias instalaciones. Una solución de gestión centralizada dedicada, que es fácil de instalar y configurar, ofrece el método más eficiente. Pero puede resultar tan costosa como enviar el equipo de TI a las instalaciones.

2. Asistencia técnica

Si su sucursal o un teletrabajador tienen un problema técnico, las operaciones de la empresa y, por consiguiente, su productividad pueden verse afectadas. Describir problemas por teléfono resulta muy complicado, tedioso, costoso y frustrante tanto para su personal de TI como para sus teletrabajadores. Enviar el dispositivo de un sitio para otro es inviable. Nadie se puede permitir el tiempo de inactividad. Sus empleados necesitan soporte virtual en las propias instalaciones que les permita volver a dedicarse a negocios importantes.

3. Implementación de políticas de seguridad

Debe decidir cómo establecer normas y políticas para sus empleados de la red que trabajan en las sucursales individuales. Dichas normas pueden ser las mismas que emplea en la oficina central. O pueden ser distintas. Algunos empleados de sucursales y teletrabajadores pueden contar con un acceso ilimitado a los activos de la empresa y otros pueden contar con un acceso muy limitado. Puede que desee implementar políticas que restrinjan el acceso a medios sociales o software de Internet.

¿Cómo se puede gestionar esto de forma rentable y eficaz? En ocasiones, las políticas corporativas pueden extrapolarse en el entorno de las sucursales. De lo contrario, la gestión de normas diferentes en distintos dispositivos de seguridad es un proceso tedioso e ineficaz.

Medidas de seguridad tradicionales para oficinas muy pequeñas

La investigación de la solución correcta para la seguridad de sucursales resulta todo un reto especialmente cuando los teletrabajadores cuentan con poca experiencia en sistemas informáticos. Un gran número de oficinas pequeñas comienzan con enrutadores de banda ancha que pueden ser económicos y de uso más sencillo para sus teletrabajadores, pero solo ofrecen la seguridad más básica y escasas funciones de generación de informes y visibilidad. Otras implementan cortafuegos empresariales de nivel básico para inspeccionar políticas de cumplimiento y tráfico, que ofrecen mayor seguridad, visibilidad, control y coste total de la propiedad.

A continuación indicamos algunas de las soluciones tradicionales que ha podido reconsiderar:

Dispositivos unified threat management (UTM) de gama baja que pueden ofrecerle la protección de seguridad necesaria para su sector. Sin embargo, su proceso de configuración es muy tedioso. Y puede descubrir que el coste total de propiedad "oculto" (TCO), mantenimiento constante, cuotas de suscripción y gestión, es demasiado elevado. Especialmente, si necesita proteger un gran número de oficinas pequeñas.

Enrutadores para usuarios que pueden parecer una alternativa económica para dispositivos UTM, ya que resultan más fáciles de configurar y gestionar. Aunque le ofrecen funciones de seguridad básicas (por ejemplo, cortafuegos o VPN), suelen carecer de medidas de protección de seguridad comercial, como por ejemplo, un sistema de prevención de intrusos, filtrado web y de correo electrónico.

Servicios gestionados VPN o MPLS que no suelen contar con funciones de seguridad. Estas herramientas son solo un medio para conectar todas las sucursales a un sitio central, donde suele ubicarse la puerta de enlace de seguridad. Con frecuencia está sujeto a contratos de servicio a largo plazo que pueden ser muy costosos.

El resultado final es que estas soluciones tradicionales no cubren sus necesidades. La gestión de varias soluciones puntuales aumenta la complejidad de su red. Incluso se multiplica al añadir numerosas soluciones puntuales en las sucursales.

Pero un nuevo método ya está disponible. Ofrece un coste total de la propiedad superior (TCO) incluso para la oficina más pequeña, y proporciona las ventajas de la gestión centralizada totalmente automatizada.

Un nuevo método: gestión centralizada sencilla

Un método innovador que opta por una solución unified threat management que integra medidas de seguridad para las sucursales en la estructura corporativa. Esta solución cuenta con un "cable Ethernet virtual" para conectar su oficina central y sucursales. En lugar de ejecutar funciones de cortafuegos, VPN, prevención de intrusos, seguridad web y correo electrónico en un costoso dispositivo para sucursales, se proporcionan de forma centralizada mediante una potente puerta de enlace de seguridad. Puede ubicarse en su oficina central o en la nube (por ejemplo, un proveedor de servicios).

Un pequeño Remote Ethernet Device (RED) reenvía tráfico cifrado de la oficina remota a un dispositivo centralizado que analiza y filtra los datos antes de enviarlos a Internet. Conecta su oficina central a su sucursal con tecnología VPN segura.

"La caja RED de Astaro es el producto más innovador que he visto. Saca partido de la inversión en seguridad en una única ubicación ampliándola a varias ubicaciones. Se trata de una solución sencilla y económica."

Experto del sector de la seguridad, Richard Stiennon

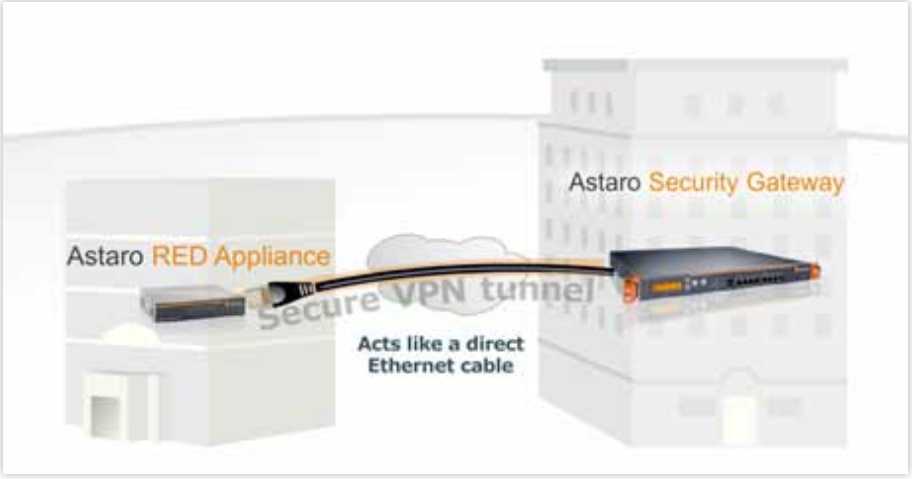


Fig. 1: Seguridad UTM completa a través de un cable Ethernet virtual

Los dispositivos RED de Astaro y los galardonados productos de Astaro Security Gateway ofrecen una solución Unified Threat Management (UTM) rentable y centralmente gestionada:

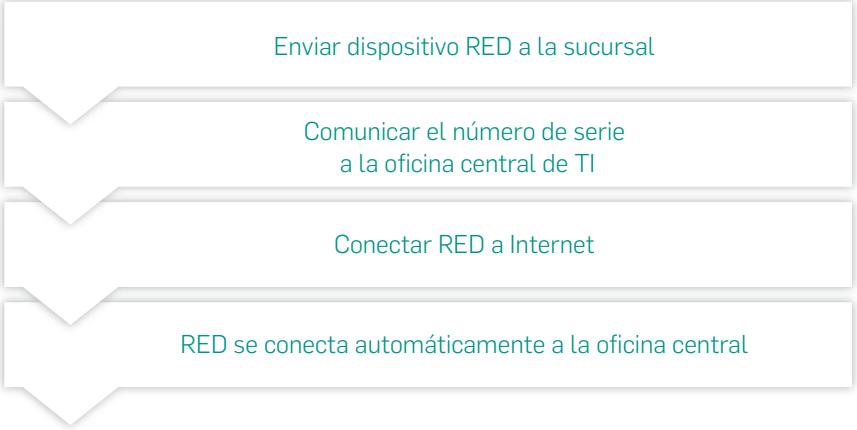
- La configuración de un nuevo dispositivo RED solo conlleva unos minutos.
- Se eliminan los costes recurrentes de tareas de mantenimiento o suscripción para la sucursal.
- Se incluyen herramientas para generar informes.

Implementación en dos minutos

Este innovador método ofrece implementación automática. Así es cómo funciona:

Los dispositivos RED se envían a las sucursales. El teletrabajador indica el número de serie de la caja de envío al departamento central de informática. Activan el dispositivo en la solución centralizada Astaro Security Gateway. El empleado local conecta el dispositivo al enrutador de Internet, conecta el enrutador al ordenador y lo conecta a la pared. El dispositivo RED recupera automáticamente su información de configuración, se configura automáticamente y establece un túnel cifrado en la oficina central. Puede implementar hasta 100 dispositivos al día con esta solución automatizada y flexible.

Cuatro pasos sencillos para garantizar la seguridad de las sucursales:



Soporte central

RED ofrece un mayor control y visibilidad de la red. Su personal de TI ahora cuenta con una solución integrada que admite herramientas centralizadas de generación de informes, que ofrecen una visibilidad de 360 grados en cada sucursal. RED elimina el desplazamiento a las sucursales, y permite a su equipo de TI de la oficina central dar soporte al personal de sus sucursales con tan solo unos clics del ratón.

Gestión sencilla de políticas

Gracias a RED, puede crear y mantener una política global que proteja y realice un seguimiento de todas las oficinas remotas en su puerta de enlace de seguridad centralizada. Puede establecer distintos derechos de usuario para empleados o sucursales individuales, al igual que en las oficinas centrales. Por tanto, la sucursal obtiene el mismo nivel de seguridad que la oficina central.

Un ahorro de hasta un 80% del coste total de la propiedad (TCO)

Compare el coste total de la propiedad (TCO) para mantener su red de sucursales, especialmente una con decenas o incluso cientos de sucursales, con soluciones UTM tradicionales. Los costes iniciales son insignificantes en comparación con los gastos constantes, desde la administración remota hasta las suscripciones de seguridad. Dichos gastos proceden principalmente de tratar cada sucursal como un entorno independiente que debe configurarse, protegerse y supervisarse. Este método UTM tradicional origina una seguridad uniforme, pero es extremadamente compleja y mucho más costosa que Astaro RED.

La tabla que aparece a continuación muestra los importantes ahorros de Astaro RED con respecto a otras soluciones Unified Threat Management:

Comparación del coste total de la propiedad (TCO) (30 oficinas remotas: 5 años)	Mercado	Astaro
Dispositivo de oficina central (1x)		ASG 220
Dispositivo	€2,995	€1,275
Mantenimiento de hardware de forma ininterrumpida (5 años)	€3,745	€1,180
Suscripciones de seguridad (5 años)	€5,015	€10,155
Dispositivo de oficina remota (30x)		Astaro RED
Dispositivo	€8,850	€8,850
Mantenimiento de hardware de forma ininterrumpida (5 años)	€11,100	€4,500
Suscripciones de seguridad (5 años)	€8,400	€0
Herramientas centralizadas de generación de informes		Incluidas
Dispositivo	€6,746	€0
Software (5 años)	€11,245	€0
Herramientas de gestión centralizada		Incluidas
Dispositivo	€4,496	€0
Software (5 años)	€7,495	€0
Costes de administración		
Configuración inicial de la oficina central	€545 (3 h/oficina)	€34 (1 hora)
Configuración inicial de la oficina remota	€3,068 (3 h/oficina)	€256 (15 min/oficina)
Mantenimiento constante de la oficina remota	€16,364	€0
Costes de desplazamiento	€17,591	€0
Total	€107.655	€26,250
Ahorro		**76%**

Resumen

Astaro RED es la mejor forma de gestionar la seguridad para sucursales.

Descubra cómo puede sacar partido de RED, el nuevo estándar de gestión de seguridad innovadora y rentable para sucursales.

Si desea obtener información adicional, visite nuestro sitio web esp.sophos.com/network

Lea más

esp.sophos.com/network

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

Sophos Whitepaper 12.11v1.dES

SOPHOS