

STORMSHIELD

Trusted SD-WAN: la combinación de rendimiento y seguridad

2022

Contenidos

04

¿Por qué es necesaria la **implementación de SD-WAN?**

07

La ciberamenaza de los Estados nación

11

SD-WAN: **mejora** de la experiencia de las aplicaciones

14

SD-WAN: **adaptabilidad** para diferentes usos

17

La necesidad de comunicaciones seguras

20

Gestión **eficaz de SD-WAN**

23

Trusted SD-WAN: **la opción que proporciona tranquilidad**

27

Trusted SD-WAN de Stormshield: **seguridad y confianza todo en uno**

Las organizaciones se han embarcado en cambios estructurales y digitales que ofrecen una mejor experiencia a sus empleados y clientes, así como mejoras en sus procesos de TI.

Por este motivo, la red de área extendida definida por software (SD-WAN) tiene un papel que desempeñar en la necesaria transformación digital de las empresas, ya que esta tecnología simplifica la tarea de gestionar las redes en diferentes sitios al tiempo que racionaliza los costes.

Este enfoque es una forma innovadora de mejorar el rendimiento y unificar la conectividad en diferentes redes, incluida la nube híbrida. SD-WAN permite a las empresas **adaptar dinámicamente el tráfico** de Internet en función de sus necesidades de prioridad y calidad de ancho de banda en cada ubicación.

Sin embargo, para proteger mejor su infraestructura, **la tecnología SD-WAN debe ser segura y de confianza** para hacer frente a las ciberamenazas y a las situaciones geopolíticas.

En un mercado saturado, ya no basta con gestionar interconexiones fiables, sino que también se necesitan elementos de protección (filtrado de flujos, túneles VPN, filtrado de URL, detección de intrusiones, etc.) para las distintas redes. Esto garantiza la seguridad del acceso a la WAN y la protección de los usuarios en cualquier circunstancia. Para hacer una elección acertada, hay que tener en cuenta como mínimo los cuatro aspectos siguientes: rendimiento, coste, seguridad y confianza.

Este libro blanco describe **los diferentes aspectos que una organización debe tener en cuenta a la hora de implementar un estrategia SD-WAN** de confianza: en otras palabras, un enfoque tecnológico seguro y de confianza. Este documento está dirigido a consultores y responsables de seguridad TI para ayudarles a entender los retos de Trusted SD-WAN en la actualidad.

¿Por qué es necesaria la **implementación de SD-WAN**?

#1

¿POR QUÉ ES ESENCIAL SD-WAN?

La transformación digital que han experimentado las empresas ha cambiado las prácticas de los usuarios de las aplicaciones que antes estaban en las instalaciones locales y eran utilizadas por los empleados que trabajaban desde las oficinas de la empresa. Ahora, las comunicaciones entre sedes pueden seguir realizándose mediante conexiones MPLS[1] para enlazar las distintas sedes de la organización, pero el coste suele ser significativo.

Del mismo modo, el uso de aplicaciones basadas en la nube (Microsoft 365, Salesforce, etc.) se ha identificado como un segundo aspecto importante:

Esta transformacióndel negocio está contribuyendo a aumentar las demandas de las WAN en ambas situaciones.

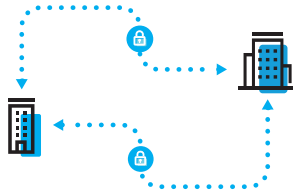
Como resultado, la forma en que fluyen los datos ha evolucionado, y las empresas están recurriendo gradualmente a la SD-WAN en su intento de seguir siendo competitivas y de hacer frente a los distintos retos tecnológicos.

SD-WAN es un paradigma de arquitectura que permite la **creación de una red de área extendida multi-sitio, y asegura un acceso de alta calidad y alta disponibilidad a las aplicaciones SaaS[2] / Web,**

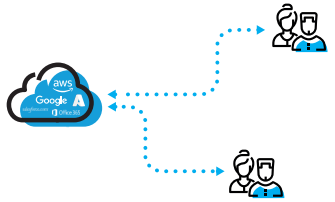
todo ello gestionado desde un punto central.

Esta tecnología está demostrando ser una estrategia atractiva para la optimización de costes. Como su nombre indica, está *definida por software* porque permite el control automático de los datos a través del software para conseguir un **mejor rendimiento y resiliencia de las aplicaciones.**

Puede gestionar el tráfico de la red a partir de políticas centralizadas basadas en diferentes criterios como la aplicación, el usuario, la hora del día, etc. El resultado es una WAN más rápida y fiable.



Comunicaciones seguras entre sedes



Conexiones de calidad hacía aplicaciones web
(AWS, Salesforce, Microsoft 365, etc.)

1 Creado a mediados de los 90, MultiProtocol Label Switching es una red privada que no transita por Internet. Es una tecnología que se utiliza cada vez menos.
2 SaaS: Software as a Service. Source

UNA ABUNDANTE OFERTA DE SERVICIOS

> *A medida que las empresas de TI amplían la operativa de su negocio a nivel global y migran a plataformas en la nube, aumenta la demanda del mercado de una* ***arquitectura WAN robusta y segura*** *para lograr una alta conectividad y mejorar el rendimiento de la red.*
>
> **— Global Market Insights**

Los cambios en las prácticas de uso han contribuido al crecimiento de las SD-WAN, que permiten una mejor gestión de las comunicaciones entre sedes y acceso a los servicios Web/SaaS. Este cambio en los requisitos de las SD-WAN está dando forma al mercado, que se construye en torno a muchos actores.

Entre los actores históricos del sector de las redes y la ciberseguridad y los proveedores de servicios en la nube, existe una gran cantidad de opciones. La elección se basa en la propuesta de valor a través de varios criterios: agilización de los enlaces WAN, simplicidad de despliegue, facilidad de gestión y supervisión, seguridad de las comunicaciones, etc.

Por lo tanto, **la elección de la solución SD-WAN se basa esencialmente en los casos de uso que se van a implementar,** así como en la estructura de la empresa y su sensibilidad a las ciberamenazas.

Por ejemplo, una empresa que utiliza soluciones SaaS para sus aplicaciones empresariales críticas tenderá a optar por un proveedor en la nube. Una organización con múltiples sedes buscará un despliegue fácil, especialmente para sus sucursales más pequeñas. Y una empresa sensible a la ciberseguridad, por su campo de actividad o sus competencias, recurrirá a un proveedor de soluciones de ciberseguridad.

La ciberamenaza de los Estados nación

#2

Más que nunca, la geopolítica internacional y europea está convirtiendo la ciberseguridad en una cuestión estratégica:

El entorno geopolítico es tenso y los ciberataques están cada vez más organizados y se caracterizan por los siguientes elementos[1]: velocidad, escalabilidad, replicabilidad y complejidad, lo que da al atacante una ventaja estructural. Como señala Philippe Piron, Presidente de GE Power Conversion & Grid Solutions[2] , *"los atacantes están en todas partes, son difíciles de detectar e identificar, son creativos y desarrollan rápidamente nuevos ataques [...]"*.

Ante este reto, los gobiernos nacionales no se quedan de brazos cruzados, sino que se arman de herramientas cibernéticas, ya sea directamente o con ayuda de grupos organizados.

Como señala el profesor Mike McGuire[3], catedrático de Criminología de la Universidad de Surrey (Reino Unido), los estados-nación invierten cada vez más *"tiempo y recursos en la obtención de ventajas cibernéticas estratégicas para promover sus intereses nacionales, su capacidad de recopilación de información y su poder militar mediante el espionaje y el robo"*.

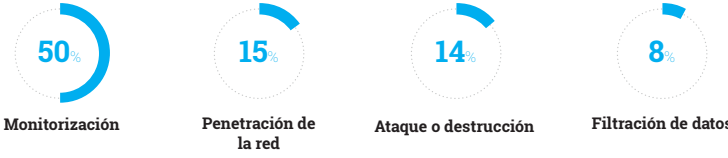
Las empresas de alto valor añadido (industriales, farmacéuticas, etc.) son las primeras en la línea de fuego; sin embargo, de forma más general, el 82%[4] de las organizaciones cree que la geopolítica y la ciberseguridad están estrechamente relacionadas.

Por lo tanto, una evaluación frecuente de **los riesgos de los ataques de los estados-nación debería ser una consideración en la estrategia de protección** de cada organización. Como señala Kevin Bocek[5], vicepresidente de Estrategia de Seguridad e Inteligencia de Amenazas de Venafi *"Todas las organizaciones deben reforzar las medidas para gestionar sus activos de seguridad críticos"*.

Principales obejtivos de los ciberataques



Principales ciberarmas empleadas



1 Philippe Piron en Ciberdefensa: la nueva arma geopolítica. Source
2 *Ibid.*
3 Usine digitale. Source
4 Global Security Mag. Source
5 *Ibid.*

SD-WAN AND CYBERSECURITY

SD-WAN garantiza conexiones de alta disponibilidad y calidad entre las ubicaciones y hacia las aplicaciones en la nube de manera eficiente y flexible.

Sin embargo, la proliferación de nuevas prácticas de uso de la Web / SaaS conlleva un aumento de los riesgos (dependencia de Internet, aplicaciones de terceros, etc.).

En consecuencia, deben aplicarse capas de seguridad adicionales dentro de la arquitectura SD-WAN para reducir el importante peligro de intrusiones y vigilancia de sus comunicaciones sensibles.

En resumen, la conectividad y la criticidad de las comunicaciones de las WAN, que son fundamentales para todos los intercambios dentro de una organización, **requieren una capa de seguridad y confianza para garantizar la confidencialidad de los datos una vez desplegada la SD-WAN.**

El

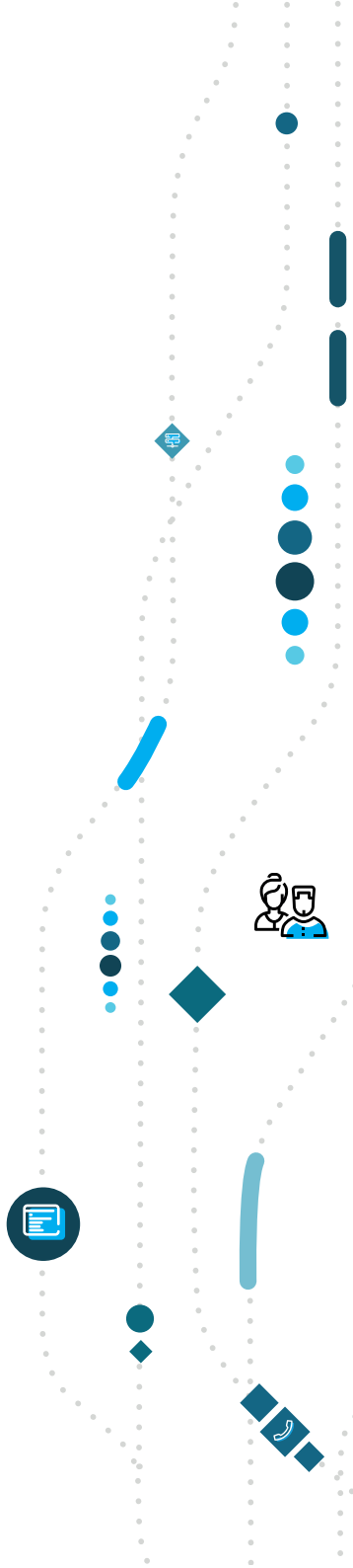
80%

de las implantaciones de SD-WAN incorporarán requisitos de servicios de seguridad en los próximos años, según Gartner.

Algunos actores siguen siendo reacios a establecer las reglas del juego para los enfrentamientos en el ciberespacio. Por lo tanto, **podríamos enfrentarnos a una escalada rápida e incontrolada**, *que llevaría a crisis sin precedentes y a efectos en cascada imprevistos".*

— Florence Parly
Ministra de las Fuerzas Armadas

Declaración en Ciber Securidad y Ciber Defensa, 8 de septiembre de 2021



SD-WAN: **mejora** de la experiencia de las aplicaciones

#3

Como se ha mencionado anteriormente, las implementaciones de SD-WAN se han adaptado a las nuevas prácticas de los usuarios y a la transformación digital que están experimentando las organizaciones. Como informa IDC, el 70% de las aplicaciones serán nativas de la nube en 2024.

Y esto exige una conexión de alta calidad. Sin embargo, esta puede ser inestable (pérdida de paquetes y/o retrasos en la recepción). En consecuencia, pueden surgir preguntas legítimas: ¿cómo se puede garantizar una calidad estable para las aplicaciones críticas para el negocio? ¿Qué calidad de vídeo y audio necesitan los usuarios? ¿Para cuántas ubicaciones?

SD-WAN optimiza el ancho de banda, mejorando el rendimiento para las diferentes necesidades (VoIP, vídeo, flujos de impresión, transferencias de archivos, aplicaciones SaaS, etc.). Esto garantiza la continuidad del servicio y una experiencia óptima para todos los empleados.

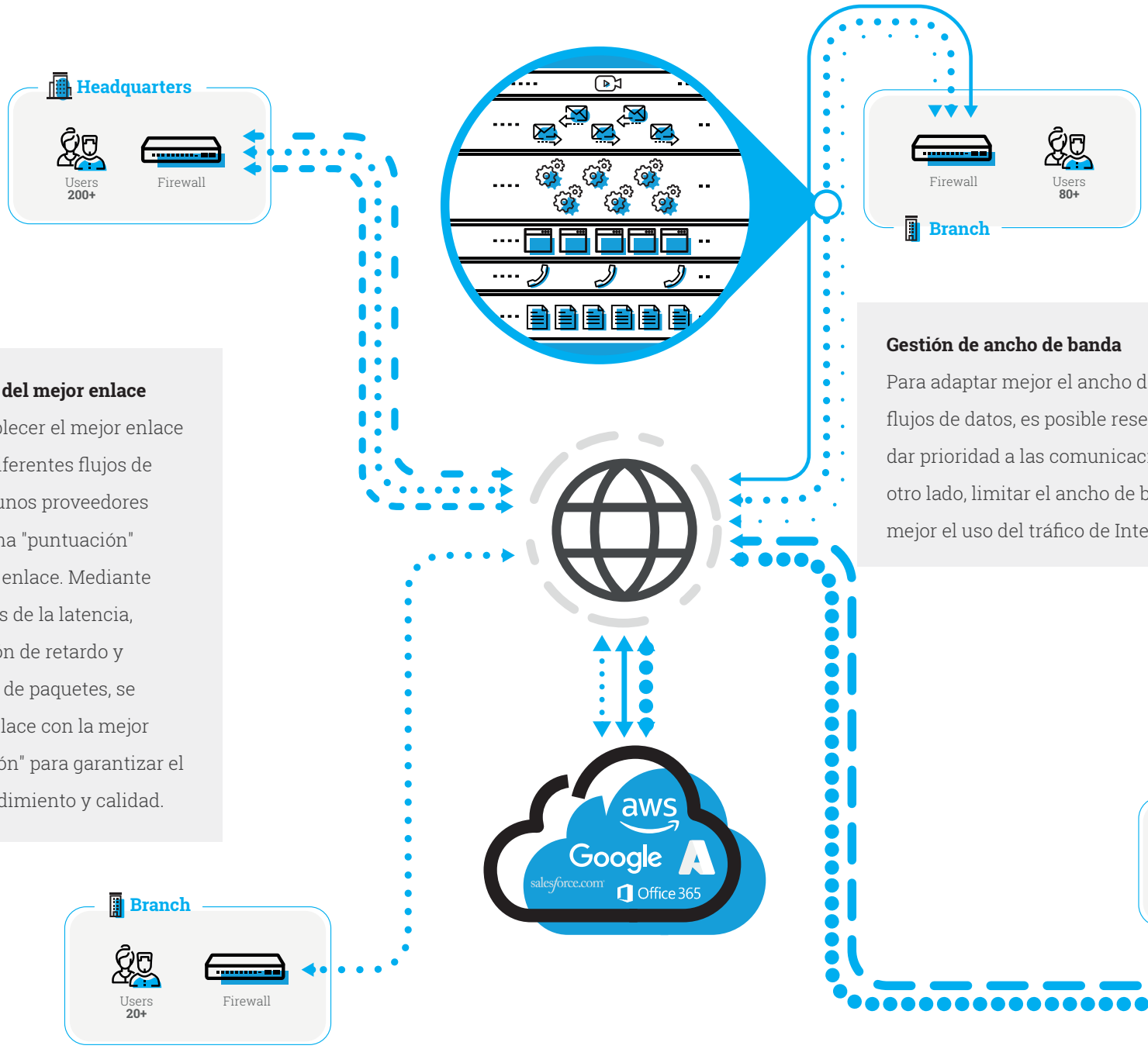
Más de **214** **mil millones de dólares** se han gastado en servicios de nube pública en 2019[1]

1 Stéphane Chmielewski, *¿Por qué SD-WAN es uno de los pilares de la transformación digital?* Fuenteource

LA MEJOR SELECCIÓN DE ENLACE Y GESTIÓN DE ANCHO DE BANDA

Con múltiples accesos WAN (Internet, sucursales, etc.) y la aparición de la nube, **SD-WAN ofrece una ventaja real, con mayores velocidades y un atractivo ratio de costes**, evitando la necesidad de invertir en costosos enlaces. Esto garantiza una conectividad y un rendimiento fiables en todo momento.

Para gestionar mejor el ancho de banda y lograr el nivel de servicio adecuado, es importante buscar soluciones que mejoren los tiempos de respuesta en las aplicaciones y/o flujos utilizados desde diferentes ubicaciones para una mejor calidad de servicio.



Selección del mejor enlace

Para establecer el mejor enlace para los diferentes flujos de datos, algunos proveedores ofrecen una "puntuación" para cada enlace. Mediante un análisis de la latencia, la variación de retardo y la pérdida de paquetes, se elige el enlace con la mejor "puntuación" para garantizar el mejor rendimiento y calidad.

Gestión de ancho de banda

Para adaptar mejor el ancho de banda a los distintos flujos de datos, es posible reservarlo, por ejemplo, para dar prioridad a las comunicaciones entre sedes. Por otro lado, limitar el ancho de banda permite gestionar mejor el uso del tráfico de Internet.

SD-WAN: **adaptabilidad** para diferentes casos de uso

#4

RECONOCIMIENTO DE APLICACIONES

La estrategia de SD-WAN se centra cada vez más en la optimización de la infraestructura para reducir los costes y mejorar el acceso a las aplicaciones entregadas desde la nube.

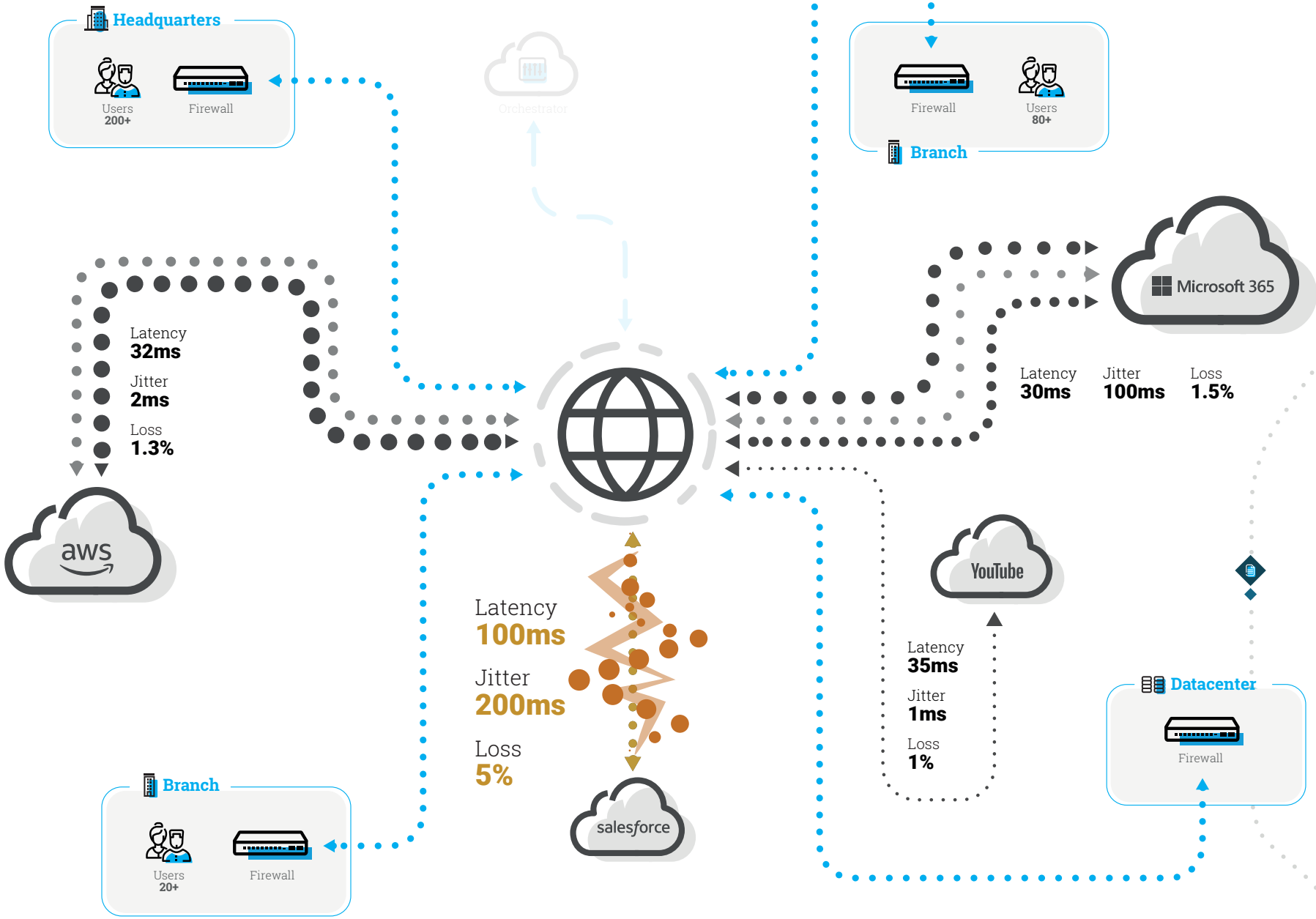
Esta transformación de la arquitectura SD-WAN gira en torno a mantener la calidad de la experiencia del usuario. Por ello, la mayoría de los proveedores optan ahora por un reconocimiento profundo de los datos que pasan por los flujos (por ejemplo, HTTPS).

Esto facilita la distinción entre las diferentes aplicaciones en la nube (estándar o personalizadas). **Esta identificación mejora la visibilidad y garantiza el establecimiento de políticas específicas de calidad de servicio (QoS) y acuerdos de nivel de servicio (SLA) para cada aplicación.**

Estas soluciones garantizan un alto rendimiento para las distintas aplicaciones SaaS utilizadas (Zoom, AWS, Salesforce, Google, etc.), así como las que están en contacto directo con los clientes.

Para un mejor análisis del tráfico de red, no hay que olvidar que el componente de seguridad debe estar presente para garantizar una buena protección de los intercambios.

Esto incluye el filtrado integral del tráfico web en tiempo real, el análisis DPI IPS para eliminar cualquier riesgo de incumplimiento de los paquetes que pasan por la infraestructura, y la inspección SSL de los distintos protocolos web para garantizar que las prácticas de uso se ajustan a la política de seguridad establecida.


Headquarters
Users
200+
Firewall
Orchestrator
Firewall
Users
80+
Branch
Microsoft 365
Latency
32ms
Jitter
2ms
Loss
1.3%
Latency
30ms
Jitter
100ms
Loss
1.5%
aws
Latency
100ms
Jitter
200ms
Loss
5%
YouTube
Latency
35ms
Jitter
1ms
Loss
1%
Datacenter
Firewall
salesforce
Branch
Users
20+
Firewall

La **necesidad** de comunicaciones **seguras**

#5

COMUNICACIONES SEGURAS

La confidencialidad e integridad de los datos, ligada a la criticidad de las comunicaciones WAN dentro de una empresa, se garantiza proporcionando comunicaciones seguras entre ubicaciones. **Los datos críticos deben ser cifrados para garantizar que no puedan ser utilizados por nadie que no tenga derecho a acceder a ellos.**

VPN iPsec ha sido una parte esencial de las WAN durante muchos años. Se trata de un protocolo con un conjunto de normas que permite conectar de forma segura diferentes comunicaciones de una WAN a través de Internet. Este método de interconexión puede utilizarse para todos los propósitos, a todos los destinos sin apenas coste.

Por esta razón, **las SD-WAN deben ofrecer un cifrado robusto de extremo a extremo**. En consecuencia, la seguridad de los datos que transitan entre las distintas ubicaciones de una empresa debe garantizarse mediante la implementación de túneles VPN. IPsec

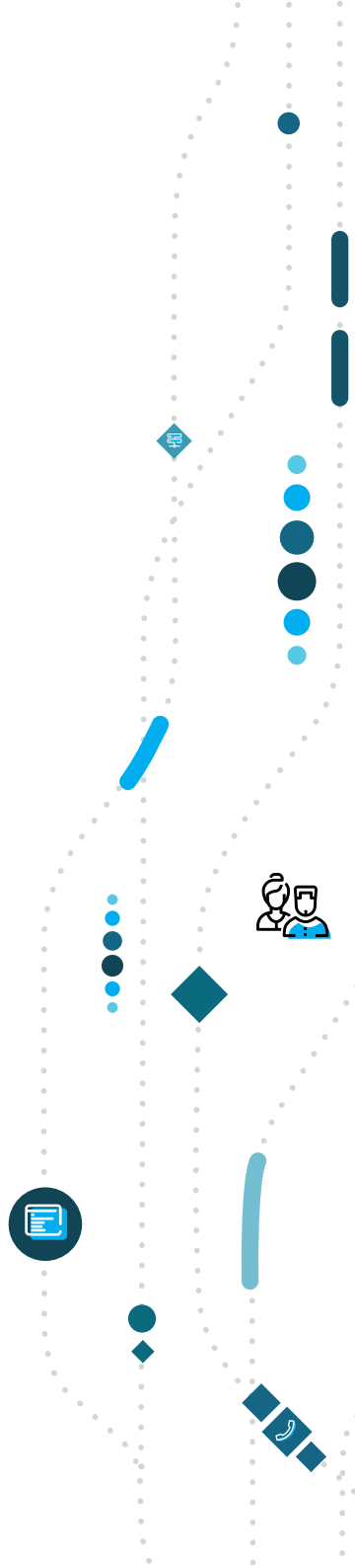


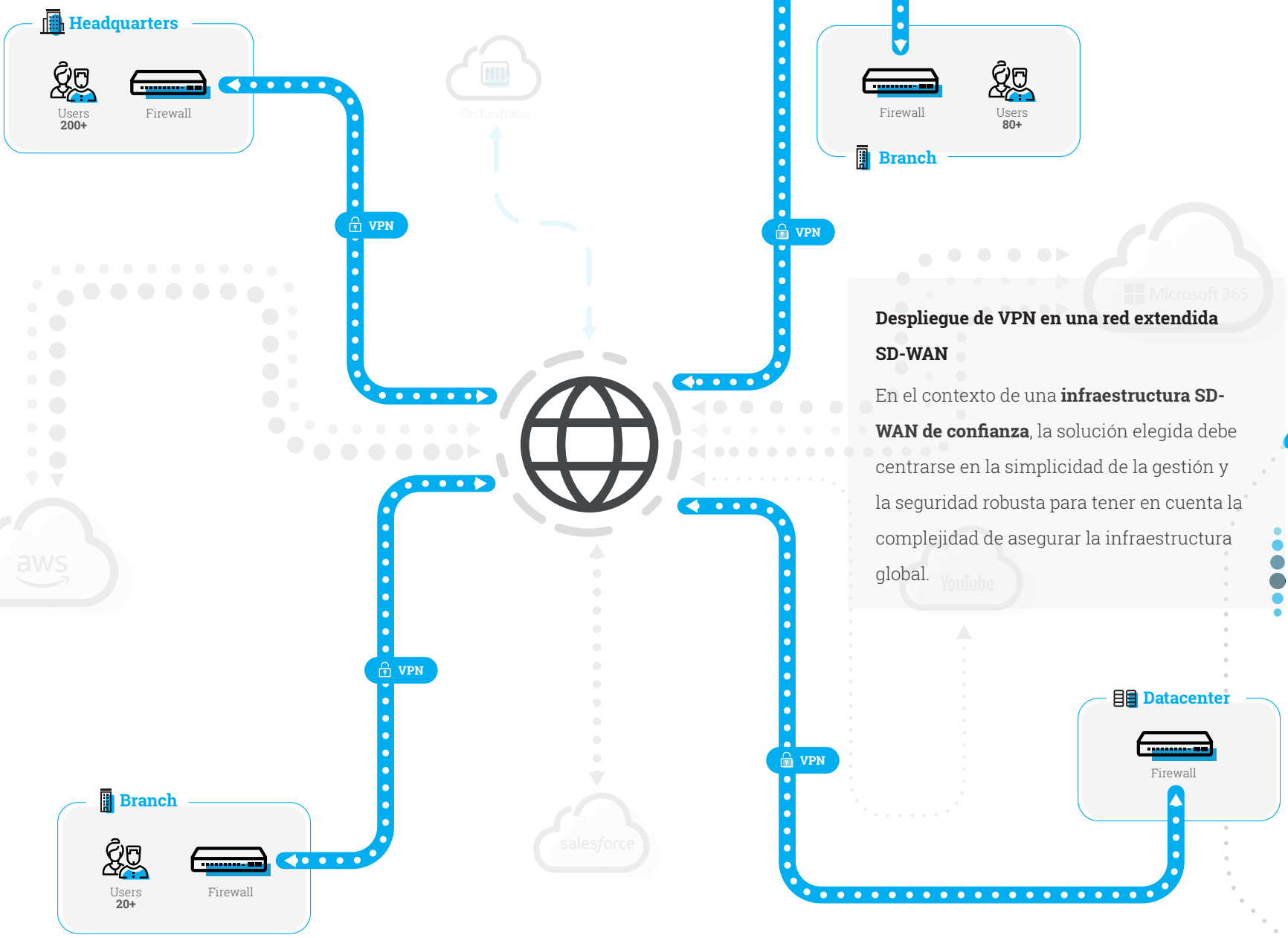
¿Sabía qué?

Para aumentar el nivel de seguridad de forma efectiva, VPN IPsec puede utilizarse como medida de seguridad complementaria para **"encapsular protocolos que ya están protegidos por otros mecanismos**[1]".

ANSSI-NT_ Guía IPsec Fuente







Despliegue de VPN en una red extendida SD-WAN

En el contexto de una **infraestructura SD-WAN de confianza**, la solución elegida debe centrarse en la simplicidad de la gestión y la seguridad robusta para tener en cuenta la complejidad de asegurar la infraestructura global.

Gestión eficaz de SD-WAN

#6

La implantación de una arquitectura SD-WAN basada en la gestión centralizada facilita el despliegue y la actualización de la infraestructura, al tiempo que proporciona una visibilidad global.

Por ejemplo, desde una única consola de gestión, se pueden desplegar o modificar las funciones de seguridad y las políticas de enrutamiento en varias ubicaciones, en lugar de enviar a un técnico a la ubicación.

Con unos pocos clics, también es posible definir las distintas interacciones entre las ubicaciones antes de que el orquestador se encargue de configurar todos los equipos de conexión y seguridad.

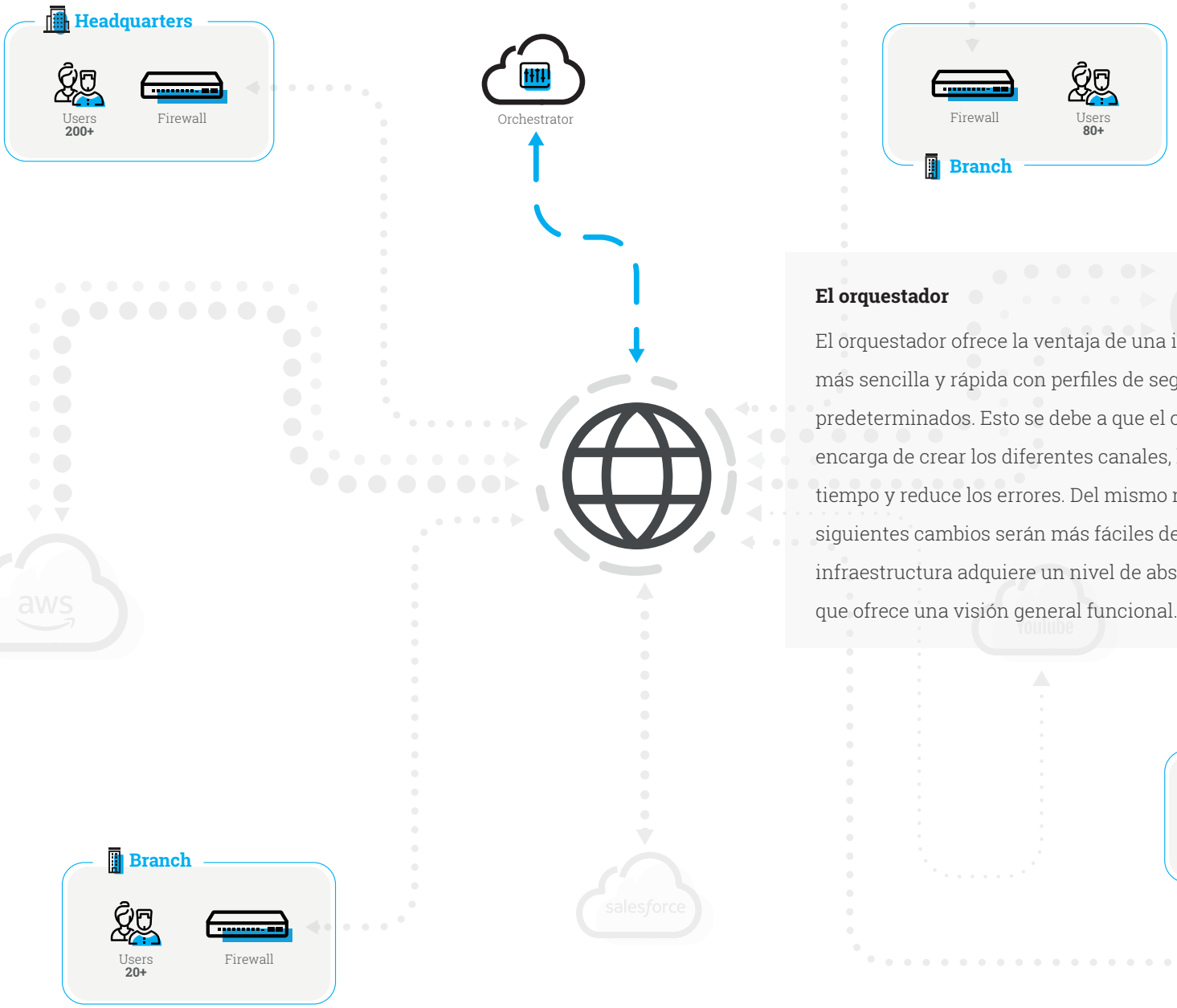
ORQUESTACIÓN

Además, la visión de conjunto que ofrecen las soluciones de orquestación garantiza una **visión de 360º del estado de la infraestructura y del rendimiento de cada aplicación.** Esta monitorización también ofrece la posibilidad de informar de los indicadores SLA (latencia, variación de retardo, pérdida de paquetes) sobre la calidad del enlace.

Esta visión global permite poner en marcha una política eficaz de gestión del ancho de banda (QoS) para garantizar una conectividad fiable en todo momento. Por último, esta visión general proporciona una visión útil del uso de las TI en la sombra.

En resumen, la solución de orquestación elegida debe **proporcionar la capa de confianza necesaria en la seguridad de la red, facilitando al mismo tiempo una configuración simplificada**. Sus funciones de supervisión pueden monitorizar los indicadores de calidad de los enlaces, al tiempo que permiten la gestión de eventos (registros de log) e incidentes de seguridad.

.



El orquestador

El orquestador ofrece la ventaja de una implementación más sencilla y rápida con perfiles de seguridad predeterminados. Esto se debe a que el orquestador se encarga de crear los diferentes canales, lo que ahorra tiempo y reduce los errores. Del mismo modo, los siguientes cambios serán más fáciles de implementar. La infraestructura adquiere un nivel de abstracción técnica que ofrece una visión general funcional..

Trusted SD-WAN: **la opción que proporciona tranquilidad**

#7

TRUSTED SD-WAN

Como se ha mencionado anteriormente, SD-WAN agiliza las comunicaciones remotas y el acceso a la nube, pero la seguridad también debe formar parte de la ecuación. Una pregunta legítima es: ¿existen arquitecturas SD-WAN seguras que estén certificadas y/o aprobadas por un organismo de certificación independiente?

En la actualidad, nos encontramos con que no hay certificaciones o calificaciones de SD-WAN independientes de los proveedores que promuevan este enfoque tecnológico.

Por lo tanto, es importante tener elementos prácticos con los que juzgar objetivamente la solución SD-WAN elegida. A la hora de seleccionar un proveedor entre varias soluciones de hardware y software, es necesario plantearse cuestiones como la solidez del producto y la fiabilidad con respecto a cuestiones geopolíticas y económicas.

En primer lugar, como señala la ANSSI[1], la robustez "*consiste en probar su capacidad de resistencia a los ataques informáticos según un contexto de uso y un nivel de amenaza definidos*".

Por lo tanto, deben preferirse las soluciones que tengan en cuenta este aspecto para la seguridad global de la infraestructura SD-WAN.

En segundo lugar, es importante que el concepto de confianza se incluya claramente en la estrategia del producto para cumplir los compromisos adquiridos con un organismo oficial de certificación/calificación.

En resumen, dada la falta de certificación oficial de SD-WAN, es necesario confiar en las diversas certificaciones/calificaciones de productos y en las diversas normas de seguridad proporcionadas por las autoridades gubernamentales para obtener una arquitectura de tipo SD-WAN de confianza

.

¿Sabía qué?

Fortalecimiento es el proceso para hacer un sistema más seguro.

Este enfoque consiste en **reducir los componentes de software instalados en el sistema, las herramientas, los usuarios y los derechos no esenciales al nivel mínimo necesario**, sin dejar de ofrecer las prestaciones necesarias para un buen funcionamiento.

1 ANSSI, Fuente

GARANTIZAR LA CALIDAD DEL SOFTWARE

Las conexiones a ubicaciones remotas y el acceso a la nube a través de SD-WAN aumentan la conectividad, pero también pueden aumentar los riesgos de seguridad si no se tiene en cuenta este componente, ya que las soluciones que componen la SD-WAN representan un objetivo de ataque para los ciberdelincuentes. Además, como señala la ANSSI[1], los elementos de software para una determinada infraestructura deben ser revisados y su configuración fortalecida antes de ser utilizados.

Asimismo, como se ha mencionado anteriormente, se debe dar **prioridad a los desarrolladores de confianza que puedan ofrecer productos calificados o certificados** por organizaciones legítimas de terceros, como la ANSSI en Francia, el CCN en España, la BSI en Alemania y ENISA a nivel europeo. Esto se debe a que garantizan el cumplimiento de los requisitos normativos, técnicos y de seguridad.

Esto garantiza una protección robusta del producto, y como indica la ANSSI [...] es un "*compromiso del proveedor de la solución para cumplir con los criterios de confianza*"[2]. Además, para lograr un alto nivel de robustez, los productos deben demostrar su resistencia a los ciberataques según un marco específico. Esto incluye una auditoría del código fuente del producto en cuestión.

Como acabamos de ver, hoy en día no existen en el mercado soluciones SD-WAN certificadas y/o calificadas. Para llenar este vacío, es necesario analizar previamente la información de forma independiente para elegir uno o varios proveedores que ofrezcan productos robustos y de confianza (preferiblemente cualificados), con funcionalidades SD-WAN (orquestación, optimización de la QoS, etc.) y opciones de seguridad (cortafuegos, filtrado de flujos, VPN, etc.), garantizando un paquete eficaz que proteja su infraestructura en todo momento.

VPN IPsec
Protegiendo interconexiones con información reservada

"Las interconexiones entre sistemas de información con información reservada deben de protegerse con túneles VPN que protejan el intercambio de flujos (confidencialidad, integridad, anti-reproducción, autenticación mutua de puntos finales). Para este propósito, la organización ha definido un protocolo VPN IPSec de información reservada.

ANSSI, Guía ANSSI-PG-075 Fuente

1 ANSSI en la Guía que ofrece recomendaciones para arquitecturas y sistemas de información sensible. Fuente
2 ANSSI. Fuente

Los 4 puntos clave
a la hora de elegir su SD-WAN confiable

#1

Optar, siempre que sea posible, por un proveedor reconocido por un organismo oficial e independiente (ANSSI, CCN, etc.)

#2

Asegúrese de que el proveedor dispone de los elementos SD-WAN y de seguridad necesarios para una mejor cobertura funcional. Arquitectura segura "todo en uno": uso de un dispositivo para proporcionar SD-WAN unificada, cortafuegos y conexiones seguras de extremo a extremo, entre otros.

#3

Favorecer las tecnologías que ofrecen una visibilidad unificada. Gestión optimizada y centralización mejorada de las diferentes funciones.

#4

Disponga de una gestión eficiente de las aplicaciones en la nube (Microsoft 365, Salesforce, etc.)

Trusted SD-WAN por Stormshield: **seguridad y confianza todo en uno**

#8

Stormshield le ayuda **en la integración de Trusted SD-WAN** en su infraestructura, **de forma segura y eficaz**



Gestione fácilmente su red extendida

Con las capacidades SD-WAN de Stormshield, **centralice y controle sus conexiones entre ubicaciones y el acceso a la nube** para su infraestructura ampliada.



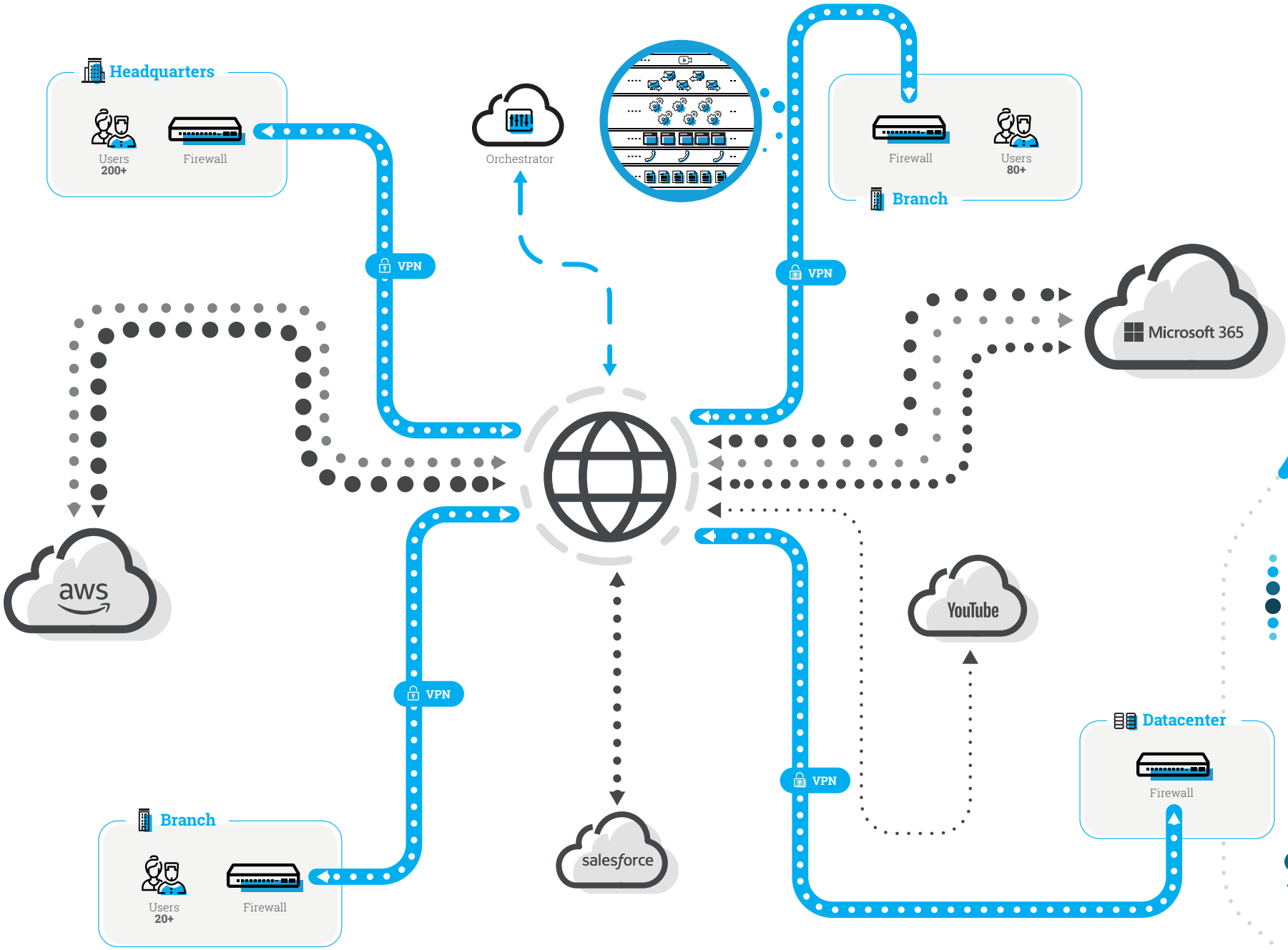
Proteja su SD-WAN en todo momento

Gane en tranquilidad con la tecnología SD-WAN segura de Stormshield **para una protección inigualable de todas sus conexiones.** Sus empleados tendrán acceso seguro a los recursos de la empresa, estén donde estén y desde cualquier dispositivo.



Elija su SD-WAN confiable

Basada en tecnología certificada según las normas europeas más estrictas, la SD-WAN de Stormshield le ofrece la confianza necesaria para garantizar la ciberseguridad de su infraestructura.


Headquarters
Users
200+
Firewall
Orchestrator
Firewall
Users
80+
Branch
VPN
VPN
Microsoft 365
aws
YouTube
VPN
VPN
VPN
Datacenter
Firewall
salesforce
Branch
Users
20+
Firewall

LA **OPCIÓN EUROPEA** EN **CIBERSEGURIDAD**

www.stormshield.com

Queda prohibida toda distribución, reproducción o representación, incluso parcial, de este libro blanco, para cualquier fin que no sea el uso privado, independientemente del soporte, y puede comprometer la responsabilidad civil y penal de cualquier persona que incumpla esta prohibición.

Copyright © 2022 Stormshield