CISCO
SECURE

Informe técnico
Información pública de Cisco

El futuro del firewall

Logre una postura más sólida hoy en día y construya un puente para satisfacer las demandas comerciales y de seguridad del futuro

cisco The bridge to possible

Contenido

Resumen 3

Sección 1: Historia del firewall 4

Sección 2: Del firewall al firewalling 6

Sección 3: Cuatro pasos para configurar la estrategia de firewalling 10

Sección 4: Una solución de seguridad preparada para el futuro 12

Sección 5: Comience a construir el futuro del firewall hoy mismo 12

© 2020 Cisco o sus filiales. Todos los derechos reservados.

Resumen

El propósito de este informe técnico es analizar la evolución de la seguridad de la red y lo que se necesitará para proteger el entorno de una organización en el futuro.

A medida que las redes se vuelven más heterogéneas, a las organizaciones les resulta cada vez más difícil lograr una administración y una aplicación de políticas uniformes y mantener una visibilidad unificada. La complejidad de estas redes interconectadas, a menudo, conduce a errores o configuraciones incorrectas, lo que las torna vulnerables a amenazas sofisticadas en constante evolución.

¿Qué puede hacer una organización para recuperar el control y lograr la uniformidad? Comienza con un enfoque integrado de la seguridad que coloca el firewall al frente y en el centro.

Los firewalls siguen siendo la piedra angular de la estrategia de seguridad de la red de una organización pero, así como las redes han evolucionado, también lo deben hacer nuestros firewalls. En el pasado, el firewall era el único dispositivo en el "perímetro" de entrada/salida que actuaba como punto de control impulsado por políticas para permitir o denegar el tráfico de red. Para tener éxito en el mundo digital actual, las organizaciones deben pensar más allá de los firewalls individuales y adoptar el "firewalling", un método impulsado por políticas que coordina estratégicamente las protecciones de seguridad avanzadas en los puntos de control lógicos en las redes heterogéneas.

El firewalling será un paso fundamental para que las organizaciones alineen mejor la seguridad con las cambiantes necesidades empresariales y de la red. Cisco ha trabajado arduamente para crear una plataforma de seguridad integrada con nuestro firewall como base para que las empresas puedan realizar la transición.

"Los firewalls siguen siendo la piedra angular de la estrategia de seguridad de la red de una organización pero, así como las redes han evolucionado, también lo deben hacer nuestros firewalls".

Con el firewalling, las organizaciones que se transforman digitalmente pueden lograr una postura de seguridad más sólida en la actualidad, mientras construyen un puente para satisfacer las demandas comerciales y de seguridad del futuro.

© 2020 Cisco o sus filiales. Todos los derechos reservados.

Sección 1: Historia del firewall

La evolución de la seguridad de la red

Tradicionalmente, el firewall se colocaba como control de acceso en el perímetro de la red. Actuaba como punto de control integral que inspeccionaba el tráfico de red a medida que atravesaba el perímetro. En el punto de entrada/salida de la red, el firewall se encargaba de validar las comunicaciones: el tráfico de red interno se consideraba intrínsecamente confiable y el tráfico externo se consideraba inherentemente poco confiable. Se crearon y aplicaron conjuntos de reglas y políticas en este único punto de control para garantizar la entrada y salida del tráfico deseado y evitar el tráfico no deseado.

Si comparamos el perímetro de la red con un foso alrededor de un castillo, el firewall actuaba como puente levadizo que controlaba todo el tráfico que entraba y salía de la fortaleza.

Seguridad de la red tradicional

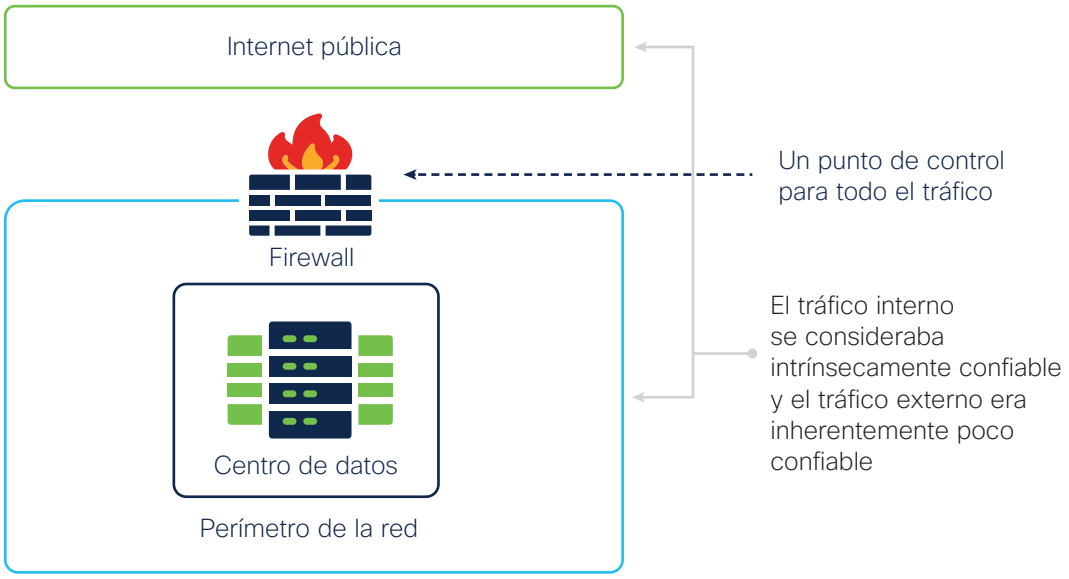


Figura 1. Enfoque tradicional del firewall de red.

Después llegó la nube. Y las aplicaciones.

No pasó mucho tiempo antes de que esta práctica de aplicación de la seguridad a través de un único punto de control fuera cuestionada. Primero, surgió el acceso remoto y la movilidad empresarial. Pero la transformación realmente comenzó con la computación en la nube. Cuando la empresa se trasladó a la nube, los dispositivos y los usuarios comenzaron a migrar en masa fuera de la red interna controlada, lo que hizo que el modelo de punto de control único fuera ineficaz. Pronto, había varios perímetros. Todos debían estar protegidos. No había una manera eficaz de colocar un foso alrededor de la red.

Hoy en día, las ubicaciones de las sucursales, los empleados remotos y el uso cada vez mayor de servicios en la nube alejan más datos del "perímetro" tradicional, eludiendo por completo el punto de control de seguridad tradicional. Además, muchas empresas han adoptado un modelo de uso de dispositivos propios (BYOD) que permite a los empleados acceder a aplicaciones empresariales confidenciales a través de sus computadoras privadas o dispositivos móviles. De hecho, más del 67 % de los empleados utilizan sus propios dispositivos en el trabajo, una tendencia en alza que no tiene fin. Los dispositivos móviles y las computadoras portátiles conectados a través de redes Wi-Fi de acceso público son frecuentes, incluso cruciales, para las operaciones comerciales diarias.

© 2020 Cisco o sus filiales. Todos los derechos reservados.

Además, la abrumadora mayoría de las ubicaciones empresariales y los usuarios también requieren acceso directo a Internet, donde actualmente se encuentra una mayor cantidad de aplicaciones y datos críticos basados en la nube. Las empresas continúan implementando cargas de trabajo en múltiples servicios en la nube, sistemas operativos, dispositivos de hardware, bases de datos y más. Las aplicaciones y los datos se descentralizan aún más y las redes se vuelven más diversas.

La nueva realidad

Este enfoque único para todos ha resultado ineficaz en el panorama actual.

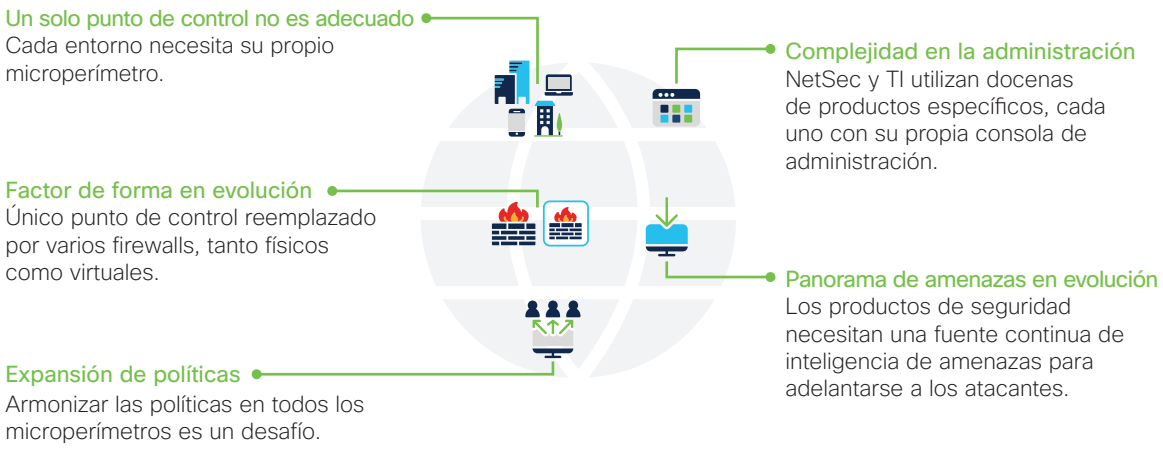
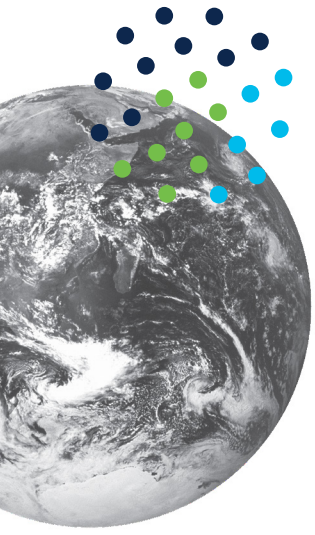


Figura 2. La complejidad de la red y las amenazas en evolución desafían el modelo tradicional del firewall.

Una realidad nueva y más compleja

Si bien estas innovaciones permiten un entorno de trabajo más interconectado y productivo, han cambiado la naturaleza misma de la forma en que hacemos negocios. Los días de controlar aplicaciones y autorizar usuarios en las instalaciones se han transformado en ecosistemas multinube dinámicos que ofrecen servicios y aplicaciones en las empresas. No solo eso, también administramos las relaciones con terceros cruciales para el negocio. La gran expansión y la subcontratación proporcionan economías de escala y eficiencia, pero no sin sacrificios. Esta evolución de las arquitecturas de red ha aumentado considerablemente nuestras superficies de ataque y ha hecho que el trabajo de proteger las redes empresariales, los datos y los usuarios sea sorprendentemente más complicado.



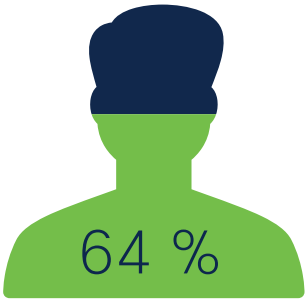
Contraataque con productos específicos

Por lo general, las organizaciones han intentado abordar estos desafíos agregando la "mejor" solución de seguridad puntual para tratar cada nuevo problema a medida que surge. Debido a este enfoque, hemos visto una enorme "proliferación" de dispositivos, con un uso empresarial promedio de hasta 75 herramientas de seguridad[1]. Varios productos de seguridad de diferentes proveedores pueden plantear problemas de administración importantes para los equipos de seguridad de la red. En la mayoría de los casos, la proliferación de dispositivos y capacidades de seguridad aumenta el riesgo de ataque. Cuando se les preguntó, al 94 % de los profesionales de TI e InfoSec les preocupaba que una mayor complejidad de la red los hiciera más vulnerables y el 88 % deseaba agilizar los cambios en las políticas de seguridad de la red[2].

Entre enero y julio de 2019, se expusieron 3800 infracciones de datos, un aumento del 54 % respecto de la primera mitad de 2018[3]. Esta fuerte subida es un testimonio de los métodos progresivamente sofisticados que los delincuentes utilizan para infringir las redes. La creciente tasa de infracciones exitosas también indica que los métodos tradicionales de seguridad de la red ya no resisten las amenazas modernas.

1 "Defensa en profundidad: deje de gastar, comience a consolidarse", CSO, 4 de marzo de 2016.
2 "Navegando por la complejidad de la seguridad de la red", informe de conocimientos de la investigación de ESG, junio de 2019.
3 "Navegando por la complejidad de la seguridad de la red", informe de conocimientos de la investigación de ESG, junio de 2019.

© 2020 Cisco o sus filiales. Todos los derechos reservados.



El **error humano** fue la causa principal de configuración incorrecta

Más amenazas, más ruido, incluso más riesgos

A medida que los terceros malintencionados atacan nuevos vectores, desde el correo electrónico hasta los endpoints no codificados en virtud de las políticas de BYOD, los portales web y los dispositivos de IoT, las organizaciones también se ven obligadas a probar cualquier otro enfoque para protegerse.

Como se mencionó anteriormente, la tendencia a agregar productos puntuales no mejora el estado general de seguridad de una organización. Es totalmente lo contrario. Genera más " ruido" para la administración de los equipos de seguridad. Si bien se esfuerzan por mantenerse atentos a nuevos ataques inevitables y malware que intenta aprovechar cualquier vulnerabilidad (conocida o desconocida), esta complejidad adicional hace que el trabajo de crear, administrar y aplicar políticas de seguridad sea cada vez más difícil.

En respuesta, los equipos de seguridad de la red tienen la tarea de configurar multitudes de recursos de la nube individualmente, lo que aumenta aún más la posibilidad de una configuración incorrecta de la seguridad que podría conducir a una infracción. Un control de seguridad que no se implementa o que se implementa con errores puede ser el mayor culpable: el 64 % de las organizaciones afirma que el error humano fue la causa principal de una configuración incorrecta[4]. Ya sea que un error de este tipo provoque una infracción de cumplimiento, una interrupción o abra la puerta a un adversario, es un riesgo que no puede afrontar.

Es hora de repensar el firewall

La seguridad de la red se ha convertido en una tarea desalentadora. El personal actual no puede seguir intentando administrar una amplia variedad de soluciones de seguridad puntuales, recursos en la nube y dispositivos. Es hora de adoptar un enfoque diferente.

Es hora de que el firewall tome su lugar como base para una plataforma de seguridad de red ágil e integrada que guíe a las empresas de hoy y el futuro.

Sección 2: Del firewall al firewalling

¿Por qué el firewalling?

A medida que nuestras redes evolucionan para adaptarse a nuevas formas de hacer negocios, también debe hacerlo la seguridad de la red. En el mundo actual de los recursos distribuidos de TI, el firewall sigue siendo fundamental para una postura de seguridad sólida.

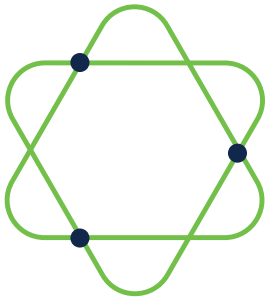
Sin embargo, los requisitos de firewall han aumentado significativamente para proteger la amplia gama de infraestructuras de red, dispositivos conectados y sistemas operativos contra amenazas avanzadas. En consecuencia, nuestros dispositivos de firewall " tradicionales" se ven aumentados por una combinación de dispositivos físicos y virtuales: algunos están integrados en la red mientras que otros se ofrecen como servicios, se basan en el host o se incluyen en entornos de nube pública. Algunos incluso adoptan nuevos factores de forma, como dispositivos en clústeres que se adaptan a grandes requisitos de tráfico, software que se ejecuta en dispositivos personales, routers SD-WAN y puertas de enlace de Internet seguras. La actividad de compartir inteligencia de amenazas a través de todos estos dispositivos de firewall dispares, independientemente de su ubicación, es vital para una visibilidad uniforme de las amenazas y una postura de seguridad sólida.

Para realizar el cambio completo y proteger mejor las redes actuales, las empresas deben alejarse del enfoque tradicional del " perímetro" . En cambio, deben establecer puntos de aplicación estratégicos en toda la estructura de la red, más cerca de la información o las aplicaciones que deben protegerse. Específicamente, la creación de microperímetros en los puntos de control físicos y lógicos se ha convertido en una realidad necesaria.

Debemos pensar menos en el firewall como un dispositivo de red físico independiente y más en la funcionalidad del *firewalling*.

4 " Infracciones a la seguridad de la nube y errores humanos" , Fugue, 7 de febrero de 2019.

© 2020 Cisco o sus filiales. Todos los derechos reservados.



¿Qué es el firewalling?

No se equivoque: el firewall es más relevante que nunca. De hecho, para proteger las redes actuales, necesitamos **más** firewalls **en todas partes**. La diferencia es que el firewalling se centra en **cómo** puede establecer controles basados en políticas en todas partes:

El firewalling puede proporcionar un enfoque ágil e integrado para centralizar las políticas, la funcionalidad de seguridad avanzada y la aplicación uniforme en las redes cada vez más complejas y heterogéneas. Debe ofrecer protecciones integrales, visibilidad, armonización de políticas y una autenticación de usuarios y dispositivos más sólida. El firewalling también deben beneficiarse del uso compartido de la inteligencia de amenazas en todos los puntos de control para establecer una visibilidad y un control uniformes de las amenazas, lo que reduce drásticamente el tiempo y el esfuerzo necesarios para detectar, investigar y corregir las amenazas.

De esta manera, el firewalling se convierte en una estrategia clave para proteger sus complejas redes en la actualidad. Y proporciona un puente hacia el futuro a medida que su empresa y el panorama de amenazas continúan evolucionando.

¿Qué aspecto tiene?

Ya sea que trate de proteger recursos y datos en la nube, en las instalaciones o en una ubicación remota, el firewalling debe proporcionar constantemente protecciones de amenazas avanzadas, aplicación de políticas e inteligencia de amenazas compartida. El desafío es ofrecer esa uniformidad en entornos dispares donde se implementan y utilizan diferentes dispositivos.

Las infracciones a la seguridad pueden originarse en cualquier dispositivo que tenga acceso a Internet, independientemente de si se encuentra en la sede corporativa, el centro de datos, los sitios remotos, las nubes públicas o cualquier ubicación en la que el empleado trabaje de manera remota. Por eso es más importante que nunca incorporar un conjunto sólido de puntos de control de seguridad en ubicaciones más lógicas para reducir la exposición y mitigar los riesgos. Los controles de seguridad se aplican donde sea necesario en entornos propios (dispositivos físicos o virtuales y dispositivos de red, como routers) y en entornos no propios (seguridad como servicio [SECaaS]), controles nativos y cargas de trabajo.

¿Qué es el firewalling?

Los puntos de aplicación están en todas partes a través de las redes heterogéneas actuales.

El firewalling ofrece una funcionalidad uniforme de prevención de amenazas con visibilidad uniforme de políticas y amenazas para que pueda prevenir, detectar y detener los ataques de manera más rápida y precisa en todas partes.

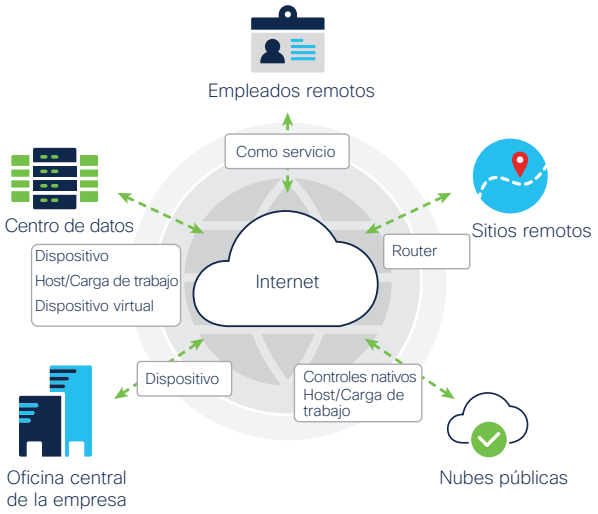


Figura 3. Principales abonados del firewalling como medio para abordar los desafíos de seguridad de las redes modernas.

© 2020 Cisco o sus filiales. Todos los derechos reservados.

Extensión de los controles de seguridad

Bajo la premisa de un firewall tradicional, dado que todo el tráfico interno y los usuarios autorizados eran inherentemente confiables (y el tráfico externo no lo era), la protección de toda la organización se lograba en el perímetro de la red. Este perímetro de la red se convirtió en el punto de control de seguridad lógico para proteger toda la organización. Todo el tráfico de red, ya sea que se originara en la sede central, el centro de datos o un trabajador remoto, se canalizaba a través de este único punto de control.

Por supuesto, este modelo no funciona en los entornos complejos de hoy en día, donde la infraestructura de TI de una organización abarca una amplia variedad de factores de forma y modelos de entrega, incluidos dispositivos físicos y virtuales, routers o switches integrados en la red, entregados como servicio, basados o incluidos en una nube pública.

Con un enfoque de firewalling se implementan controles de seguridad uniformes para proporcionar visibilidad completa, políticas unificadas y visibilidad integral de las amenazas. Estos controles de seguridad permiten una autenticación de usuarios y dispositivos más sólida en entornos cada vez más heterogéneos. Reúnen, comparten y responden al contexto sobre usuarios, ubicaciones, dispositivos y más para garantizar que los dispositivos cumplan con los requisitos de seguridad definidos. Mediante el uso de controles de seguridad uniformes en cada microperímetro, los equipos de seguridad pueden comenzar a automatizar las tareas (como la cuarentena automática de los usuarios y dispositivos que no cumplen con las normas, el bloqueo de dominios cuestionables en todos los controles de seguridad y la admisión de una microsegmentación eficaz). En el firewalling, la visibilidad completa proporciona una vista integral de todas las alertas de seguridad y los indicadores de riesgo; la inteligencia de amenazas compartida ofrece la detección de amenazas más actualizada a cualquier dispositivo conectado.

Administración basada en la nube

No se trata solo de productos específicos. La explosión de perímetros de red y recursos en la nube también ha aumentado la exposición a las brechas. Proteger los recursos más valiosos de una empresa en entornos de nube complejos mientras se administran diversos productos de seguridad no es una tarea fácil. Los equipos de seguridad necesitan visibilidad instantánea y administración optimizada para ayudar a reducir la configuración incorrecta.

El firewalling promueve una postura de seguridad más sólida al respaldar una administración centralizada basada en la nube a fin de ayudar a los equipos de seguridad a superar la complejidad y alinear las políticas en toda la organización. Las plantillas pueden mejorar el diseño y la uniformidad de las políticas redactando una política una vez y ampliando su aplicación a decenas de miles de controles de seguridad en toda la red. El uso de plantillas de políticas estándar para implementar rápidamente nuevos dispositivos ayuda a reducir los errores de configuración. A medida que las organizaciones crecen, las nuevas implementaciones heredan automáticamente las políticas más recientes. Un sistema de administración de políticas escalable integra varias funciones de seguridad en una sola política de acceso y optimiza las políticas en todos los dispositivos de seguridad para identificar inconsistencias y corregirlas rápidamente.

Además, una solución de administración centralizada y basada en la nube lleva las capacidades de un equipo al siguiente nivel. Identifica rápidamente los riesgos en todos los dispositivos y los lleva a un estado más uniforme y seguro. Con una única consola de administración, los objetos se pueden comparar en todos los dispositivos para descubrir incoherencias y optimizar el estado de seguridad actual. El personal puede optimizar la administración de políticas, mejorar la eficiencia y lograr una seguridad más uniforme mientras reduce la complejidad.

Contraataque con inteligencia de amenazas

A medida que el perímetro de la red se expande y la cantidad de dispositivos conectados directamente a Internet prolifera, nuestras superficies de ataque también se expanden. Las amenazas de ciberseguridad que involucran malware, criptomonedas, suplantación de identidad (phishing) y actividad de botnets están aumentando; los ciberdelincuentes recurren al aprendizaje automático y la inteligencia artificial

© 2020 Cisco o sus filiales. Todos los derechos reservados.

para aprovechar las vulnerabilidades de software existentes y acelerar los ataques maliciosos. Muy pocas organizaciones tienen recursos adecuados para probar y calificar por completo todos los parches de vulnerabilidad de proveedores de software; la mayoría se enfrenta al desafío de defenderse de la avalancha de amenazas emergentes y en evolución.

Otro aspecto convincente del firewalling puede ser de ayuda. El aprovechamiento de la inteligencia de amenazas líder del sector con la investigación de amenazas más reciente, algunas de ellas casi inmediatas, y el acceso a actualizaciones de protección ayudan a mitigar el flujo constante de amenazas. Los investigadores de amenazas identifican rápidamente los indicadores de riesgo y confirman y comparten las amenazas rápidamente. Utilizando economías de escala, su objetivo es proteger a las organizaciones contra el desarrollo de amenazas antes de que ocurran. Compartir la inteligencia de amenazas a través de redes interconectadas, endpoints, cargas de trabajo y entornos de nube ayuda a los equipos de seguridad a correlacionar eventos aparentemente desconectados, eliminar el ruido y detener las amenazas más rápidamente.

¿Cuáles son los riesgos de no utilizar el firewalling?

A medida que la red avanza, las organizaciones se adaptan e implementan diversos productos puntuales para respaldar los requisitos comerciales y las operaciones. Hacen lo mismo a medida que se publicitan nuevos vectores de ataque, agregando producto tras producto para protegerlos contra la última amenaza XYZ. Aquellos que dependen de un firewall tradicional para proteger cada dispositivo conectado a través de varios perímetros corren el riesgo de exponer sus datos y activos más valiosos a infracciones de seguridad. Según el almanaque de ciberseguridad de 2019, los daños por delitos cibernéticos costarán al mundo USD 6 billones anuales para 2021[5].

Estas amenazas pueden infiltrarse en una red rápidamente y poner en riesgo las operaciones de una empresa que carece de seguridad integral de red y visibilidad de endpoints.

Dicho esto, proteger la red, los entornos de nube, los dispositivos y los datos de una organización donde sea que se encuentren es una carga enorme para los equipos de seguridad.

El firewalling comienza y termina con el firewall como piedra angular de la seguridad de la red preparada para el futuro

En Cisco, hemos estado trabajando arduamente para hacer realidad esta visión. Trabajamos con negocios y empresas de todos los tamaños en todo el mundo y todos necesitan que la seguridad de su red sea más ágil y esté más integrada en la propia red. Es por eso que ofrecemos la arquitectura más segura de la historia: una plataforma potente y completa con el firewall como base.

Proporcionar un nivel de protección sin precedentes a través de este concepto es un componente importante de nuestra estrategia de seguridad. El portafolio de seguridad de Cisco y la familia de firewalls de Cisco lo mantienen un paso adelante de las amenazas en evolución con controles de seguridad de primer nivel donde sea que los necesite, políticas y visibilidad uniformes e innovaciones que mejoran las operaciones de seguridad.

En una era en la que el panorama de amenazas es más dinámico que nunca, Cisco une el liderazgo en redes y la tecnología de vanguardia para que pueda tener la postura de seguridad más sólida disponible ahora y en el futuro.

5 " Almanaque de ciberseguridad de 2019: 100 hechos, cifras, predicciones y estadísticas" , Cybercrime Magazine, 6 de febrero de 2019.

© 2020 Cisco o sus filiales. Todos los derechos reservados.

Los firewalls tradicionales proporcionan una vista limitada; la TI necesita una mayor visibilidad en toda la red con inteligencia de amenazas compartida para detectar y bloquear amenazas más temprano y más rápidamente. El firewalling va más allá mediante la entrega de una postura de seguridad integral basada en la administración unificada y las funcionalidades de seguridad integrales, como la prevención de intrusiones, el filtrado de URL y la protección contra malware avanzado, que aprovecha la automatización y el aprendizaje automático para una mayor eficiencia.

Sin una estrategia de firewalling implementada, la complejidad de la red puede llevar a configuraciones incorrectas, lo que aumenta el riesgo de una infracción a la seguridad. Según un informe de Gartner: " Hasta 2022, al menos el 95 % de las fallas de seguridad en la nube serán culpa del cliente" .[6] Al adoptar una estrategia de firewalling de armonización de políticas de seguridad en varios puntos de control, las organizaciones mejoran su estado general de seguridad.

Sección 3: Cuatro pasos para configurar la estrategia de firewalling

Paso 1: establezca la base para una estrategia de firewalling exitosa con un firewall moderno de próxima generación. Cisco Secure Firewall ofrecerá políticas de seguridad uniformes, visibilidad y una mejor respuesta ante amenazas para su solución de seguridad integrada.

Paso 2: una vez que haya seleccionado Cisco Secure Firewall, el siguiente paso es estandarizar una solución de administración. Tenga en cuenta estos factores al determinar qué solución es adecuada para su organización:

- Determine la ubicación de administración preferida (en las instalaciones o la nube) y qué grupo será responsable de administrar la seguridad (SecOps o NetOps).
- Lo más importante es garantizar que la solución de administración se alinee con los objetivos actuales y futuros de la TI. Si traslada las cargas de trabajo a la nube, inicia un portal de proveedores o aborda proyectos de transformación digital o aplicaciones de SaaS, es posible que desee adoptar una administración basada en la nube. Si su organización depende de aplicaciones antiguas monolíticas, las aplicaciones en las instalaciones pueden satisfacer sus necesidades. En general, las aplicaciones heredadas requieren cierta reestructuración para ejecutarse correctamente en la nube y, si no hay planes inmediatos para actualizar estas aplicaciones, generalmente es mejor un sistema de administración en las instalaciones.
- Una solución de administración basada en la nube ayuda a los equipos de operaciones de red a alinear las políticas en toda la organización, reducir la complejidad y administrar todos los puntos de control de seguridad desde un panel central. Simplifica la organización y administración de políticas de manera uniforme desde un solo lugar para brindar protección contra las amenazas más recientes. Con una aplicación centralizada basada en la nube, puede optimizar la administración de la seguridad, implementar nuevos dispositivos más rápidamente con plantillas y realizar un seguimiento de todos los cambios en el entorno.

Paso 3: fortalezca su postura de seguridad con la integración. Su estrategia de firewalling debe proporcionar cobertura integral en todos los microperímetros y ofrecer protección y control en todos los dispositivos conectados y las soluciones de seguridad. La integración de la seguridad en toda su red heterogénea a través de aplicaciones y servicios en la nube, correos electrónicos corporativos y todos los endpoints conectados protege a su empresa contra el panorama de amenazas en expansión.

Este paso configura su equipo de seguridad para bloquear más amenazas, responder más rápidamente a las amenazas avanzadas y ofrecer automatización en toda la red a las aplicaciones en la nube y los endpoints.

Paso 4: por último, asegúrese de que su estrategia de firewalling incorpore un análisis de amenazas avanzado continuo para proteger sus activos comerciales y ayudarlo

6 " ¿Es segura la nube?" Gartner, 27 de marzo de 2018.

© 2020 Cisco o sus filiales. Todos los derechos reservados.

a mantenerse un paso adelante de las amenazas emergentes. Una de las maneras más fáciles es elegir una solución que proporcione automáticamente la información de amenazas más reciente a la red a través del firewall. La inteligencia actualizada y la visibilidad total permiten que los equipos de seguridad comprendan las vulnerabilidades más recientes. Y si una amenaza penetra, puede identificar dónde y cómo sucedió. La funcionalidad integrada del IPS de próxima generación automatiza las clasificaciones de riesgo y los indicadores de impacto para identificar las prioridades a fin de reconocer y priorizar los recursos y la información más críticos. Los equipos de seguridad pueden tomar medidas correctivas inmediatamente y corregir las amenazas, manteniéndose enfocados en los recursos más críticos en lugar de verse abrumados por el " ruido" , lo que hace que las operaciones de SOC sean más seguras.

Comienza con el firewall correcto como base

Los equipos de seguridad actuales necesitan:

Una mejor seguridad respaldada por la inteligencia de amenazas líder del sector para proteger su red compleja y detectar amenazas antes y actuar más rápido.

Una manera de **establecer, escalar y armonizar de forma eficiente las políticas de seguridad** en toda la red.

Visibilidad y complejidad reducidas con una administración y automatización unificadas para acelerar las operaciones de seguridad y mejorar su experiencia.

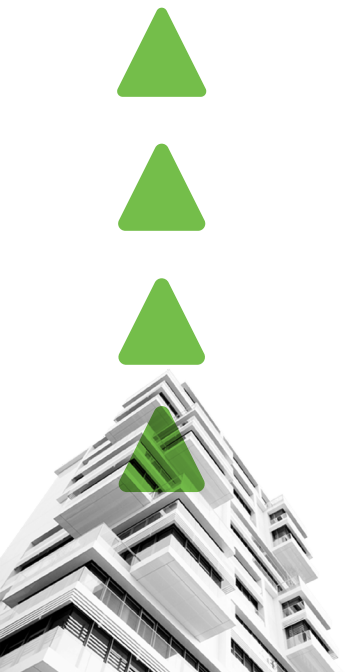
Redes y seguridad que funcionen en conjunto para maximizar sus inversiones existentes. La solución adecuada proporcionará un conjunto profundo de integraciones para una seguridad integral que proteja todo, en todas partes.

Beneficios de la estrategia de firewalling con Cisco Secure Firewall

Conversión de toda la red en una extensión de su arquitectura de seguridad: al compartir políticas comunes, funcionalidades de prevención de intrusiones y otras funciones básicas con Cisco Secure Firewall, los switches y routers pueden aplicar la seguridad, vinculando la infraestructura de red en un portafolio de seguridad integral. Comparta la inteligencia de amenazas a través de su arquitectura rápidamente para correlacionar eventos aparentemente desconectados, eliminar el ruido y detener las amenazas con mayor celeridad.

Controles de seguridad de primer nivel: Cisco Secure Firewall brinda una eficacia superior contra amenazas para proteger su red compleja contra los ataques cada vez más sofisticados de la actualidad. La inteligencia de amenazas avanzada y líder del sector ayuda a su organización a encontrar nuevos dominios de malware y URL maliciosas, así como vulnerabilidades desconocidas o no divulgadas a fin de detectar amenazas con antelación y actuar más rápidamente. El IPS integrado de próxima generación ofrece visibilidad completa con clasificaciones de riesgo automatizadas e indicadores de impacto para identificar las prioridades de su equipo de seguridad y minimizar el ruido. La seguridad retrospectiva lo mantiene informado y analiza continuamente las amenazas después de la detección inicial para identificar mejor el malware sofisticado que inicialmente puede ocultarse de la detección.

Políticas unificadas y visibilidad de amenazas: los equipos de seguridad pueden lograr uniformidad y armonización de las políticas estandarizando y aplicando controles de seguridad en cada dispositivo, desde dispositivos de red hasta hosts y en toda la nube. La administración centralizada y flexible de Cisco permite que su equipo aplique controles escalables en muchos dispositivos de manera rápida y sencilla para mantener políticas uniformes. Reduce la complejidad con la administración unificada y la correlación de amenazas automatizada con funciones de seguridad estrechamente integradas, como firewalling de aplicaciones, NGIPS y AMP. Optimice la administración de dispositivos y políticas de seguridad en las redes extendidas y acelere las operaciones de seguridad clave, como la detección, la investigación y la corrección.



© 2020 Cisco o sus filiales. Todos los derechos reservados.

Sección 4: Una solución de seguridad preparada para el futuro

La manera en que trabajamos ha cambiado. Nuestros negocios y redes se han transformado, cambiando las reglas de seguridad de la red. Estos desarrollos nos obligan a repensar el firewall y adoptar el firewalling.

Cisco impulsa la innovación para abordar estas tendencias con una plataforma de seguridad que ofrece controles de seguridad de clase mundial donde sea que los necesite con visibilidad y políticas de seguridad uniformes, respaldadas por la inteligencia de amenazas líder del sector. La última generación de Cisco Secure Firewall constituye la base de nuestro portafolio de productos estrechamente integrados.

La solución emblemática de administración en la nube de Cisco, **Cisco Defense Orchestrator**, ofrece armonización de políticas en una variedad de productos de seguridad de Cisco.

En cada producto de seguridad de Cisco se incluye **Secure Threat Response**, una solución de respuesta a amenazas automatizada que reacciona a los nuevos ataques cibernéticos compartiendo e implementando automáticamente contramedidas en toda la arquitectura de seguridad.

Secure Endpoint ofrece inteligencia global sobre amenazas, sandboxing avanzado y bloqueo de malware en tiempo real. AMP analiza continuamente la actividad de los archivos en toda la red extendida para detectar, contener y eliminar rápidamente el malware avanzado.

Talos Threat Intelligence es un equipo mundialmente reconocido de investigadores de amenazas a tiempo completo, científicos de datos e ingenieros que recopilan información sobre amenazas existentes y en desarrollo. Talos respalda todo el ecosistema de seguridad de Cisco y ofrece protección contra ataques y malware. Talos proporciona visibilidad de las últimas amenazas globales, inteligencia procesable en defensa y mitigación, y respuesta colectiva para proteger activamente a todos los clientes de Cisco.

El sistema de prevención de intrusiones de próxima generación SNORT (SNORT NGIPS) es un NGIPS de código abierto, líder en la industria, que realiza análisis de tráfico, registro/análisis de paquetes y análisis de protocolos. SNORT NGIPS aprovecha la inteligencia de amenazas de Talos para ayudar a toda la comunidad de seguridad compartiendo políticas que protegen contra el desarrollo de amenazas.

El acceso adaptable y confiable en todas partes basado en el contexto está disponible con Identity Services Engine (ISE). Proporciona protección inteligente e integrada a través de políticas basadas en la intención y soluciones de cumplimiento.

Secure Access by Duo proporciona autenticación de varios factores, visibilidad de endpoints, autenticación adaptable y aplicación de políticas con acceso remoto e inicio de sesión único para proteger proactivamente el acceso a las aplicaciones.

El análisis de red seguro, la carga de trabajo segura y la infraestructura centrada en aplicaciones (ACI) funcionan en conjunto y controlan a los usuarios donde sea que vayan y sus cargas de trabajo de aplicaciones dondequiera que se encuentren mediante el aprendizaje automático, el modelado del comportamiento, la telemetría de infraestructura de red y la segmentación para burlar las amenazas emergentes.

Implemente su estrategia de firewalling preparada para el futuro invirtiendo en la plataforma de seguridad de Cisco y en Cisco Secure Firewall. Obtendrá la postura de seguridad más sólida disponible en la actualidad y estará preparado para el futuro.

Sección 5: Comience a construir el futuro del firewall hoy mismo

Cisco une el liderazgo en redes y la tecnología de seguridad de vanguardia para ofrecer la arquitectura más segura de la historia. Ya sea que esté mejorando la seguridad de su red con la optimización de las inversiones existentes o transformando sus routers en un firewall, Cisco continúa innovando.

Cisco Secure Firewall es la seguridad de red diseñada para la transformación digital de su negocio por la empresa que creó la red.

Obtenga más información sobre Cisco Secure Firewall y comience hoy mismo con su futuro firewalling. Lea más sobre las últimas tendencias que dan forma a las redes del futuro en el Informe de tendencias de redes globales de 2020.

© 2020 Cisco o sus filiales. Todos los derechos reservados. Cisco y el logotipo de Cisco son marcas registradas o marcas comerciales de Cisco y/o de sus filiales en los Estados Unidos y otros países. Para ver una lista de las marcas registradas de Cisco, visite la siguiente URL: www.cisco.com/go/trademarks. Las marcas comerciales de terceros mencionadas en este documento pertenecen a sus respectivos propietarios. El uso de la palabra partner no implica una relación de asociación entre Cisco y cualquier otra empresa. 10/20