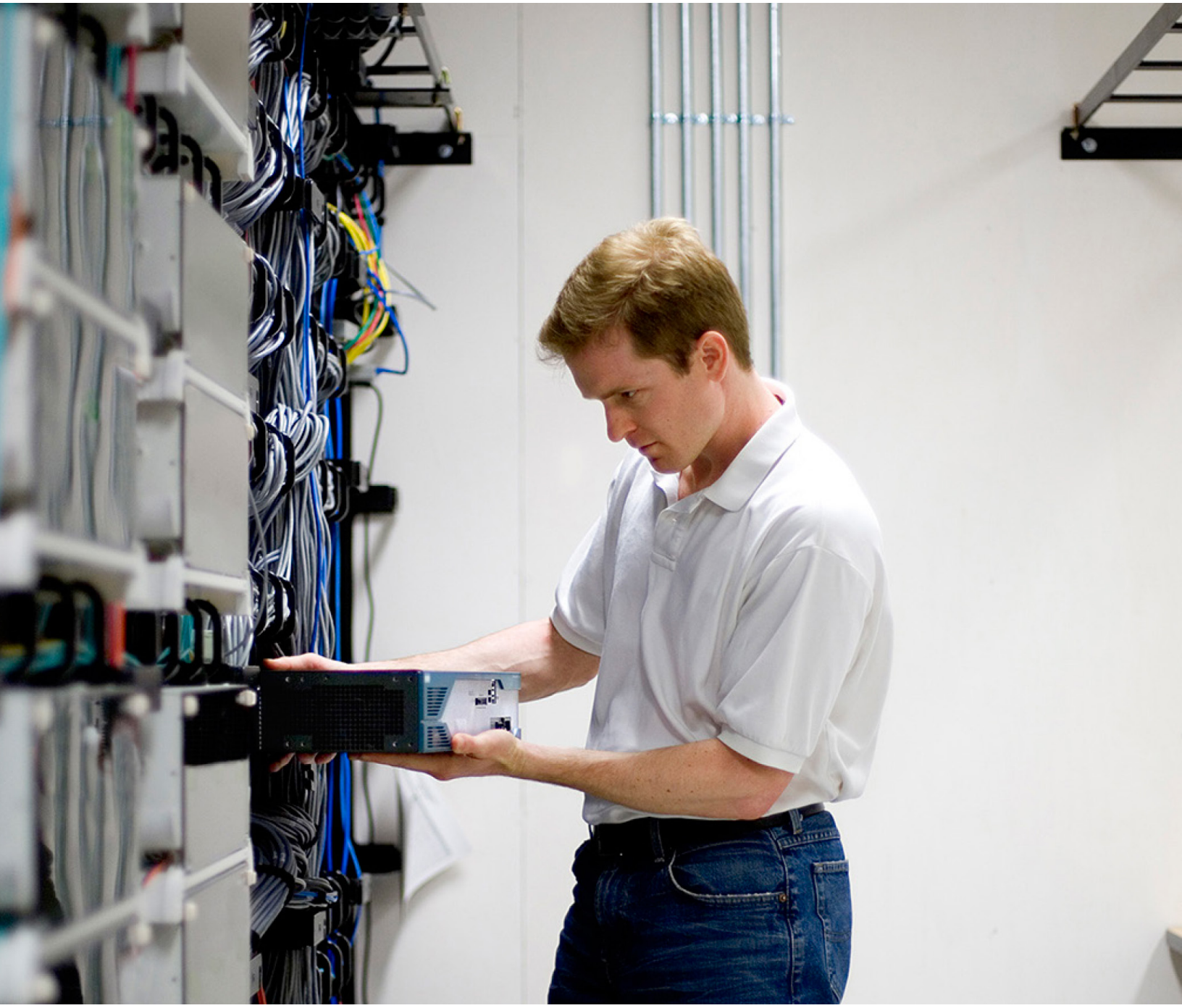
Consiga que su perímetro de la red sea inteligente y satisfaga las necesidades del futuro hoy



Resumen ejecutivo

En la nueva realidad de empresa digital, el perímetro de la red nunca ha sido tan importante. A menudo pasado por alto, el perímetro de la red es la piedra angular que permite conseguir el éxito digital o fracasar en el intento. Analice todo lo que ocurre en el perímetro de la red:

- Es la primera línea de defensa contra la infiltración de dispositivos maliciosos o poco fiables.
- Es un conducto que ofrece aplicaciones y servicios al público objetivo, a menudo con una gran inversión.
- Es el gateway estratégico para conectar organizaciones muy descentralizadas.
- Es el puente entre su organización y los clientes.
- Es el punto en el que los nuevos dispositivos IoT (Internet of Things) se conectan y gestionan.
- Es el lugar idóneo para comprender por completo qué sucede en su empresa.

El perímetro de la red a menudo se implementa con la creencia de que todas las soluciones de red son prácticamente iguales. Cisco no está de acuerdo y considera que la nueva empresa digital necesita una gran inteligencia en el perímetro.

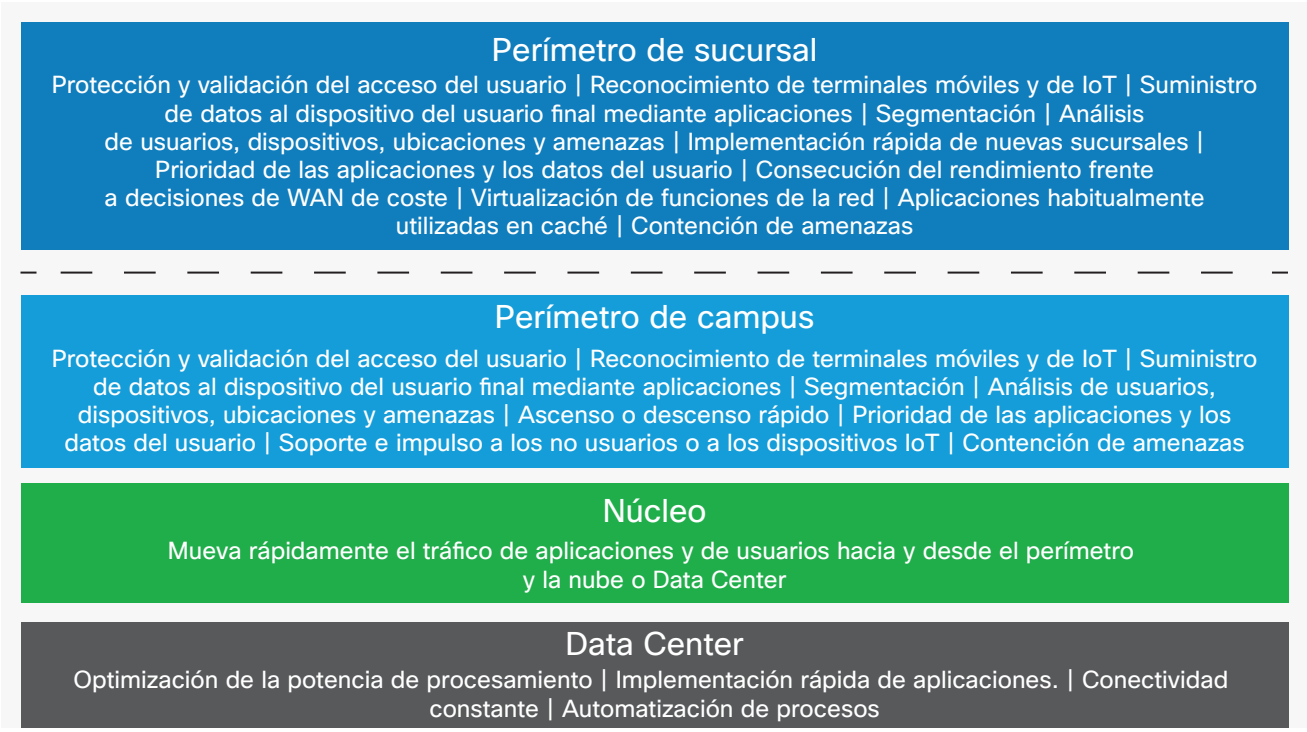
Ofrecemos soluciones y funcionalidad estratégica para conducir a su empresa al éxito. Cisco impulsa el nuevo perímetro de la red digital focalizándose en:

- Defender a los activos críticos en el perímetro. Las organizaciones pueden evitar el 99,2% de las brechas en la red al aprovecharse de la misma como sensor y ejecutor. Esto puede realizarse mejorando al mismo tiempo la protección y ofreciendo unas respuestas más rápidas.
- Permitir el conocimiento de la aplicación y los dispositivos con una itinerancia ocho veces más rápida y visibilidad en más de 1200 aplicaciones. Esto es posible gracias a una asociación estratégica con Apple y con innovaciones de Wi-Fi.
- Adaptar rápidamente la red a medida que su empresa evoluciona con un enfoque definido por software en conexiones LAN inalámbricas, LAN y WAN. Esto supone una reducción del 79 % en los costes de implementación mediante la disociación del hardware y la virtualización del extremo de la WAN.
- Una plataforma diseñada para satisfacer las futuras demandas mediante el establecimiento de fundamentos programables y basados en estándares que puedan agregar rápidamente nuevas funcionalidades cuando sea necesario.
- Proporcionar percepciones más profundas y rápidas de los ámbitos de venta al por menor y hostelería, ganando así hasta un metro en la granularidad de los datos de ubicación, para tomar mejores decisiones empresariales.

Hoy en día, la red es fundamental a la hora de llevar a cabo cambios virtuales en todas las organizaciones a medida que inician su proceso de transformación digital. Este proceso de transformación ayudará a las organizaciones a aumentar su agilidad, productividad, a comunicarse mejor con los clientes y a proteger la propiedad intelectual y los activos fundamentales.

El perímetro de la red tiene un papel fundamental en esta transformación y tiene el conjunto de responsabilidades más amplio en comparación con las redes principales y las redes centrales de datos. Tal y como se muestra en la figura 1, al comparar cada nivel de la red, observamos que el perímetro de la red tiene una amplia variedad de responsabilidades en el campus. Esto es así también para las sucursales.

Figura 1. Niveles de red y sus funciones



La función del perímetro de la red

La transformación digital hace que el perímetro de la red sea más importante que nunca. Analice todo lo que sucede en el perímetro de la red:

- **Es la primera línea de defensa.** El perímetro es donde se aplica y se valida la política, sin limitar su capacidad de acceder a lo que necesita. Si el acceso no se gestiona correctamente, su empresa puede ser susceptible a la infiltración o a la proliferación de amenazas, y la gravedad aumenta a medida que el panorama de amenazas crece. El dispositivo, firmware y el sistema operativo son todos elementos comprometidos.
- **Es un conducto que ofrece aplicaciones con una gran inversión.** El perímetro de la red es donde sucede la priorización. Una experiencia insuficiente en el perímetro reducirá la aceptación de aplicaciones, lo que reducirá el retorno de la inversión.
- **Es un gateway estratégico para conectar organizaciones ampliamente distribuidas.** Ofrecer una experiencia sin problemas a sus empleados, partners y clientes es lo más importante, estén donde estén. Una red de segunda clase proporcionará niveles de desviación de servicios al público clave.
- **Es el puente entre su organización y los clientes.** Si forma parte de una empresa minorista o de hostelería, el acceso de secundarios impedirá su capacidad de conectarse con los clientes a nivel personal y afectará negativamente a su marca.
- **Se ha diseñado para potenciar y responder a las crecientes demandas de los dispositivos IoT.** El perímetro de la red se adapta al entorno físico al mover virtualmente todas las industrias a la edad digital mejorando las operaciones y reduciendo los costes. Sin la funcionalidad adecuada del perímetro, las organizaciones pueden quedarse atrás en términos de reducción de costes y eficacia operativa.
- **Es el lugar idóneo para comprender qué sucede en su empresa.** En una red distribuida, solo el perímetro puede ver todo el tráfico de datos al recopilar datos y análisis del perímetro. Los datos sobre usuarios, aplicaciones, dispositivo y amenazas pueden ofrecer perspectivas que realmente sean de ayuda para tomar mejores decisiones y ayudar a los empleados, reducir riesgos, y costes y proporcionar información al público objetivo. Sin el nivel adecuado de granularidad uniforme, estos datos se distorsionan y dejan de ser fiables.

¿Es buena la mercantilización del perímetro?

Muchas soluciones de perímetro adoptan la mercantilización al utilizar componentes que ya están disponibles para crear dispositivos de red de perímetro y diseñar directamente en los estándares del sector. Esto a menudo se realiza para reducir los costes de ingeniería y producción del equipo, aprovechando los diseños que ya están disponibles proporcionados por los fabricantes de componentes. Esto deriva en la mercantilización del perímetro. El enfoque de dar prioridad al coste y la gestión a la hora de ofrecer innovaciones clave para el crecimiento y la seguridad hace que su empresa se exponga a un mayor riesgo.

¿Cuál es el riesgo?

Los componentes y diseños no solo están disponibles para los fabricantes de dispositivos, también llegan a las manos de personas que buscan infiltrarse en la red. Cada dispositivo que se asocia con la red es un punto de infiltración a la misma. Las organizaciones actuales confían en el creciente número de dispositivos móviles y de IoT de la red para conseguir su éxito empresarial. Las organizaciones deben considerar soluciones que aborden el acceso de seguridad, que empiecen en el perímetro y continúen en la comprobación exhaustiva del tráfico en cada paso, desde el perímetro hasta el Data Center.

También existe el riesgo de tener que volver a diseñar la red si se presenta un nuevo requisito empresarial. Las soluciones disponibles están diseñadas para satisfacer un gran número de casos de uso, pero están limitadas en términos de flexibilidad y personalización. También están limitadas en relación a estar preparadas para la evolución imprevista de su red. La plataforma de red necesita adaptarse al cambiante mundo digital actual.

La mayoría de las soluciones disponibles están diseñadas para alinearse directamente con los estándares del sector, que son importantes para proporcionar el conjunto principal de requisitos y de funcionalidad. Sin embargo, los estándares pueden cambiar. El proceso de los estándares a menudo es largo y la velocidad con la que los fabricantes de dispositivos, desarrolladores de aplicaciones y usuarios deben enfrentarse a nuevas demandas cambia constantemente. Los que utilizan un enfoque basado en estándares pueden encontrarse en desventaja cuando se trata de satisfacer las altas expectativas de los clientes. Hay ocasiones en las que una solución puede iniciarse cumpliendo un estándar, pero entonces se tiene la capacidad de desarrollar una funcionalidad adicional a esos estándares cuando sea necesario. Satisfacen las nuevas demandas del mundo digital sin verse limitadas por los estándares, lo que puede llevar años para su mejora y ratificación.

También existe un riesgo de que se vea comprometida la integridad del dispositivo. Las organizaciones maliciosas interceptan los dispositivos cuando se envían a todo el mundo, alteran los componentes, intercambiando los procesadores o integrando monitores para adquirir datos confidenciales, por ejemplo.

¿Cuál es el coste real?

A menudo la mercantilización del perímetro se realiza para reducir los costes de ingeniería y producción, y permite que algunas soluciones se vendan a un precio más bajo. Sin embargo, al medir el coste, no solo se debe considerar el capital puro o los costes operativos, sino también los costes asociados al riesgo. Cada organización es diferente, por lo que determinar los costes reales que representen a todas ellas no es posible. Pero hay que considerar:

- El coste de una brecha de la seguridad. La propiedad intelectual y los recursos de muchas organizaciones son el sustento de la organización. Si caen en las manos equivocadas, ¿cuáles serán las consecuencias? Las organizaciones maliciosas son especialmente buenas en la monetización de la propiedad intelectual mediante el rescate, la extorsión y la reventa al mejor postor. Algunos estudios revelan que los informes médicos se han rescatado por unos 40,00 dólares por registro. Con miles de registros, los hospitales podrían tener que pagar una gran cantidad de dinero para recuperar su propiedad.
- El coste de una aplicación vital para la empresa que no se ha adoptado por parte de los empleados. Muchas organizaciones invierten una gran parte del presupuesto en nuevas aplicaciones y sistemas para mejorar la productividad. Si los empleados tienen poca experiencia con estas aplicaciones o servicios, las abandonarán y la rentabilidad de la inversión caerá en picado.

- El coste de una oportunidad perdida. Si forma parte de una organización minorista o de hostelería, se comunica con los clientes a través de dispositivos móviles. Pero si sus clientes tienen dificultades para conectarse, la organización habrá perdido la oportunidad de establecer una relación con el cliente e influir en su comportamiento deseado.
- El coste de falta de visibilidad. La red de perímetro consta de una gran cantidad de información de usuarios, dispositivos, qué aplicaciones utilizan, dónde van e, incluso, información sobre posibles amenazas existentes. Sin esta visibilidad su organización podría pasar innumerables horas intentando comprender cómo interactúan los usuarios con el entorno, cómo acceden y consumen información e, incluso, perder una posible amenaza que se podría haber mitigado a tiempo.

Cisco ofrece inteligencia en el perímetro

Cisco adopta un enfoque diferente a la mercantilización del perímetro. Hemos realizado grandes inversiones en el desarrollo de innovaciones que ayuden a trasportar a las organizaciones a la edad digital. Nos hemos centrado en la defensa de los recursos principales para sensibilizar sobre aplicaciones y dispositivos. Cisco le ayuda a adaptarse a medida que su empresa evoluciona y le prepara para lo que el futuro pueda deparar. Esto lo conseguimos elaborando una funcionalidad única desde cero o mejorando la funcionalidad de los componentes que ya se han probado. Cisco proporciona esta funcionalidad para ayudarle a satisfacer las demandas del perímetro de la red hoy y en el futuro.

Defensa de los recursos principales en el perímetro

El perímetro de la red es el punto de acceso no autorizado u hostil número uno, ya que es dónde se encuentran los usuarios y dispositivos. Tiene que ser de confianza para identificar y controlar qué sucede en la red.

Aceptar que la mercantilización de la seguridad del perímetro es efectiva sugiere que la seguridad disponible funciona. Si esto es así, ¿por qué el robo de información, la extorsión y los rescates ha crecido rápidamente hasta 1 billón de dólares en el sector?

Los enfoques de seguridad del perímetro actuales no funcionan. Cisco es el líder del mercado en tecnologías innovadoras para saber qué y quién es un determinado elemento, además de conocer su estado, antes de dejar que acceda a la red y permitir la itinerancia.

Existen varias innovaciones en materia de seguridad de perímetro de la red de Cisco® para los clientes de Cisco:

- **Identidad y estado del dispositivo y del usuario**. Los dispositivos del perímetro de Cisco integran la tecnología de examinación de perfiles de terminales más amplia. Además, Cisco AnyConnect® Security Agent realiza una comprobación del estado de cumplimiento de la posición y de la política antes de permitir el acceso a la red de producción. La identidad de terminal más precisa mantiene a los dispositivos no autorizados y con mal estado (infectados por malware) completamente fuera de la red hasta que se aprueban y autorizan por completo.
- **Privilegios de acceso que cambian la puntuación de la amenaza**. Gracias a la integración con Cisco Identity Services Engine, los usuarios y dispositivos pueden cambiar automáticamente sus privilegios de acceso a medida que cambia la puntuación de vulnerabilidad de CVSS o de la amenaza STIX. STIX y CVSS son expresiones de uso general para describir la gravedad de las amenazas de seguridad y las vulnerabilidades.
- **Integración de la segmentación definida por software**. La creación y gestión de la segmentación con LAN virtuales y listas de control de acceso (ACL) suelen ser complicadas y demuestran ser más difíciles a medida que la segmentación se convierte en clave para garantizar la seguridad de las operaciones de IoT. Los dispositivo de perímetro de Cisco envían segmentación definida por software de Cisco TrustSec® al sistema operativo, así como un ASIC para garantizar una identidad y segmentación sencilla y de alto rendimiento desde el punto de acceso a una aplicación de Data Center.
- **La red como ejecutora de políticas de seguridad**. Segmentación definida por software integrada en dispositivos de perímetro que permite una aplicación instantánea y uniforme de la política de seguridad para controlar el acceso y contener las amenazas. Gracias a la integración con las tecnologías Identity Services Engine, Cisco Stealthwatch y Cisco Security Technology se pueden aplicar políticas para contener una amena, todo desde un único panel o un único producto.

- **La red como sensor**. Disfrute de una visibilidad integral avanzada con NetFlow e interpretación de Cisco Stealthwatch. Dado que todos los dispositivos de perímetro de Cisco incluyen Flexible NetFlow, puede tener una visibilidad integral del flujo para detectar comportamientos anómalos. Con las tecnologías de los productos es incapaz de ver los comportamientos que muestran lo que los usuarios hacen cuando entran en la red y qué hacen en Internet.
- **Integración de Stealthwatch Learning Network License**. Esta innovación permite que todos los dispositivos de sucursales compartan datos de comportamientos y obtengan una visión más inteligente de lo que es permisible, lo que hace que el proceso sea más rápido, sencillo y escalable.
- **Aplicación de políticas defcon de minuto cero**. Esto significa que puede haber preconfigurado políticas para responder a los eventos catastróficos, como malware de día cero o evento de pirateo que se propaga rápidamente. Al pulsar un botón puede aplicar cambios en las políticas de acceso para cada dispositivo de la red para restringir o detener todas las comunicaciones hasta que la amenaza se solucione.
- **Identidad de terminal de IoT y segmentación automática**. La examinación de los dispositivos de perímetro de Cisco ayuda a identificar la mayor colección de dispositivos IoT actual y la tecnología se expande a muchos otros sectores. Gracias a la integración con tecnologías avanzadas como Identity Services Engine, los dispositivos de red de perímetro podrán identificar y segmentar mejor y automáticamente los terminales más ocultos y agregarlos de forma automática a segmentos de red discretos para protegerlos de ataques. Así que cuando un trabajador conecta un dispositivo en la red, se identifica, clasifica y coloca en su respectivo segmento de red de seguridad.
- **Contención rápida de amenazas**. Los dispositivos de perímetro de Cisco integran Identity Services Engine y TrustSec, de manera que cuando Cisco o un partner de integración de tecnología detecta un ataque, pueden colocar el terminal amenazado en un segmento de red, ya sea por un comando de TI o automáticamente. Las amenazas se detectan más rápidamente y la respuesta de contención es instantánea.
- **Detección de malware en tráfico cifrado**. A medida que los hackers encuentran formas desapercibidas de acceder a la red, Cisco utiliza nuestra capacidad para examinar los tramos de red e identificar malware, incluso en tráfico cifrado.
- **Nube, malware y protección contra ransomware**. La integración con Cisco Umbrella Branch permite que los dispositivos de perímetro de Cisco sean la parte fundamental de la solución contra el ransomware de Cisco. Umbrella evita que los empleados accedan a sitios web sospechosos, peligrosos o con malware. También evita que el malware y los bots de ransomware alcancen lleguen a su elementos principal, que por lo general es necesario para funcionar.
- **Protección de los trabajadores móviles**. Los trabajadores móviles son probablemente los puntos de infiltración de malware más comunes, ya que a menudo tiene acceso libre a Internet cuando trabajan en remoto. El agente de seguridad Cisco AnyConnect con VPN puede aumentarse con la protección frente a malware avanzado de Cisco y Cisco Umbrella for Mobility, para mantener la seguridad cuando se encuentre fuera de la red. También permite la conexión mediante VPN a varios dispositivos de perímetro de Cisco. Ningún dispositivo móvil de seguridad de agente único funcionará en un entorno de productos.
- **Integridad del dispositivo de red**. Los hackers tienen más formas de infiltrarse y comprometer los sistemas que solo sobrepasando las vulnerabilidades de las aplicaciones y los sistemas operativos. Atacan el stack de hardware y de software de los dispositivos de red, de manera que la seguridad del dispositivo de red se encuentra en estado crítico. Al tener sistemas operativos y aplicaciones, las vulnerabilidades de los dispositivos de red seguirán descubriéndose. Cisco aplica estrictas reglas en el desarrollo del software y el hardware, que completa con pruebas de regresión para asegurarse que sus clientes puedan seguir trabajando en una red de confianza.

Datos más precisos y percepciones más rápidas

El perímetro de Cisco aporta una gran cantidad de conocimiento a lo que realmente sucede en su empresa, ya que tiene excelente visión de los usuarios, los dispositivos que utilizan y las aplicaciones a las que tienen acceso. Posee la capacidad de comprender y aprender de los dispositivos en la red para poder así adaptarse automáticamente a los cambios y las necesidades. Proporciona datos basados en la ubicación para entender mejor cómo los usuarios interactúan con el entorno para tomar mejores decisiones empresariales y poder proporcionar diagnósticos de amenazas para entender cómo se infiltran en la empresa.

Con Cisco IOx Fog Computing, el perímetro puede decidir el lugar óptimo, in situ o en la nube, en el que procesar los datos, permitiendo a la organización mejorar el rendimiento y reducir costes. Los análisis de ubicación de Cisco Connected Mobile Experiences (CMX) ofrecen análisis de ubicación impulsados por Wi-Fi pormenorizado y Bluetooth de baja energía (BLE) para proporcionar una visión realista de cómo las personas interactúan con el entorno.

Las organizaciones de empresa a consumidor (B2C), como la venta al por menor, la hostelería y la educación, han podido conseguir menos de un metro de precisión con Wi-Fi + BLE e impulsan aumentos de ingresos directos. Algunos ejemplos incluyen un 20% de ingresos fuera de la oficina por Hyatt Regency, un aumento tres veces mayor del tiempo de permanencia del cliente, y un 80% de mejora en la experiencia de usuario en Stary Browar, todo a la vez que se proporcionan experiencias móviles personalizadas.

Además, Cisco Prime™ proporciona una vista de 360 grados de los usuarios finales, sus dispositivos y las aplicaciones que utilizan en la red. Esto permite una mejor planificación de la red, medidas de adopción de la aplicación y unos menores costes.

Adaptación a medida que la empresa evoluciona mediante la automatización

Con más usuarios, más dispositivos y más ubicaciones que gestionar, la necesidad de automatizar los procesos y los nuevos servicios con capacidades de día cero y primer día pasa a ser algo más que un mero requisito. En el espacio de acceso por cable o inalámbrico, un fabric de Data Center o de campus con superposición de software disociado ejecutándose en circuitos integrados específicos de una aplicación personalizada (ASIC) permite:

- Una mayor escalabilidad
- Garantía de servicio
- Seguridad
- Otros servicios para dispositivos físicos y virtuales, aplicaciones y usuarios

La virtualización de la red permite gestionar la red y las políticas por tipo de usuario para iniciar y personalizar rápidamente las aplicaciones y contener las amenazas más rápido. Es un enfoque centralizado para la implementación segura de nuevas ubicaciones remotas en minutos en lugar de en días, con cualquier tipo de conexión.

El módulo empresarial de controlador de infraestructuras de políticas de aplicaciones (APIC-EM) de Cisco proporciona aplicaciones PnP (enchufar y usar) controladas de manera centralizada y una funcionalidad de calidad de servicio (QoS) para facilitar su implementación sin intervención del usuario en el perímetro. Esto permite la priorización dinámica de sus aplicaciones más importantes.

Cisco ofrece la agilidad habilitada por software para la personalización. A través de plataformas de software y hardware perfectamente integradas podemos proporcionar beneficios significativos a su organización, evidentes en el perímetro de acceso y WAN. Los componentes personalizados por la WAN incluyen ASIC más rápidos, y el software de gestión en la nube hace que la virtualización de las funciones de red empresarial (NFV empresarial) de Cisco sea real y pueda activar los servicios de red en minutos en lugar de en meses. Enterprise NFV proporciona capacidades de procesamiento, almacenamiento, infraestructura de la red, gestión y garantía para ejecutar servicios de red de manera que pueda reducir la complejidad en la sucursal y habilitar nuevos servicios en el perímetro según se necesite.

Las organizaciones han experimentado una reducción del 79% en los costes de implementación con el PnP de APIC-EM, y un 85% de aprovisionamiento más rápido con las aplicaciones WAN inteligentes de APIC-EM.

Debido al gran número de usuarios y dispositivos conectados desde todos los tipos de sitios, el perímetro de la red puede ubicarse en campus grandes o en sitios remotos pequeños. Las vistas de topología global con capacidades de PnP automatizadas reducen significativamente el coste de integrar o actualizar un dispositivo de red, como un switch, router o punto de acceso. Las aplicaciones adicionales del controlador permiten el aprovisionamiento de QoS en toda la red, protegiendo rápidamente el tráfico crucial para la empresa de consumidores de ancho de banda no fundamentales. Las aplicaciones especializadas como la aplicación WAN inteligente (IWAN) permiten el aprovisionamiento, la supervisión y la resolución de problemas de seguridad, cifrado, selección de rutas y visibilidad de aplicaciones, así como de control en la WAN.

Además, el software Cisco ONE™ ofrece una forma útil y flexible de comprar software para el perímetro. En cada etapa del ciclo de vida del producto, Cisco ONE Software facilita la compra, la gestión y la actualización del software de redes. Obtenga un importante ROI a medida que su inversión crece mediante innovaciones y actualizaciones costantes de las máquinas virtuales y físicas.

Importancia de las aplicaciones y los dispositivos

Cisco es el único partner que se aliado con la empresa líder en dispositivos móviles a nivel mundial, Apple, para ofrecer una mejor experiencia móvil. Esta asociación estratégica para ambas empresas saca provecho de la inteligencia en la red para ofrecer la mejor experiencia Wi-Fi gracias a una itinerancia óptima. En otras palabras, es una vía rápida para las aplicaciones vitales para la empresa instaladas en dispositivos Apple iOS usados en el lugar de trabajo para mejorar la productividad de los empleados.

Las empresas disfrutan de una itinerancia hasta ocho veces mayor y unas llamadas por Wi-Fi hasta un 66% más fiables, una reducción del 50% en la sobrecarga de la gestión de la red debido al menor número de SSID y, además, los usuarios finales pueden alargar la duración de la batería de los dispositivos iOS hasta un 30%.

Durante muchos años Cisco ha ofrecido innovaciones en el mundo del Wi-Fi que transcienden el estándar actual y sirven como puntos de prueba para los estándares del futuro. La tecnología inalámbrica de Cisco Aironet® ofrece innovaciones en las experiencias de alta densidad que mejoran las ondas de radio, el rendimiento del dispositivo y la experiencia con la aplicación. Cisco también ha sido pionero en la tecnología de asignación de radio flexible que optimiza el rendimiento de la red Wi-Fi sin limitar la disponibilidad del radio. Esta capacidad permite que los puntos de acceso inalámbricos identifiquen las necesidades inesperadas de ancho de banda inalámbrico y adapten automáticamente la red inalámbrica para satisfacer esas necesidades. Esto es fundamental en áreas en las que hay un gran número de usuarios que se disputan el ancho de banda inalámbrico.

La empresa digital depende de las aplicaciones que utiliza para aumentar la productividad y captar clientes. Cisco ofrece control y visibilidad de las aplicaciones para detectar las aplicaciones del perímetro conectado por cable o inalámbrico. Utilizamos un control de ruta inteligente para seleccionar la mejor ruta de su WAN a la vez que optimizamos la prestación por sus redes LAN inalámbricas o por cable para que los usuarios disfruten de la mejor experiencia posible con sus aplicaciones.

Las organizaciones pueden disfrutar de una visibilidad magnífica de más de 1200 de aplicaciones y priorizar las aplicaciones vitales para la empresa solo con hacer clic en un botón con APIC-EM y Cisco Prime Infrastructure.

El perímetro ofrece la posibilidad de controlar y mejorar la experiencia de los empleados en el espacio físico. El límite digital de Cisco amplía los beneficios de IoT al converger varias redes de construcción, como:

- Iluminación
- Calefacción y refrigeración
- Vídeo IP
- Sensores IoT
- Y mucho más a través de una plataforma de red segura e inteligente

El límite digital propicia nuevas experiencias y eficiencias para trabajadores, y reduce los costes de funcionamiento de las instalaciones.

Diseñado para lo que depare el futuro

Diseñado con el futuro en mente, sin un sistema operativo Cisco IOS-XE que tenga un modelo basado en estándares que impulsen la programabilidad, el perímetro de Cisco prepara la red para agregar la nueva funcionalidad y adaptarla según los cambios en el entorno, la empresa o el sector. Esto hace que la red del perímetro sea abierta, programable y extensible.

El perímetro cambia desde un modelo de dispositivo a dispositivo personalizado, en el que se agrega el control de acceso y segmentación a una configuración de red, hasta una solución de políticas automatizada completa. En el futuro, las redes no necesitarán aprovisionamiento directo. Podrá aplicar políticas de manera sencilla. Además, puede determinar qué usuarios o grupos tienen acceso a ciertos grupos de datos o aplicaciones, ya sea in situ o en la nube. La red se podrá aprovisionar automáticamente para ejecutar esta política, mientras siga habiendo una gran flexibilidad para supervisar, resolver problemas, remediar o aplicar servicios adicionales a un tráfico determinado.

El perímetro pasa a ser también completamente programable. Las soluciones de orquestación pueden interactuar con el perímetro mediante API impulsadas por el modelos estándar, programación Python u otras herramientas del estilo Linux. Esto facilita la integración del perímetro en métodos de desarrollo de software modernos, lo que posibilita una agilidad y personalización nunca vistas.

Innovación continua en el perímetro de la red

Con el aumento que se espera de la conectividad, que ofrece una oportunidad significativa, las empresas están empezando a reconocer que esta transformación requerirá cambios importantes en las infraestructura de sus redes y en la capacidad de gestionar y analizar los datos. Somos líderes gracias a esta transformación, al impulsar la innovación en la infraestructura de la red, la gestión de la infraestructura y el análisis para extraer percepciones procesables de los datos.

Cisco pretende transformar la resolución que es reactiva a proactiva, y reducir el tiempo de resolución de días a minutos. Lo haremos al tratar cada dispositivo de la red como un sensor y un elemento del procesamiento de datos distribuidos.

Al obtener los datos del dispositivo del perímetro, distribuyendo el procesamiento más cerca del origen de los datos, podemos realizar análisis a velocidad de línea para generar percepciones procesables por el aprendizaje mediante máquinas.

Con las mayores soluciones de ASIC personalizadas y de base instalada, Cisco se encuentra en una posición privilegiada para diseñar el hardware y el software optimizados para los análisis. Aproveche la eficiencia de la base instalada. Por cable o inalámbrica, en combinación con una red, logrará que la inteligencia del perímetro pueda ayudarle a resolver problemas en segundos, sucedan en el perímetro o no. Y con el tiempo corregirá los posibles problemas antes incluso de que se produzcan. Esto ayudará a los departamentos de TI a proporcionar en el acuerdo de nivel de servicio (SLA) el rendimiento de las aplicaciones y de las redes necesario para el futuro.

Conclusión

Con tanta responsabilidad en el perímetro de la red, la mercantilización de las redes LAN y WAN conectadas por cable o inalámbricas supone un riesgo que podría ocasionar la violación de la seguridad, la pérdida de productividad e ingresos, de oportunidad y la falta de visibilidad. El perímetro de red de Cisco permite que las organizaciones vayan más allá del enfoque disponible, proporcionando inteligencia de gran valor en el perímetro.

Este enfoque permite a la organización:

- Proteger la empresa con una fuerte primera línea de defensa
- Ofrecer de manera confidencial aplicaciones al público objetivo
- Ofrecer una experiencia ágil a los empleados en cualquier lugar
- Establecer relaciones con los clientes para impulsar un nuevo flujo de ingresos
- Gestionar mejor los dispositivos IoT y optimizar el entorno físico
- Proporcionar una visión óptima de lo que ocurre realmente en la empresa

Para obtener más información

Para obtener más información, visite la página de la tecnología Cisco Unified Access en http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.