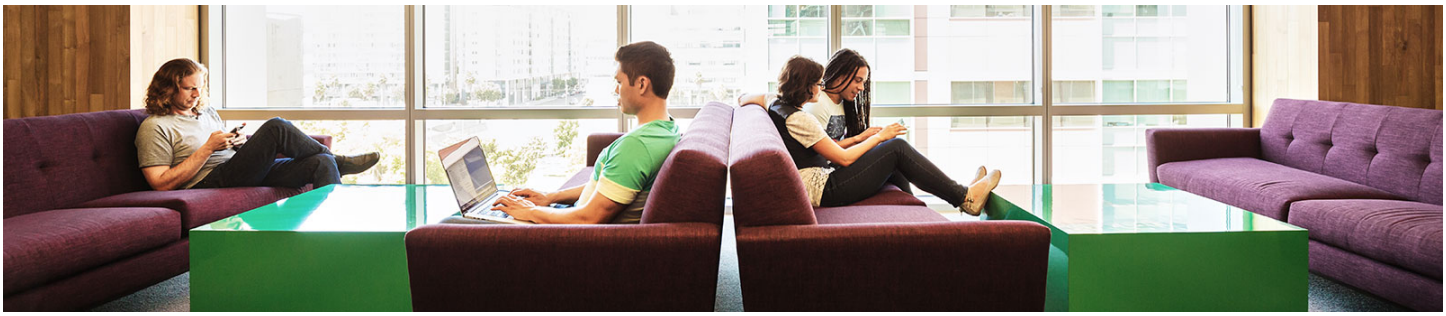


Informe técnico de Cisco Secure Network Access

Experiencia de acceso ininterrumpida y desconectada

Introducción

Ver webinars Ofertas disponibles Compare las soluciones

Los usuarios, las cosas y las aplicaciones están en todas partes, se mueven constantemente y se vuelven más “conectados” para hacer que nuestras vidas sean más cómodas. Sin embargo, a medida que aumenta nuestra dependencia de la conectividad de red, surge la necesidad de una nueva arquitectura. Con la expansión de la cantidad de dispositivos conectados, la creciente demanda de aplicaciones con uso intensivo de datos y las crecientes amenazas de red, las redes tradicionales simplemente no pueden mantenerse al ritmo de los cambios constantes en su entorno.

La infraestructura y el acceso a la red son partes fundamentales de cualquier organización. Desde el almacenamiento de importantes documentos financieros y de diseño hasta la colaboración interna del equipo y la comunicación con los clientes, cada operación comercial depende de un acceso a la red confiable, escalable y seguro.

La velocidad del cambio sigue aumentando. Por lo tanto, es imprescindible que las organizaciones cambien no solo la manera de hacer negocios, sino también la manera en que aplican la conectividad para hacerlo. A medida que aumenta la expectativa de los clientes, la criticidad de la conexión de red ininterrumpida y desconectada continúa aumentando y, con ella, la necesidad de una red inteligente en un mundo digital conectado.

Transformación de la red

Gartner predice que en 2023, más del 60 % de las empresas considerará que la red es fundamental para sus estrategias digitales, cifra superior respecto del menos del 20 % en la actualidad[(1)]. A medida que las organizaciones adoptan tecnologías digitales como la nube, la tecnología móvil y los análisis para innovar con mayor rapidez y ser más ágiles, claramente tienen una métrica clave en la mira: la experiencia del usuario. Ir más allá de la digitalización hacia la transformación digital al definir objetivos estratégicos (en gran parte impulsados por las exigencias de la experiencia del usuario) es donde las organizaciones son capaces de transformar fundamentalmente sus negocios para obtener ventajas competitivas en sus mercados.

Dado que casi todas las tecnologías digitales están intrínsecamente centradas en la red, la red se considera como el facilitador estratégico para estas iniciativas digitales. El ritmo acelerado y la incertidumbre de un entorno empresarial requieren que las redes se adapten rápidamente y admitan la velocidad de los negocios sin obstaculizar las transformaciones digitales exitosas.

Las empresas deben transformar sus redes para ocuparse de una cantidad masiva y cada vez mayor de usuarios, dispositivos y aplicaciones, y poder abordar todo tipo de problemas de conectividad y seguridad. Pueden impulsar sus prioridades empresariales y enriquecer las experiencias del cliente, tan solo al aprovechar la potencia y el valor de sus redes. Por lo tanto, la transformación digital está motivando la adopción de nuevas plataformas de red o, en otras palabras, la transformación de la red.

Desafíos de la red

Al recorrer el camino hacia una red preparada para la era digital, las organizaciones deben mirar más allá de las características básicas, como la conectividad rápida y la simplicidad de la administración. Su mejor conectividad y prestación de servicios posibles no garantizan que se abordarán las expectativas cambiantes de los clientes. En el mundo actual, la presión se encuentra en que la red conecte de manera segura todas las cosas digitales; y, si bien está claro que la red es la fuente del cambio transformacional, hay una gran cantidad de desafíos que se interponen en el camino.

Todos los días entra en el mercado un nuevo producto inalámbrico

Más de 4 mil millones dispositivos Wi-Fi llegan el mercado cada año. Las computadoras y los smartphones nuevos no son los únicos ni los principales impulsores de este crecimiento caótico de IoT; los dispositivos cotidianos desde termostatos y detectores de humo hasta relojes inteligentes sí lo son. Por ejemplo, una gran variedad de nuevos dispositivos de IoT especializados y variados, como la realidad aumentada (AR) y la realidad virtual (VR), avanzan rápidamente hacia empresas, escuelas, hospitales y empresas. Por lo tanto, ¿cómo nos aseguramos de que estos productos digitales se conecten sin inconvenientes a la red y ofrezcan la mejor experiencia posible del usuario?

Todo siempre está conectado y encendido

En el mundo actual conectado digitalmente, todo parece ser un conducto de Internet, desde bombillas hasta equipos médicos. Y a medida que más objetos requieren acceso a Internet, se prevé que para el año 2022 habrá 28,5 mil millones de dispositivos y conexiones en red en todo el mundo. Dado que estas cosas permiten la manera en que hacemos negocios y son menos tolerantes con el tiempo de inactividad que los seres humanos, deben depender de una conexión siempre activa. ¿Cuál sería la estrategia correcta para que las redes no se vean afectadas por deficiencias de latencia y ancho de banda?

Todo el mundo busca una experiencia unificada

Con un crecimiento exponencial en el número y los tipos de dispositivos móviles conectados a la red, las organizaciones de TI tienen la tarea de ofrecer una experiencia unificada para los usuarios. Los usuarios buscan una experiencia uniforme, ilimitada y siempre disponible desde sus dispositivos conectados desde cualquier lugar y en cualquier momento. Los administradores de redes están diseñando constantemente maneras eficientes de identificar, clasificar e incorporar dispositivos móviles de manera automática, para garantizar una política y administración uniformes en entornos cableados e inalámbricos, y para protegerse contra ataques sofisticados. ¿Cómo ayudamos a devolver el tiempo a los equipos de TI sin comprometer la seguridad y la productividad?

En todas partes, puede verse a un atacante que intenta nuevas formas de irrumpir

Con la oportunidad llegan los riesgos. La movilidad y la IoT, por definición, amplían la superficie de ataque, y cada vez más de estos productos no se administran y, en consecuencia, son vulnerables a las amenazas. A medida que los atacantes innovan, debemos estar un paso adelante con una red más inteligente y más segura que tenga una visibilidad profunda de los patrones de tráfico y la inteligencia más reciente para proteger y defender el negocio. ¿Su seguridad está incorporada o añadida?

Reinventar el acceso a la red

Los desafíos y las tendencias de la red dictan la necesidad de una nueva arquitectura de red: una arquitectura que no solo admita la optimización de la conectividad de cada usuario a la multinube, sino que pueda incorporarse de manera transparente y segura a un conjunto cada vez más diverso de dispositivos y aplicaciones.

Es hora de reinventar la red de acceso.

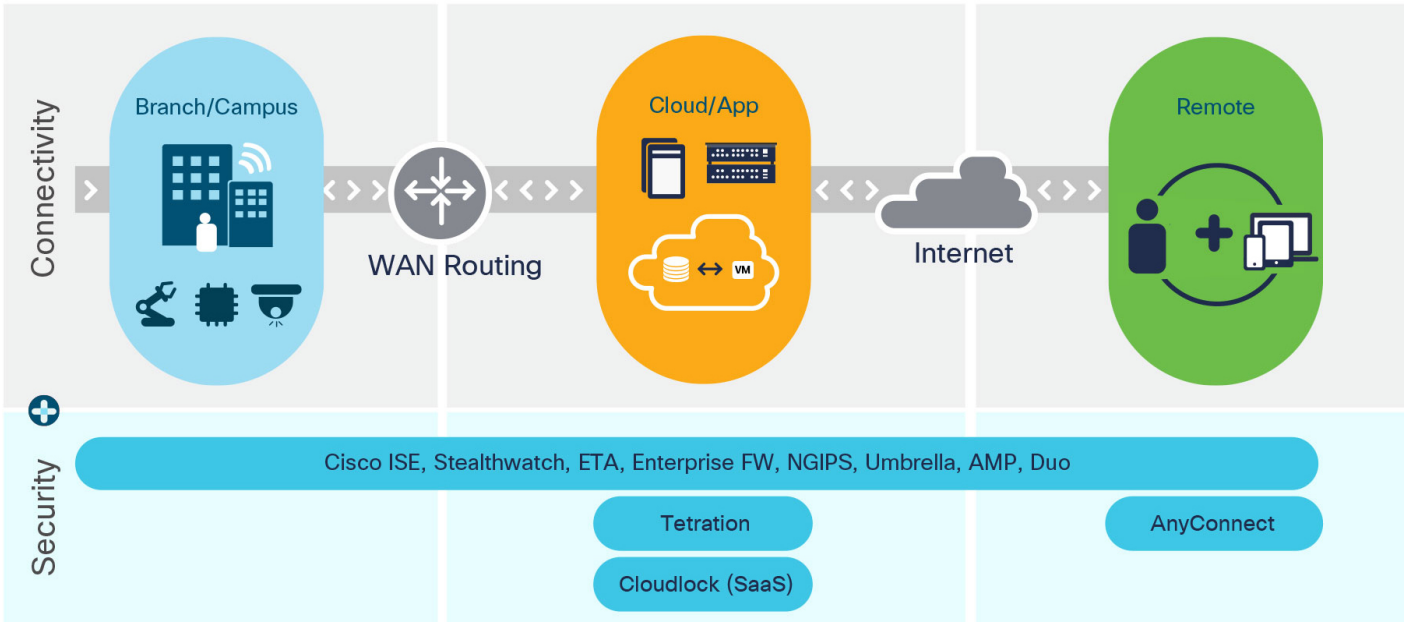
Cisco Secure Access es un plan avanzado para una nueva conectividad de red. Como arquitectura de red basada en la intención, ofrece una experiencia de conexión uniforme para los usuarios y sus dispositivos a los datos y las aplicaciones adecuados en cualquier momento y lugar. También garantiza un acceso confiable y seguro entre las cargas de trabajo dondequiera que residan (Figura 1).

Al automatizar y unificar la política de administración de acceso para todos los switches y productos inalámbricos y al analizar constantemente los datos de la red, Cisco Secure Access garantiza que la red respalde los objetivos comerciales deseados. Está diseñado para brindar mayor confiabilidad, agilidad y seguridad, y es capaz de admitir y administrar más usuarios y dispositivos, sin importar dónde se encuentran.

Los productos de redes habilitantes de esta arquitectura se extienden a cada switch y solución inalámbrica de Cisco, como los switches, puntos de acceso y controladores de Cisco Catalyst. Las soluciones de seguridad de Cisco están integradas en los productos de red. La integración permite que las aplicaciones de seguridad y la red trabajen en conjunto para reducir el tiempo de prevención, detección y mitigación de amenazas.

Cisco Tetration y Cisco Cloudlock para entornos en la nube son aplicaciones de seguridad diseñadas específicamente para atender dominios de red específicos, mientras que otras se expanden a través de varios dominios y pueden activarse en función del caso de uso específico del cliente. Por ejemplo, Stealthwatch puede detectar amenazas en toda la red privada, la nube pública y el entorno híbrido, mientras que Cisco Advanced Malware Protection (AMP) evita las intrusiones, detecta y elimina el malware de los terminales, así como de las redes.

Figura 1: Cisco Secure Access Architecture

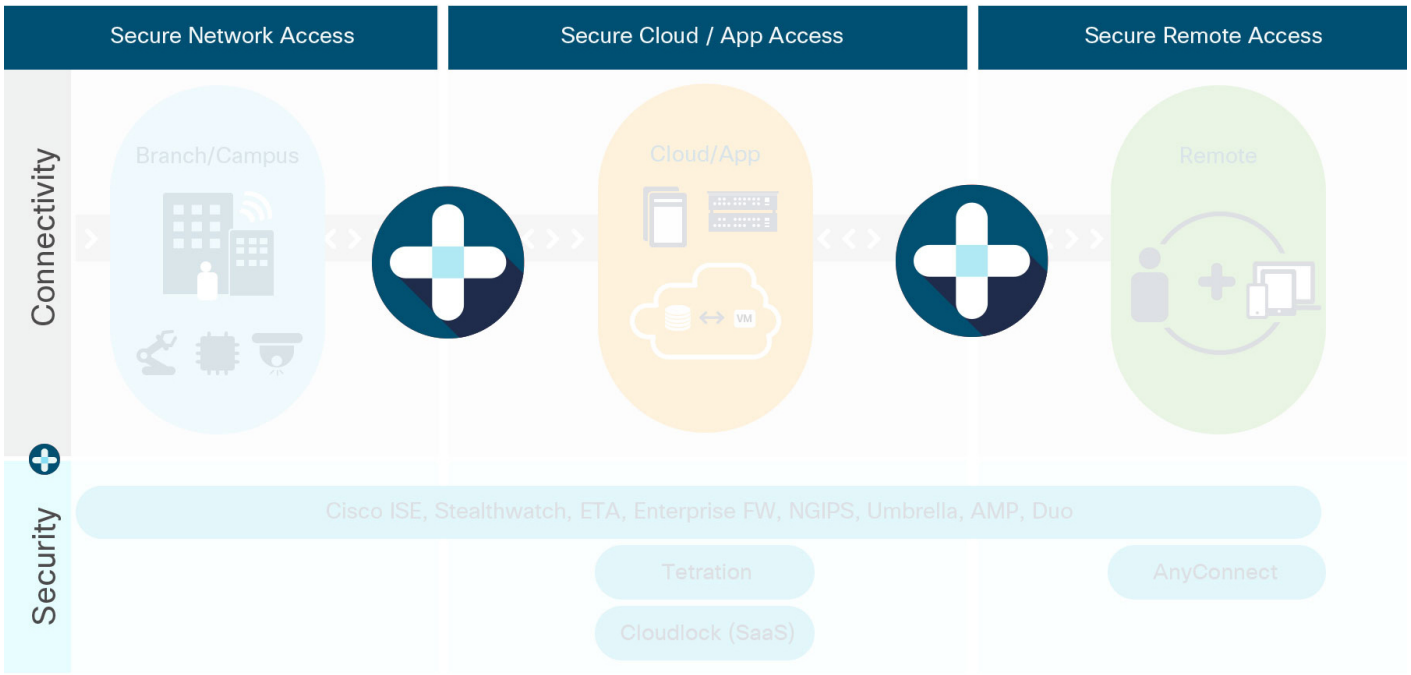


Esta experiencia de conectividad (o acceso) segura y sin inconvenientes debe abarcar cada dominio de red: sucursal, campus, sitio remoto, centro de datos y multinube. Esto significa que cada dominio de red funciona como una única solución de acceso seguro (Figura 2):

- **Acceso seguro a la red:** garantiza que todas las conexiones de usuarios, dispositivos y aplicaciones en y a través de las redes de la sucursal o del campus sean seguras
- **Acceso seguro a la nube/aplicación:** garantiza que solo los usuarios autorizados tengan acceso a los datos y a las aplicaciones dondequiera que residan.
- **Acceso remoto seguro:** garantiza que los usuarios remotos y los dispositivos tengan acceso seguro y uniforme a los datos y las aplicaciones.

Lo que une a estos dominios de redes es una administración de políticas de acceso compartido que permite que los dominios, mientras que funcionan de manera independiente, se unan para lograr la intención empresarial colectiva. Puede definir una política una vez, aplicarla en todas partes y monitorearla sistemáticamente para garantizar que se esté realizando su intención comercial[(2)]. Esta política de acceso sigue a los usuarios y las cargas de trabajo, independientemente de dónde se encuentren y de dónde vayan.

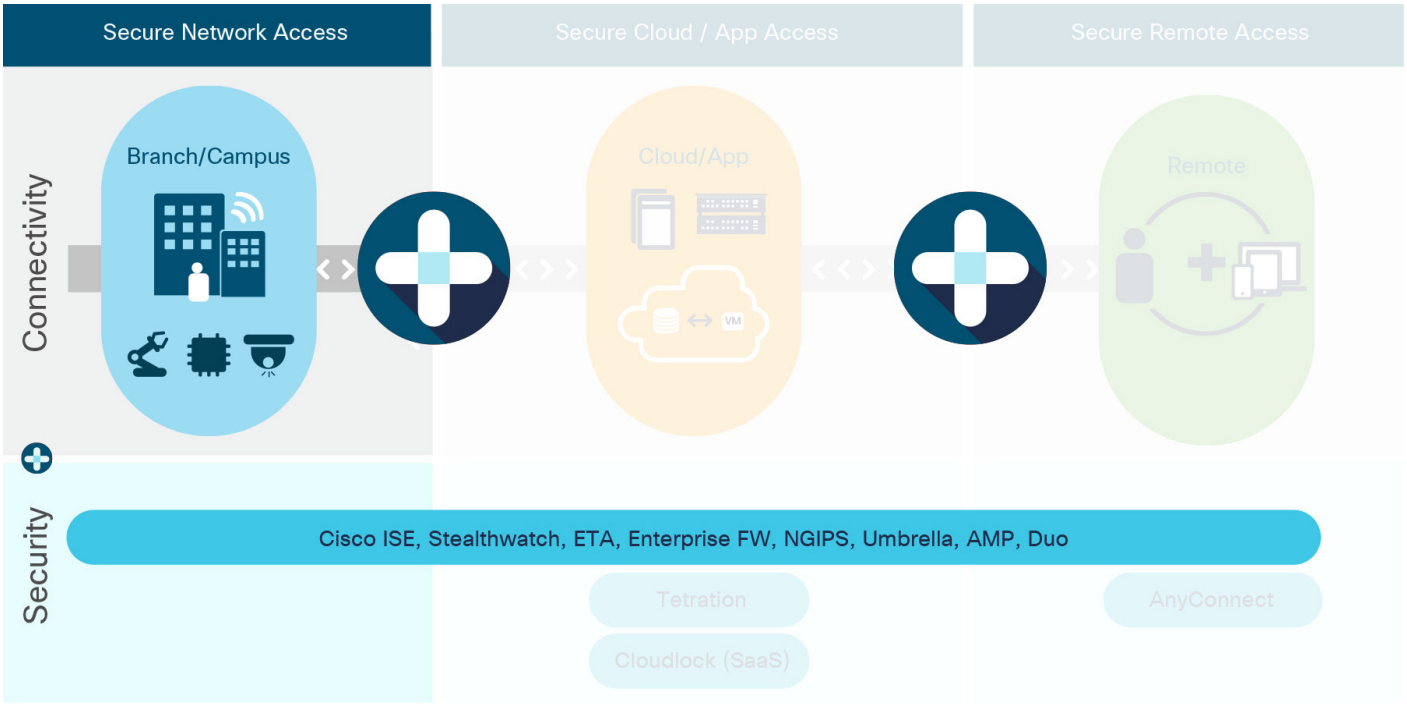
Figura 2: Componentes de Cisco Secure Access Architecture



Cisco Secure Network Access

Al unir una potente automatización de políticas y la coordinación de la red de análisis a través del software Cisco con una amplia gama de switches, puntos de acceso y controladores de última generación para el campus, Cisco Secure Network Access ayuda a TI a incorporarse de manera segura y segmentar a todos y todo lo que viene en las redes, lo que genera nuevos niveles de productividad empresarial y experiencia del usuario.

Figura 3: Cisco Secure Network Access



Los fundamentos de nuestras soluciones de acceso seguro a la red están anclados en cuatro principios arquitectónicos y puntos de diseño:

Tecnología inalámbrica en primer lugar

Hoy en día, la movilidad empresarial y el acceso a cualquier lugar han hecho que la tecnología inalámbrica sea el modo de conexión preferido para aplicaciones y datos. Para ofrecer una gran experiencia inalámbrica, necesita mirar más allá de Wi-Fi y crear un entorno inalámbrico dominante que siempre esté activo y siempre sea seguro para que los usuarios puedan recorrer sin inconvenientes y todo esté siempre conectado sin interrupciones. Cisco Secure Network Access es impulsado por soluciones cableadas de Cisco para crear un rendimiento y una confiabilidad óptimos para cualquier usuario o dispositivo en cualquier aplicación. Su estructura definida por software incorpora y segmenta de manera segura a todos y todo lo que se encuentra en las redes, lo que genera nuevos niveles de productividad empresarial y experiencia del usuario.

Impulsado por la nube

La nube acelera el ritmo de la innovación para ofrecer inteligencia impulsada por datos para las operaciones empresariales y de TI. Cisco Secure Network Access aprovecha un software de red basado en la nube con una escala inigualable para ofrecer nuevas innovaciones y adoptar funcionalidades para un mayor tiempo de obtención de valor. Permite que TI pase de reactivo a proactivo,

comprenda el estado de la red y vea tendencias antes de que afecten a los usuarios. El marco basado en la nube de la red de acceso brinda agilidad empresarial, eficacia operativa y coordinación uniforme de políticas en las redes cableadas e inalámbricas.

Optimización de datos

La red ofrece millones de puntos de datos, lo que brinda contexto a los usuarios, su experiencia y sus vulnerabilidades. Al agregar estos puntos de datos recopilados de todas las fuentes (usuarios, dispositivos, aplicaciones, amenazas) y utilizar análisis potentes y el aprendizaje automático, puede tomar mejores decisiones comerciales, de TI y de seguridad. Solo Cisco ofrece el acceso más amplio a los datos de la red a través de la integración de la pila completa de ASIC al software y a través de switching y productos inalámbricos. Estos datos pueden ofrecer perspectivas comerciales para experiencias personalizadas, perspectivas de TI para minimizar el tiempo de inactividad y conocimientos de seguridad para detectar y detener amenazas antes de que ocurran.

Siempre seguro

La seguridad integrada brinda visibilidad de quién y qué se encuentra en la red, control de todas las conexiones y segmentación definida por software para una superficie de ataque reducida basada en la intención comercial. Cisco es el único proveedor que ofrece una solución inalámbrica y cableada convergente integral que incluye seguridad, segmentación e innovaciones como el análisis de tráfico cifrado (ETA) que puede detectar la actividad de malware disfrazada de tráfico de red cifrado sin descifrar.

Componentes arquitectónicos

Como su nombre lo indica, los componentes básicos de Cisco Secure Network Access constan de dos capas funcionales: la red y la seguridad (Figura 4).

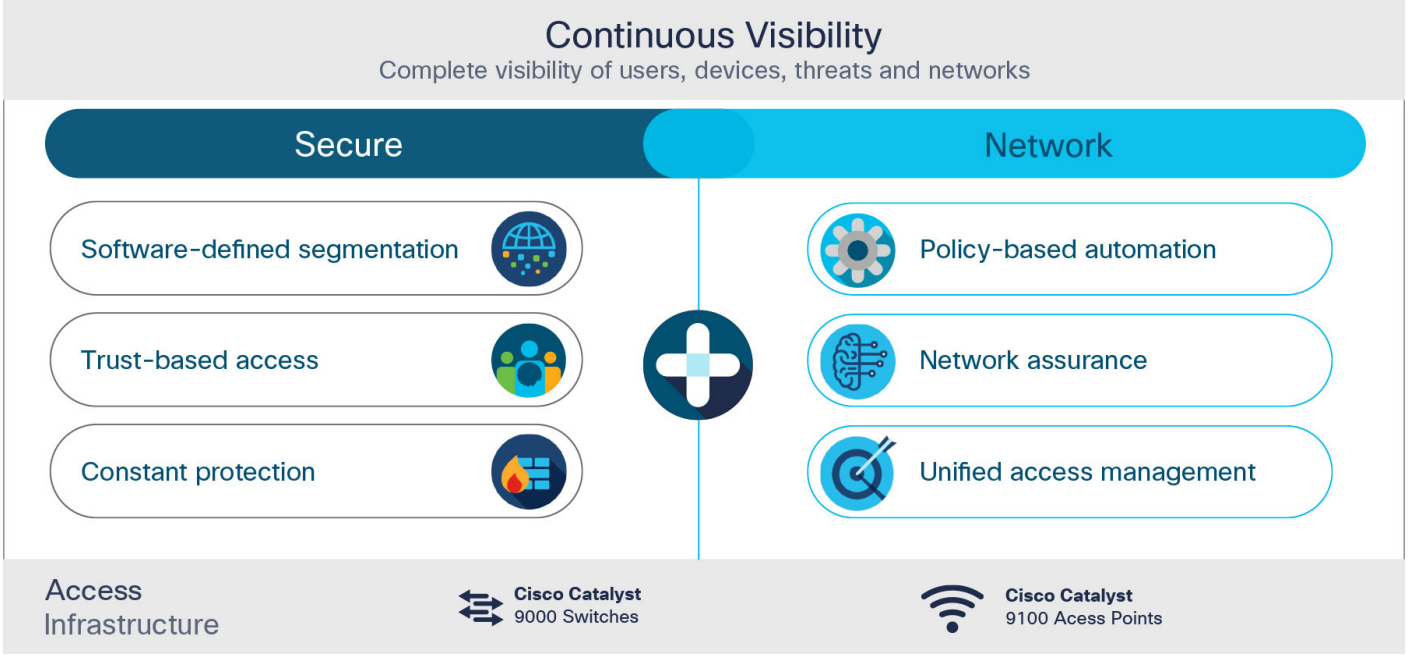
Un conjunto completo de portafolios Cisco Catalyst, switches Cisco Catalyst de la serie 9000 y puntos de acceso Cisco Catalyst 9100 es la infraestructura principal para esta solución. Los switches Cisco Catalyst 9000 son la próxima generación de switches de clase empresarial construidos para la seguridad, IoT, movilidad y multinube. Estos switches están optimizados para manejar el tráfico de Wi-Fi 6 y admiten la programabilidad y el mantenimiento completos, así como la convergencia entre tecnología cableada e inalámbrica en una sola plataforma.

Los puntos de acceso Cisco Catalyst 9100 impulsados por la tecnología Wi-Fi 6 y el soporte de la arquitectura de red basada en la intención de Cisco están listos para las crecientes expectativas de los usuarios, los dispositivos de IoT y las aplicaciones de última generación impulsadas por la nube. Con la capacidad de manejar el aumento del tráfico móvil, así como el soporte de IoT a escala, los puntos de acceso Wi-Fi 6 de Cisco tienen innovaciones de RF superiores y ampliarán el acceso inalámbrico con inteligencia para proporcionar una experiencia inalámbrica segura y confiable de alta calidad para todas las redes. Además de las funcionalidades de Wi-Fi 6, Cisco Catalyst 9100 amplía la potencia de las redes basadas en la intención con innovaciones de hardware y software, con el análisis avanzado y el soporte de múltiples RF (Wi-Fi, BLE y ZigBee). Junto con un mejor diseño industrial, ofrecen un rendimiento de RF mejorado y ofrecen confiabilidad, seguridad e inteligencia a escala.

Los puntos de acceso Cisco Catalyst 9100 constan de los puntos de acceso Cisco Catalyst 9115, 9117, 9120 y 9130, y son los productos de próxima generación para los puntos de acceso Cisco Aironet. Los puntos de acceso Catalyst 9120 y 9130 cuentan con la tecnología ASIC de RF de Cisco que realiza un análisis avanzado del espectro de RF y ofrece funciones exclusivas que superan el estándar para una experiencia de RF superior, que incluye:

- Tecnología Cisco CleanAir® para mitigar el impacto de la interferencia inalámbrica y proteger el rendimiento.
- Cisco Wireless Intrusion Prevention System (wIPS) para detectar, localizar, mitigar y contener elementos dudosos y amenazas cableadas o inalámbricas en las capas 1 a 3.
- Detección de selección dinámica de frecuencias (DFS) para evitar interferencias para un rendimiento óptimo.

Figura 4: Pilares de Cisco Secure Network Access



Nivel de red

La función de red de la solución Cisco Secure Network Access se basa en principios de redes basados en la intención: capturar la intención comercial y alinear la red de manera continua con esa intención. Esta capa está impulsada por la automatización avanzada y la coordinación unificada, y es capaz de escalar de cientos a miles e incluso a millones de usuarios y dispositivos conectados. El proceso manual de administración de dispositivos individuales (ya sea por cable o inalámbricos) como parte de una estructura unificada, se sustituye por una política basada en la intención administrada a nivel global, controlada desde una sola ubicación. Además, el uso del aprendizaje automático y el análisis contextual de los datos antes, durante y después de la implementación para cerrar la brecha entre lo que su empresa necesita y lo que su red ofrece en términos de escalabilidad, eficacia operativa y seguridad.

Las características clave de la capa de red pueden definirse en tres categorías principales:

Administración de acceso unificado

Una herramienta de administración unificada (Cisco DNA Center) se trata de implementar y administrar una infraestructura de red en la que las redes inalámbricas y cableadas se reconocen como igualmente críticas para la misión y se complementan entre sí. Esta consola controla no solo las funcionalidades comunes de la red, como el aprovisionamiento, la configuración, la supervisión de la conexión y la generación de informes, sino que es capaz de una administración inalámbrica específica, como la supervisión del espectro y la funcionalidad de seguimiento basada en la ubicación. Con su software de Cisco IOS común, Cisco DNA Center tiene

como objetivo optimizar la operación, agregar eficiencia y simplificar las tareas de administración mediante el uso de una sola interfaz para descubrir e incorporar nuevos usuarios y dispositivos a la creación y aplicación de políticas de acceso, a través de redes cableadas e inalámbricas.

Automatización basada en políticas

Para optimizar aún más la operación, además de la administración unificada, las redes cableadas e inalámbricas de Cisco se extienden e integran a través de varios dominios mediante la automatización basada en políticas para los usuarios, los dispositivos y las cosas. Esta es una funcionalidad única e instrumental para una implementación sin interacción, actualizaciones y mejoras de software sencillas y segmentación simplificada de aplicaciones, usuarios y dispositivos. La automatización elimina muchas operaciones manuales y serviles y obtiene un tiempo de respuesta más rápido para los negocios, ya que garantiza que se establezcan las políticas adecuadas para cualquier usuario o dispositivo con cualquier aplicación en toda la red.

Garantía de la red

Esta función crítica se refiere a la verificación continua, las perspectivas y las acciones correctivas. Cisco tiene un amplio acceso a los datos de la red en las infraestructuras cableadas e inalámbricas. Con la ayuda de Advanced Analytics y AI/ML, Cisco DNA Assurance puede aportar perspectivas clave sobre el negocio, proporcionar mayor visibilidad de la red y acelerar la corrección para solucionar problemas de la red.

Nivel de seguridad

Las aplicaciones de seguridad de Cisco garantizan una protección completa en todos los dominios de red. Con la seguridad integrada en las soluciones de Cisco Catalyst, puede obtener visibilidad de quién y qué se encuentra en la red, contribuir a un modelo completo de seguridad de acceso de confianza cero y desarrollar políticas de prevención, detección y respuesta de amenazas para una protección constante. En el campus y las sucursales, por ejemplo, Cisco Advanced Malware Protection (AMP) proporciona la máxima protección contra malware avanzado y Cisco Umbrella™ utiliza DNS para detener las amenazas en todos los puertos y protocolos. Además, Cisco ISE evita amenazas con su partición de red adaptable y dinámica, y el análisis de tráfico cifrado (ETA) de Cisco detecta la actividad de malware disfrazada de tráfico de red cifrado sin descifrar.

Las características clave de la capa de seguridad de Cisco Secure Network Access se pueden definir en tres categorías principales:

Segmentación definida por software

Con la capacidad de segmentar las redes, las organizaciones pueden controlar el nivel de acceso a ciertas secciones de la red de una empresa de usuarios, dispositivos y aplicaciones no autorizados. El aislamiento del tráfico que viene con la segmentación impide que los ataques se propaguen fácilmente en toda la red y se conviertan en intrusiones destructivas. Cisco Identity Services Engine (ISE) hace que sea fácil controlar la política de segmentación de manera uniforme en las conexiones inalámbricas y cableadas. Con ISE,

puede configurar grupos basados en roles para usuarios y dispositivos, y asignarlos a los niveles adecuados de acceso que necesitan, aplicando automáticamente las políticas de acceso mediante las identidades contextuales de cada terminal.

Las soluciones cableadas e inalámbricas de Cisco garantizan el aislamiento y la seguridad completos del tráfico entre segmentos, así como la protección de los datos dentro de cada segmento mediante un conjunto de funcionalidades de seguridad integradas de manera nativa, como firewall empresarial, filtrado de URL, intrusión prevención y monitoreo de DNS.

Acceso basado en la confianza

Cisco Zero Trust es un enfoque integral para garantizar el acceso a todos los usuarios, dispositivos, API, IoT y muchos más dentro de sus redes. Protege su fuerza laboral, las cargas de trabajo y el lugar de trabajo.

El acceso definido por software de Cisco (SD-Access) una solución de confianza cero de Cisco para la red del campus, permite y aplica grupos de políticas de seguridad uniformes para el control de acceso basado en roles de gran escala empresarial. Mejora la experiencia del usuario mediante la automatización de la política de acceso y la aplicación del nivel adecuado de acceso a los usuarios y los dispositivos con autenticación y autorización de la red. A través de la integración con un ecosistema de otras aplicaciones y productos de seguridad, como Umbrella o AMP, puede proporcionar una seguridad de confianza cero completa para el entorno del campus empresarial.

Protección constante

Las aplicaciones y las soluciones de seguridad integradas de Cisco le brindan el alcance, la escala y las funcionalidades para estar al tanto de la complejidad y el volumen de las amenazas. Proporcionan funciones de seguridad avanzadas que protegen la integridad del hardware, así como el software y todos los datos que pasan por el switch y la red. Garantizan una protección constante que solo puede lograrse mediante la creación de prevención, detección y respuesta ante amenazas en cada dispositivo de red.

Con el acceso a las mejores soluciones, como Cisco Stealthwatch, puede averiguar quién está en su red y qué está haciendo con la telemetría de la infraestructura de red.

Visibilidad continua

La visibilidad completa de los entornos de TI que cambian rápidamente, inicialmente móviles e impulsados por la nube es fundamental para cubrir las brechas en las soluciones de red perimetral tradicionales. En un entorno del campus, la visibilidad comienza con la clasificación de quién y qué se encuentra en la red del campus, dónde se conectan los dispositivos móviles de propiedad personal o los puntos de acceso inalámbricos dudosos, y cómo los usuarios o los dispositivos de IoT interactúan con los servicios o las aplicaciones. Obtener una comprensión base de todas las comunicaciones de red, incluso en la nube, ofrece un inventario completo en el que se puede crear una política basada en grupos. Permite supervisar el comportamiento inusual, lo que podría representar una amenaza o una violación de políticas. También el aprendizaje automático es fundamental para clasificar mejor todos los tipos de dispositivos o cargas de trabajo y para identificar más rápidamente las anomalías de base.

Conclusión

Las organizaciones de todos los tamaños pueden acelerar su proceso de transformación digital con una sólida base de red basada en la intención proporcionada por Cisco Secure Network Access. Ofrece la nueva era de conectividad cableada e inalámbrica, lo que alimenta una nueva era de experiencias de red inmersivas, con la capacidad de implementar software de red en la nube para ofrecer nuevas innovaciones a escala. La red inalámbrica es la prioridad, está impulsada por la nube y optimizada para datos con seguridad en el núcleo. A diferencia de otras soluciones, Cisco Secure Network Access ofrece un modelo operativo simplificado con una administración, un sistema operativo común, una seguridad generalizada y una política común en las redes cableadas e inalámbricas. Con él, los equipos de TI pueden automatizar y escalar la conectividad de red a miles de usuarios y dispositivos, anticipar el cambio y alternar de manera rápida y segura a medida que adoptan las mejores prácticas con una red diseñada para el futuro.

Serie de demostraciones de software Cisco DNA

50 % de Catalyst serie 9800

Recursos

Cisco Secure Network Access

Una red inteligente con una infografía de seguridad integrada

Puntos de acceso Cisco Catalyst 9100

Familia de switching e inalámbrica Cisco Catalyst 9000

Solución Cisco Wi-Fi 6 (802.11 AX)

Fuentes

(1) Informe de tendencias en redes

(2) Integraciones multidominio de Cisco para redes basadas en la intención

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.
© 2020 Cisco and/or its affiliates. All rights reserved.