Resumen

Beneficios

- **Centralice y unifique un control de acceso altamente seguro** basado en el rol empresarial para brindar una política uniforme de acceso a la red a los usuarios finales, mediante conexión cableada, inalámbrica o de VPN.
- **Obtenga una mayor visibilidad y una identificación de dispositivos más precisa** mediante la creación de perfiles de los dispositivos de Cisco® Identity Services Engine (ISE) y el servicio de alimentación de perfiles de dispositivos que, en conjunto, reducen la cantidad de terminales desconocidos.
- **Simplifique las experiencias de los usuarios temporales** para lograr una integración y administración más sencillas de los dispositivos de estos usuarios mediante portales de marca móviles y de escritorio para los usuarios temporales completamente personalizables, creados en pocos minutos con flujos de trabajo dinámicos y visuales que le permiten administrar fácilmente la experiencia del acceso de los usuarios temporales.

Cisco Identity Services Engine

La red empresarial ya no se encuentra dentro de cuatro paredes seguras. Se extiende hasta donde llegan los empleados y los datos. Los empleados exigen ahora más que nunca el acceso a los recursos de trabajo desde más dispositivos y a través de más redes no empresariales. La movilidad e Internet de todo (IdT) están cambiando la forma en que vivimos y trabajamos. Las empresas se encuentran ante el desafío de tener que brindar soporte a la proliferación de nuevos dispositivos habilitados para la red mientras que una infinidad de amenazas de seguridad y violaciones de datos de público conocimiento demuestran claramente cuán importante es proteger el acceso a la red empresarial en constante evolución.

A medida que se expande la red moderna, también crece la complejidad de poner en orden los recursos, administrar soluciones de seguridad dispares y controlar los riesgos. La extendida conectividad de IdT, los ya restringidos recursos de TI y el impacto potencial de no lograr identificar y remediar las amenazas de seguridad, en conjunto, se vuelve ciertamente más grande.

Se requiere de un enfoque diferente tanto para administrar como para asegurar la empresa móvil en evolución. Se llama Cisco® Identity Services Engine (ISE).

Limite su exposición y reduzca el riesgo

Adelántese a las amenazas con visibilidad y control. Esto incluye una profunda visibilidad de los usuarios y dispositivos que acceden a la red y el control dinámico para asegurarse de que solo las personas permitidas con los dispositivos correctos obtengan el acceso justo a los servicios empresariales.

ISE 2.0, con su nuevo diseño, simplifica aún más la distribución uniforme del control de acceso seguro en redes de varios proveedores tanto cableadas como inalámbricas y conexiones VPN remotas. Con las funcionalidades inteligentes de gran alcance de sensores y creación de perfiles, Cisco ISE puede alcanzar una mayor profundidad en la red para ofrecer visibilidad superior de quién y qué accede a los recursos. Con la posibilidad de compartir datos contextuales vitales con las integraciones de partners del ecosistema y la implementación de políticas de Cisco TrustSec para la segmentación definida por software, Cisco ISE transforma la red para que pase de ser un simple conducto por el que circulan los datos a ser un guardián de la seguridad que acelera el tiempo de detección y el tiempo de resolución de amenazas a la red.

© 2015 Cisco y/o sus filiales. Todos los derechos reservados.

- **Acelere el BYOD y la movilidad empresarial** con una configuración sin complicaciones, asignación y administración de autoservicio para los dispositivos, administración interna de certificados de dispositivos y software partner de administración de movilidad empresarial (EMM) para la asignación de dispositivos tanto dentro como fuera de las instalaciones.
- **Cree una política de segmentación definida por software para contener las amenazas a la red** mediante la tecnología Cisco TrustSec® para aplicar un control de acceso basado en roles en la capa de routing y switching. Segmente el acceso de manera dinámica sin la complejidad de LAN múltiples o la necesidad de volver a diseñar la red.
- **Comparta datos contextuales completos con soluciones de seguridad y redes de partners** para mejorar la eficiencia general así como para acelerar el tiempo de detección (TTD) y el tiempo de resolución (TTR) de las amenazas a la red.
- **Contenga automáticamente las amenazas** gracias a la integración con Cisco Firepower Management Center, ya que ISE puede contener los terminales infectados para corregirlos, observarlos o eliminarlos.

Las actualizaciones y mejoras de ISE 2.0 incluyen:

- Integración con Cisco Mobility Services Engine (MSE) para proporcionar datos de ubicación a fin de crear y aplicar el acceso específico a la ubicación para que, por ejemplo, los profesionales médicos puedan acceder solo a los registros médicos de los pacientes que se encuentran en la sala de emergencias.
- Mejora de nuestra arquitectura abierta para ciertos partners del ecosistema de ISE, para que los clientes puedan usar sus soluciones de seguridad existentes para trabajar con ISE e identificar las amenazas en la red a fin de contenerlas y corregirlas rápidamente.
- Soporte para terminales IPv6 y dispositivos de acceso a la red (NAD) de terceros, que extiende la llegada y el alcance de ISE para que los terminales se encuentren en cumplimiento en una variedad mayor de redes.
- Administración de políticas optimizada, incluida la administración de dispositivos con autenticación, autorización y auditoría (AAA) simplificada con funcionalidades de acceso RADIUS y TACACS+, para que la implementación de políticas de control de acceso seguro en las redes cableadas sea mucho más fácil.
- Con Cisco AnyConnect 4.2 se presenta el nuevo módulo de visibilidad de la red (NVM) que proporciona un nivel de detalle de los flujos de tráfico de las aplicaciones que antes no estaba disponibles sobre los terminales fuera de las instalaciones.

Además, ISE utiliza la tecnología Cisco Platform Exchange Grid (pxGrid) para compartir datos contextuales completos con las soluciones integradas del ecosistema de partners. Esta tecnología acelera las funcionalidades para identificar, mitigar y solucionar amenazas de seguridad en toda su red extendida. En general, el control de acceso seguro está centralizado y simplificado para desempeñar los servicios vitales del negocio de manera segura, mejorar la seguridad de la infraestructura, asegurar el cumplimiento y modernizar las operaciones de servicios.

Gracias a las integraciones con soluciones líderes de información de seguridad, defensa contra amenazas (TD) y administración de eventos (SIEM), una visibilidad de red profunda y funcionalidades de control de acceso seguro, ISE desempeña un papel fundamental en las soluciones de defensa ante amenazas cibernéticas, red como sensor y red como guardián de Cisco. Por último, ISE brinda la visibilidad, el contexto y el control dinámico que requieren las empresas para implementar de manera eficaz la seguridad que aborda la secuencia completa del ataque, pues administra el acceso a la red antes de un ataque, permite la visibilidad y contención de las amenazas durante un ataque, y mejora el tiempo de detección (TTD) y el tiempo de resolución (TTR) después de un ataque.

Próximos pasos

Para obtener más información sobre Cisco ISE, visite http://www.cisco.com/go/ise o comuníquese con su ejecutivo de cuenta local.

© 2015 Cisco y/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 comerciales de Cisco, visite la siguiente URL: www.cisco.com/go/trademarks. Todas las marcas registradas 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 compañía. (1110R)
C45-654884-13 10/15