Resumen

Ventajas

- **Centralizar y unificar el control de acceso de alta seguridad** basándose en roles empresariales para lograr una política de acceso a la red uniforme para los usuarios finales, tanto si se conectan a través de una red por cable o inalámbrica como mediante una VPN.
- **Conseguir una mayor visibilidad y una identificación más precisa de los dispositivos** mediante el servicio de difusión de perfiles de dispositivos y la definición de perfiles de Cisco® Identity Services Engine (ISE), lo que reduce el número de terminales desconocidos.
- **Simplificar la experiencia de los invitados** para lograr conectarlos y administrarlos de forma más sencilla mediante portales de invitados para equipos de escritorio o móviles totalmente personalizados que se crean en cuestión de minutos y ofrecen flujos de trabajo visuales y dinámicos para gestionar fácilmente la experiencia de los invitados.

Cisco Identity Services Engine

La red de la empresa ya no está entre cuatro paredes seguras. Llega hasta donde viajen los empleados y los datos. Los empleados exigen poder acceder a los recursos profesionales desde más dispositivos y a través de más redes no corporativas que nunca. La movilidad y el concepto de Internet of Everything (IoE) están cambiando la forma en que vivimos y trabajamos. Las empresas deben hacer frente a la proliferación de nuevos dispositivos listos para conectarse a la red, mientras que la enorme cantidad de amenazas de seguridad y las brechas en los datos de gran trascendencia pública demuestran claramente la importancia de garantizar la seguridad del acceso a una red empresarial en evolución.

A medida que se expanden las redes modernas, también aumenta la complejidad de administrar los recursos, gestionar soluciones de seguridad diversas y controlar los riesgos. Si añadimos la conectividad en cualquier lugar de IoE a unos recursos de TI limitados, el impacto potencial de no identificar y remediar las amenazas de seguridad aumenta notablemente.

Se requiere un enfoque diferente para la gestión y la protección de la red empresarial que no deja de evolucionar. La solución se llama Cisco® Identity Services Engine (ISE).

Limite su exposición y reduzca el riesgo

Anticípese a las amenazas gracias a una mayor visibilidad y un mejor control. Esto incluye una amplia visibilidad de los usuarios y los dispositivos que acceden a la red y el control dinámico necesario para asegurarse de que solo las personas apropiadas que usen los dispositivos adecuados tengan el acceso correspondiente a los servicios corporativos que necesitan.

La solución ISE 2.0 se ha rediseñado para facilitar aún más un control de acceso seguro uniforme a través de redes por cable o inalámbricas de varios proveedores y las conexiones VPN remotas. Con funciones de definición de perfiles y sensores inteligentes de gran alcance, Cisco ISE profundiza en la red para ofrecer una visibilidad superior acerca de quién y qué accede a los recursos. Al compartir datos contextuales vitales con integraciones de partners de ecosistema y la implementación de la política de Cisco TrustSec para la segmentación definida por software, Cisco ISE transforma la red para que deje de ser un simple conducto de datos y se convierta en un agente de seguridad estratégico que reduzca el tiempo necesario para la detección y resolución de las amenazas de red.

- **Agilizar el modelo BYOD y la movilidad corporativa** con configuraciones sencillas, aprovisionamiento y gestión automática de dispositivos, así como software de gestión interna de certificados de dispositivos y administración integrada de la movilidad empresarial (EMM) para facilitar la conexión de dispositivos tanto dentro como fuera de la empresa.
- **Crear políticas de segmentación basadas en software destinadas a contener las amenazas para la red** usando la tecnología Cisco TrustSec® para aplicar el control de acceso basado en roles en la capa de routing y switching. Segmentación dinámica del acceso sin la complejidad de varias VLAN ni la necesidad de rediseñar la red.
- **Compartir datos contextuales sofisticados con soluciones de seguridad y redes de partners** para aumentar su eficacia general, además de reducir el tiempo de detección (TTD) y de resolución (TTR) de las amenazas en la red.
- **Contener automáticamente las amenazas mediante** la integración con Cisco Firepower Management Center, ya que ISE puede contener terminales infectados para su remediación, observación, o eliminación.

Entre las actualizaciones y mejoras que ofrece ISE 2.0, destacamos las siguientes:

- Integración con Cisco Mobility Services Engine (MSE) para proporcionar datos de ubicación que permitan crear y aplicar un acceso específico a la ubicación a fin de que, por ejemplo, los profesionales médicos solo puedan acceder a los historiales médicos de los pacientes que están en urgencias.
- Mejora de nuestra arquitectura abierta para ciertos partners del ecosistema ISE con objeto de que los clientes puedan usar las soluciones de seguridad existentes para trabajar con ISE e identificar las amenazas en la red con la finalidad de contenerlas y remediarlas.
- Compatibilidad con dispositivos de acceso a red (NAD) de terceros y terminales IPv6 para ampliar el alcance y el ámbito de ISE a fin de lograr la conformidad con los terminales en una gama de redes más amplia.
- Administración de políticas optimizada, incluidos aspectos como la administración simplificada de dispositivos mediante autenticación, autorización y administración (AAA) con capacidades de acceso TACACS+ y RADIUS para facilitar enormemente la implementación de una política de control de acceso seguro.
- Con Cisco AnyConnect 4.2 se incluye el nuevo Network Visibility Module (NVM), que proporciona información detallada sobre los flujos de tráfico de aplicaciones que antes no estaba disponible en los terminales fuera de las instalaciones.

Además, ISE usa la tecnología Cisco Platform Exchange Grid (pxGrid) para compartir diversos datos contextuales con las soluciones del ecosistema de partners integrados. Esta tecnología aumenta su capacidad de identificar, mitigar y remediar las amenazas de seguridad en su red extendida. En general, se centraliza y simplifica el control de acceso seguro para prestar servicios empresariales cruciales seguros, aumentar la seguridad de la infraestructura, aplicar el cumplimiento de normativas y optimizar las operaciones de servicio.

Gracias a su integración con soluciones punteras de sistemas de gestión de eventos e información de seguridad (SIEM) y de defensa frente a amenazas (TD), su profunda visibilidad de la red y sus funciones de control de acceso seguro, ISE desempeña un papel integral en soluciones como Cisco Cyber Threat Defense, Network-as-a-Sensor y Network-as-an-Enforcer. En resumen, ISE ofrece la visibilidad, el contexto y el control dinámico que necesitan las empresas para implantar de forma eficaz una seguridad que aborde todo el ciclo del ataque, por lo que gestiona el acceso a la red antes de un ataque, ofrece visibilidad y contención de amenazas durante un ataque y reduce el tiempo de detección (TTD) y el tiempo de resolución (TTR) después de un ataque.

Siguientes pasos

Para obtener más información acerca de Cisco ISE, visite http://www.cisco.com/go/ise o póngase en contacto con su representante de cuenta local.

C45-654884-13 10/15