Video: Aspectos básicos de ISE (5 min)

Recuerdo mi primera política de seguridad. Tan simple. El contenido bueno queda, el contenido malo sale. De todas formas, con los años, se hizo bastante difícil trazar una línea entre lo bueno y lo malo. Por lo que, una política se convirtió rápidamente en dos, luego en 10, y más y, una vez creadas, también había que aplicarlas. Ahora hay cumplimiento y existe la necesidad de probar que estoy seguro. Además de todo eso, todo el mundo lleva su dispositivo Wi-Fi preferido y espera obtener un acceso total a la red. Mantenerse al día en estas cuestiones implica tiempo, personal y dinero, sin mencionar cómo traduzco términos de la política como ubicación, usuarios, dispositivos y aplicaciones en idioma "Geek" como IP, MAC, ACL, puertos, y 802.1x. ¡Suficiente! Una respuesta para nosotros.

El Cisco Identity Services Engine o ISE es una plataforma de políticas basada en la identidad que permite el cumplimiento, aumenta la seguridad y agiliza las operaciones. Su arquitectura única permite recabar información contextual en tiempo real acerca de los usuarios y los dispositivos, a fin de aplicar la política de gobernanza en toda la infraestructura de la red. Si pensamos en eso, ¿cómo podría todo esto ser de otra forma? Como elemento central de política de la solución TrustSec de Cisco, ISE es la única fuente de creación de políticas, control y generación de informes. ¿Quieren conectarse a mi red?

Permítame mostrarle el conjunto de herramientas. Triple A. Autenticación, autorización y contabilidad. ¿Cuál es su nombre de usuario y su contraseña? Genial. Le daré acceso solo a lo que necesita, y por cierto, estoy registrando esta sesión por si acaso. Postura. ¿Está limpio este dispositivo? ¿Tiene aplicaciones sospechosas o virus? ¿No? Detector de perfil. Dice ser una impresora, ¿pero actúa como una cámara web? Le enseñaré la puerta. ¡Fuera! Y ahora, administración de usuarios temporales. ¿Necesita acceso temporal? No hay ningún problema. Tendrá el acceso necesario, pero cuando termine el tiempo, se interrumpirá. Y automáticamente. La ventaja para mi es que ni siquiera lo tengo que configurar como usuario temporal. Todo eso lo hace la persona que quería que la visitara.

Muchos de ustedes deben pensar: “Esto suena a Cisco NAC y ACS”. Y tienen razón. Es ahí donde comienza. ISE combina la funcionalidad de los dos, con una implementación más sencilla y una administración común. Avanzando en el tema, ISE se extenderá más en la red, el centro de datos y la capa de aplicación. Cisco Identity Services Engine es la única fuente de verdad de los terminales de la red.

Ahora, realmente solo hay dos paquetes para entender aquí. El paquete base se relaciona con la autenticación, la ID y los servicios para usuarios temporales como lo que se ofrece en Cisco ACS y NAC Guest Server. El paquete avanzado agrega la detección de perfiles y servicios de posturas a la combinación. Un análisis más profundo e inteligente de cualquier elemento que solicite acceso. NAC Appliance y Profiler serían los puntos de referencia aquí. Y para anticiparme a la próxima pregunta lógica, no, esto no significa el fin de vida útil para NAC o ACS. Cada red es distinta. ICS es para los que queremos consolidar políticas dentro del marco 802.1x. Por otro lado, están los que quieren un cuello de botella en línea o quizá desean autenticar únicamente a los dispositivos de los administradores u otra cosa. Bien, ¿productos NAC o ACS existentes? Van a ser una mejor opción.

Ahora, hablando de la mejor opción, tiene tres dispositivos de hardware diferentes para elegir, así como un dispositivo virtualizado basado en VMware. Dado que Cisco envía el mismo hardware que utilizan NAC y ACS, hay una protección incorporada de la inversión. Siempre un punto a favor para ofrecer a las personas conservadoras, ¿correcto? A diferencia de otras soluciones, Cisco ISE permite ejecutar determinadas funciones en puntos críticos de la red. Por ejemplo, un par de dispositivos ISE para administración, mantenimiento, solución de problemas e inicio de sesión con una configuración de alta disponibilidad. Esto podría encontrarse en una ubicación centralizada, pero con dispositivos distribuidos para tomar decisiones sobre políticas lo más cerca posible del usuario o dispositivo, que se comunican con la infraestructura de red Cisco para fines de cumplimiento. Este es un punto de diseño realmente importante para mencionar. Cisco ISE trabaja con sus dispositivos de red actuales, switches, controladores inalámbricos y concentradores de VPN, a fin de equilibrar la carga de trabajo y mantener el cumplimiento lo más cerca posible del terminal. Si tiene equipos antiguos en su red, no se preocupe. ISE también puede realizar la tarea de cumplimiento con ellos. Este ejemplo era un diseño de red grande simplemente para ilustrar la flexibilidad disponible.

Aún puede obtener un gran valor con solo dos de estos elementos. Redundancia, ¿correcto? Comience poco a poco, agregue capacidad mediante equipos o licencias adicionales en la medida que sean necesarios. De acuerdo. Nuestro ataque de la complejidad sigue ahora con una interfaz simple que incluye cosas como un panel centralizado con vínculos activos para obtener más detalles, filtrado flexible de la sesión activa, reorganización de reglas mediante la función arrastrar y soltar, objetos reutilizables. ISE emplea widgets de última generación para hacer saltos de página y desplazamientos increíbles. Simplemente le encantará la claridad que proporciona ISE en este punto. La visibilidad de lo que sucedió, cuándo sucedió, quién y qué estaban involucrados y cómo se manejó. Todos sabemos que la complejidad es enemiga de la buena seguridad. Por eso, el panel de ISE, las herramientas de informes y los registros en vivo son tan robustos y valiosos.

Así que aquí lo tiene. Cisco Identity Services Engine. Único punto de verdad para la restauración de visibilidad y control al borde de la red. Ya basta, ¿ah? ¿Por qué no lo comprueba usted mismo? (rascarse con un lápiz)