Control de admisión a la red de Cisco

El propósito de Cisco Network Admission Control (NAC) es permitir que solo los sistemas autorizados y compatibles, ya sean administrados o no administrados, accedan a la red. Cisco NAC también está diseñado para hacer cumplir la política de seguridad de la red. NAC ayuda a mantener la estabilidad de la red al proporcionar autenticación, autorización y evaluación de la postura (evaluar un dispositivo entrante en comparación con las políticas de la red). NAC también pone en cuarentena los sistemas que no cumplen con los requisitos y gestiona la reparación de los sistemas que no cumplen.

Como se muestra en la tabla de la Figura 1, hay dos categorías de productos Cisco NAC:

- **Marco de NAC: el marco de** NAC utiliza la infraestructura de red de Cisco existente y el software de terceros para imponer el cumplimiento de la política de seguridad en todos los puntos finales. Como se muestra en la Figura 2, diferentes dispositivos en la red, no necesariamente un solo dispositivo, pueden proporcionar las características de NAC.

- **Dispositivo NAC de Cisco**: como parte de la solución Cisco Obsec, el dispositivo NAC de Cisco incorpora funciones NAC en un dispositivo y proporciona una solución para controlar el acceso a la red.

El dispositivo NAC de Cisco se puede utilizar para:

- Reconocer a los usuarios, sus dispositivos y sus roles en la red.

- Evaluar si las máquinas cumplen con las políticas de seguridad.

- Haga cumplir las políticas de seguridad bloqueando, aislando y reparando las máquinas que no cumplen con las normas

- Proporcionar acceso fácil y seguro a los huéspedes

- Simplifique el acceso a dispositivos no autenticados.

- Auditar e informar quién está en la red.

El dispositivo NAC de Cisco extiende NAC a todos los métodos de acceso a la red, incluido el acceso a través de redes LAN, pasarelas de acceso remoto y puntos de acceso inalámbrico. También es compatible con la evaluación de la postura de los usuarios invitados.

Nota: los NAC están evolucionando de la protección de seguridad básica a los controles más sofisticados de **visibilidad, acceso y seguridad de los puntos finales (EVAS)**. A diferencia de las tecnologías NAC anteriores, EVAS utiliza información más granular para aplicar políticas de acceso, como datos sobre la función del usuario, la ubicación, las consideraciones de los procesos empresariales y la gestión de riesgos. Los controles EVAS también ayudan a otorgar acceso más allá de las computadoras, permitiendo a los administradores de red proporcionar acceso a través de dispositivos móviles e IoT.

Funciones Cisco NAC

El objetivo tanto del marco NAC como del dispositivo NAC de Cisco es garantizar que solo los hosts que están autenticados y que han examinado y aprobado su postura de seguridad estén permitidos en la red. Por ejemplo, las computadoras portátiles de la empresa utilizadas fuera del sitio durante un período de tiempo podrían no haber recibido actualizaciones de seguridad actuales o haberse infectado con otros sistemas. Esos sistemas no pueden conectarse a la red hasta que se examinan, actualizan y aprueban.

Los dispositivos de acceso a la red funcionan como la capa de aplicación, como se muestra en la figura. Obligan a los clientes a consultar a un servidor RADIUS para la autenticación y autorización. El servidor RADIUS puede consultar otros dispositivos, como un servidor antivirus Trend Micro, y responder a los ejecutores de la red.

Componentes Cisco NAC

Los productos de Cisco Secure Access Control son parte de la solución Cisco◆ec basada en el dispositivo NAC. Cobec es un componente central de la arquitectura de redes sin fronteras seguras. En el enfoque de la tecnología de NAC Appliance, Cisco NAC Manager (NAM) es un servidor de políticas que funciona con Cisco NAC Server (NAS) para autenticar a los usuarios y evaluar sus dispositivos a través de conexiones LAN, inalámbricas o VPN, como se muestra en la figura. El acceso a la red y los recursos se basa en las credenciales del usuario y sus funciones en la organización, así como en el cumplimiento de las políticas de los dispositivos de punto final:

- **Cisco NAC Manager (NAM)** : Centro de administración y políticas para un entorno de implementación de NAC basado en dispositivos, Cisco NAC Manager define el acceso de usuario basado en roles y las políticas de seguridad de punto final.

- **Cisco NAC Server (NAS)** : evalúa y aplica el cumplimiento de la política de seguridad en un entorno de implementación NAC basado en dispositivos.

- **Cisco NAC Agent (NAA)** : un agente ligero opcional que se ejecuta en un dispositivo de punto final. Realiza una inspección profunda del perfil de seguridad del dispositivo mediante el análisis de la configuración del registro, los servicios y los archivos.

Estas son dos herramientas adicionales de cumplimiento de la política de cobro:

- **Servidor invitado de Cisco NAC** : administra el acceso a la red de invitados, incluido el aprovisionamiento, la notificación, la administración y el informe de todas las cuentas de usuarios invitados y las actividades de la red.

- **Cisco NAC profiler** : ayuda a implementar el control de acceso basado en políticas al proporcionar descubrimiento, perfiles, ubicación basada en políticas y monitoreo posterior a la conexión de todos los dispositivos de punto final.

Acceso a la red para invitados

Cisco NAC Guest Server proporciona la aplicación de políticas de invitados al dispositivo Cisco NAC o al controlador de LAN inalámbrica de Cisco, donde se aplican las políticas de invitados. Cisco NAC Guest Server, un componente de la solución Cisco◆ec, brinda soporte completo para el ciclo de vida del acceso de invitados, incluyendo aprovisionamiento, notificación, administración e informes.

Cisco NAC Guest Server proporciona la capacidad para que los patrocinadores, como los empleados de la empresa, creen cuentas de invitados. Los patrocinadores se autentican en el servidor invitado y se otorgan permisos en función de sus funciones. Los patrocinadores pueden obtener permisos basados en roles para crear cuentas, editar cuentas, suspender cuentas y ejecutar informes.

Hay tres formas de otorgar permisos de patrocinador para:

- Solo aquellas cuentas creadas por el patrocinador.

- Todas las cuentas

- No cuentas (es decir, no pueden cambiar ningún permiso)

Después de crear una cuenta de invitado, los invitados pueden iniciar sesión en la red con los detalles proporcionados por el patrocinador.

La creación de una cuenta de usuario en un servidor invitado de Cisco NAC se muestra en las Figuras 1 a 8.

Cisco NAC Profiler

Cisco NAC Profiler permite el descubrimiento dinámico, la identificación y el monitoreo de todos los puntos finales conectados a la red dentro de una red empresarial. Administra estos dispositivos de manera inteligente, según las políticas de seguridad definidas por el usuario.

Cuando se implementa como parte de una implementación más amplia de NAC, Cisco NAC Profiler facilita la implementación y la administración de los sistemas de Cisco NAC. Descubre y rastrea la ubicación y el tipo de todos los puntos finales conectados a la LAN, incluidos aquellos que no pueden autenticarse.

Cisco NAC Profiler permite a los administradores de seguridad:

- Simplifique la implementación de Cisco NAC automatizando la identificación y autenticación de dispositivos y facilitando las tareas administrativas.
- Facilite la implementación y la administración de la infraestructura basada en Cisco ACS 802.1X o las soluciones de superposición de Cisco NAC.
- Recopile información de perfiles de dispositivos de punto final y mantenga un inventario contextual en tiempo real de dispositivos en red.
- Monitoree y administre las anomalías de comportamiento de los dispositivos, como el intercambio de puertos, la falsificación de direcciones MAC y los cambios de perfil.
- Asegure todos los puntos finales propiedad de la empresa, incluidos los dispositivos sin autenticación, como impresoras y teléfonos IP.

Cisco NAC Profiler tiene dos componentes: el NAC Profiler Collector, que se muestra en las Figuras 1 y 4, y la aplicación NAC Profiler Server, que se muestra en las Figuras 2 y 3. Las Figuras 1 a 4 ilustran secuencialmente cómo el Cisco NAC Profiler recopila, agrega, filtra, y actualiza los datos del dispositivo.