

Control de Admisión a la Red Con Seguridad (NAC)



El control de admisión a la red (NAC), un conjunto de tecnologías y soluciones basadas en una iniciativa de la industria patrocinada por Cisco, utiliza la infraestructura de la red para hacer cumplir la política de seguridad en

todos los dispositivos que pretenden acceder a los recursos informáticos de la red, limitando así el daño causado por amenazas emergentes contra la seguridad. Los clientes que usan NAC tienen la capacidad de permitir que accedan a la red sólo dispositivos de punto terminal (por ejemplo computadoras, servidores y agendas PDA) confiables que cumplan con las políticas de seguridad y pueden limitar el acceso de los dispositivos que no las cumplen

Un buen sistema de control de acceso a la red (NAC, Network Admisión Control) garantiza que sólo los dispositivos seguros que cumplan con las normativas puedan conectarse a su red, y bloquea y repara aquellos dispositivos que no cumplen con las normas antes de permitirles el acceso. Mediante el uso de la sólida tecnología de Symantec, los asesores de Symantec proporcionan una completa solución que ofrece seguridad a los endpoints de la empresa

La tecnología NAC Appliance, basada en la línea de productos Cisco Clean Access, permite una rápida implementación con servicios incorporados de evaluación de puntos terminales, administración de políticas y servicios correctivos

La tecnología NAC Framework, a través del programa de control de admisión a la red de Cisco, integra una infraestructura de red inteligente con soluciones de más de 75 de los principales fabricantes de antivirus y otras soluciones de software de seguridad y gestión

<http://www.cisco.com>

La Seguridad Básica Que Un Usuario De PC Debe Saber

- Mantener Actualizados sus programas
 - No abrir correos que procedan de fuentes desconocidas
 - No seguir ningún vinculo que llegue por correo o mensajería instantánea
 - No ejecutar archivos que procedan de fuentes desconocidas
 - No descargarse por 2P2 archivos sospechosos
 - No conectar dispositivos móviles como llaves USB o PDA sin haberse asegurado antes de que no están infectados
 - Bloquear el equipo cuando no se esté en el puesto de trabajo
 - Evitar tener contraseñas a la vista
-
-