

# NAC visto como una solución interoperable

Cisco Systems propone una estrategia de control de admisión a la red adaptada a las necesidades del cliente, de forma que la empresa pueda invertir de manera gradual desde una instalación en la red de dispositivos NAC hasta un proyecto integral.

**E**l Control de Admisión en Red o *Network Admission Control* (NAC) de Cisco es un componente principal de la estrategia global de seguridad de Cisco denominada Redes de Auto-defensa o *Self-Defending Networks*. Su objetivo principal es la comprobación del estado de salud del equipo desde el que un usuario intenta acceder a la red, de forma que se permita el acceso sólo a los dispositivos "seguros" y se bloquee la entrada a aquellos equipos que no cumplan con los requisitos mínimos de protección exigidos por la política de seguridad corporativa. Los elementos de red y las

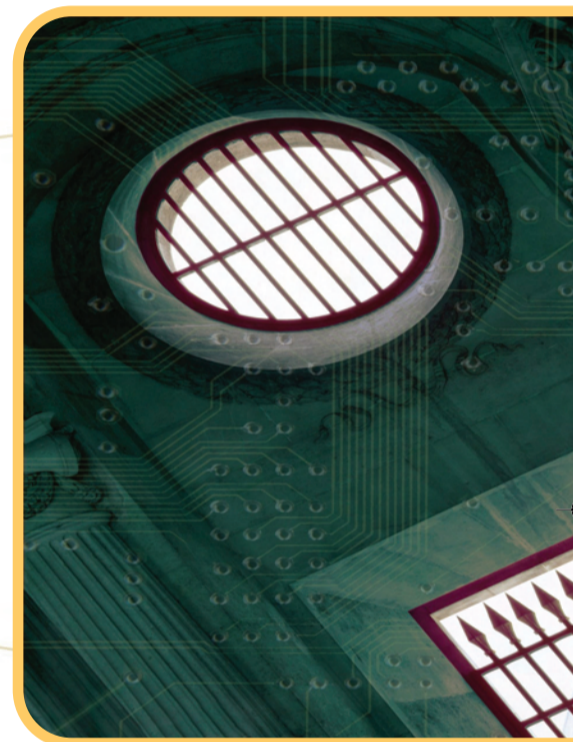
aplicaciones utilizadas para comprobar y garantizar el estado adecuado del dispositivo realizan una labor conjunta de protección de la infraestructura, permitiendo o restringiendo el acceso de los dispositivos en función de su identidad y nivel de protección.

La solución es aplicable a todos los métodos de acceso: red de área local, red inalámbrica, red de área extensa y accesos remotos ya que se ha desarrollado para los accesos a través de cualquier dispositivo de red: conmutadores, equipos Wi-Fi, routers y concentradores VPN respectivamente.

Cisco hizo su primer anuncio sobre el programa NAC en noviembre del 2003 y actualmente cuenta con la participación de más de 88 fabricantes que colaboran en dicho programa. El resultado obtenido hasta la fecha, como fruto de esta colaboración, permite ofrecer al usuario soluciones totalmente novedosas en el ámbito del control de acceso y aumentar enormemente las garantías de futuro de la solución. El programa NAC supone un hito sin precedentes en la colaboración entre fabricantes en los entornos de seguridad en red, aplicaciones antivirus, aplicaciones de remedio ante problemas, software cliente de seguridad y auditoría en red. Un claro ejemplo de la colaboración entre fabricantes es la propuesta de interoperabilidad entre la solución NAC de Cisco y la solución *Network Access Protection* (NAP) de Microsoft. Esta solución estará disponible a partir del lanzamiento al mercado del nuevo servidor Windows de Microsoft conocido como *Longhorn* y permitirá a los clientes aprovechar todas las prestaciones de la solución de control de admisión en red y la protección en los accesos desde equipos con software de Microsoft tanto en su modalidad de estación de trabajo como servidor.

## Propuesta flexible

Asimismo, Cisco ha iniciado el proceso de estandarización de los protocolos no



estándar desarrollados para mejorar la solución (se utilizan protocolos propietarios cuando no se dispone de un protocolo alternativo ya normalizado), manteniendo su apuesta clara por impulsar la incorporación de soluciones abiertas una vez que se defina el estándar de control de admisión.

La propuesta de control de admisión de Cisco es la más flexible del mercado ya que permite a los clientes invertir en la solución de forma gradual. El despliegue de la arquitectura NAC puede iniciarse mediante la instalación en la red de los dispositivos NAC y posteriormente convertirse en un proyecto integral de infraestructura NAC ya que Cisco garantiza esta migración.

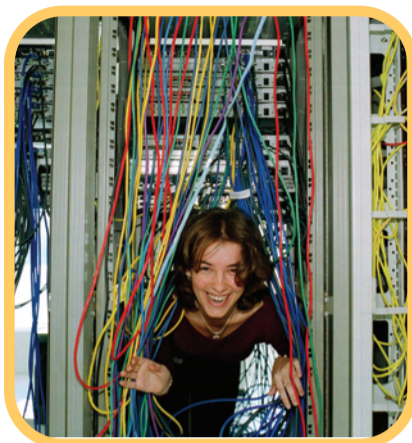
## Equipamiento Cisco

Sea cual sea el punto de entrada a la red, la solución de dispositivos NAC identifica un grupo de usuarios y equipos en red, desde empleados a proveedores e invita-

## Dispositivos para el Control de Admisión en Red

Los componentes de la solución de dispositivos NAC (*Clean Access Server*, *Clean Access Manager*, cliente *Clean Access* y servicios de suscripción) permiten un despliegue sencillo y rápido de la solución de control de acceso en redes pequeñas, redes con electrónica de red heterogénea o en partes de la red que requieran una intervención inmediata por ser más vulnerables ante posibles infecciones propagadas por los dispositivos que normalmente se conectan a ellas, por ejemplo segmentos de red dedicados a dar conectividad a dispositivos de terceras compañías. *Cisco Clean Manager* proporciona un interfaz de gestión basado en web para crear políticas de seguridad y gestionar los usuarios conectados. Adicionalmente puede hacer la función de servidor de autenticación *Proxy* hacia los servidores de autenticación del *back end*. Los administradores pueden utilizarlo para definir niveles de usuarios,

comprobación de cumplimiento de políticas y requisitos en situaciones de remedio. Este dispositivo gestiona y se comunica con el servidor *Cisco Clean Access* que es el dispositivo que se encarga de permitir o no el acceso desde la red. El servidor *Cisco Clean Access* realiza la comprobación de cumplimiento de políticas cuando los usuarios intentan acceder a la red. El agente *Cisco Clean Access* es opcional y cuando se instala en los dispositivos finales realiza una inspección exhaustiva del perfil de seguridad de la máquina mediante el análisis de la configuración de los registros, los servicios y los ficheros. Tras dicho análisis, el agente determina que acción de remedio es necesaria y arranca la versión adecuada de antivirus así como otras aplicaciones de seguridad como *Cisco Security Agent*. Como el agente se descarga y ejecuta fácilmente, se puede instalar en los equipos no gestionados bajo demanda.



El programa NAC supone un hito sin precedentes en la colaboración entre fabricantes en los entornos de seguridad en red, aplicaciones antivirus, aplicaciones de remedio ante problemas, software cliente de seguridad y auditoría en red

## Ventajas principales de la solución NAC

- Los dispositivos NAC constituyen la solución que cuenta con un mayor número de referencias en la actualidad. La amplia experiencia de Cisco en estos productos reduce los tiempos de implementación a unos días.
- Tanto los dispositivos NAC como la solución de infraestructura NAC pueden adquirirse ya. Además, Cisco garantiza la migración desde una solución basada en dispositivos a una solución integral o de infraestructura.
- La solución NAC permite un control exhaustivo de cualquier intento de acceso ya que Cisco puede modificar el código ejecutado en los equipos de red, sea cual sea el método de acceso utilizado por el usuario (a través de conmutadores, routers, equipos Wi-Fi, concentradores VPN, etc.). Además, es

la única solución aplicable a entornos con tecnología punta como la telefonía IP.

- La solución NAC ofrece un cien por cien de compatibilidad entre dispositivos y *hosts* por lo que no se requiere la instalación de múltiples servidores.
- NAC se aplica a dispositivos gestionados, no gestionados e invitados a la red y es la única solución que permite la integración del control de identidad y estado de cumplimiento de la normativa de seguridad en los equipos finales.
- Con NAC, las decisiones sobre qué acciones realizar según el estado de cumplimiento o no de la política de seguridad se realizan desde la red y no desde el propio dispositivo final. De esta forma se evitan los fraudes asocia-

dos a una interpretación errónea (accidental o premeditada) sobre el estado de cumplimiento de las políticas en el equipo que intenta acceder a la red.

- Cisco es el único fabricante que dispone de una solución basada en dispositivos y una solución de infraestructura NAC y, por tanto, es el único capaz de ofrecer protección de la inversión a aquellos clientes que opten por un despliegue inicial de dispositivos NAC y una migración posterior a la solución de infraestructura.
- Cisco puede ofrecer servicios avanzados de consultoría y despliegue de soluciones NAC integrando la solución NAC con la infraestructura de red existente, la política de admisión en red, la seguridad de los extremos de la red y las tecnologías antivirus.

dos a una interpretación errónea (accidental o premeditada) sobre el estado de cumplimiento de las políticas en el equipo que intenta acceder a la red.

dos con diversos sistemas operativos (Windows, Macintosh, Linux), PDAs, impresoras y teléfonos IP. Los dispositivos NAC comprueban el cumplimiento de las políticas de seguridad de la empresa y conceden los derechos correspondientes de acceso a la red. Los equipos que no cumplan las políticas de seguridad corporativas quedan bloqueados y en cuarentena. Las actualizaciones de vulnerabilidad se administran automáticamente para el sistema operativo utilizado así como el software de antivirus y *antispyware*.

Por otra parte, los dispositivos NAC proporcionan cómodas funciones de registro para clientes VPN, clientes inalámbricos y dominios de Directorio Activo de Windows. Esta funcionalidad, junto con las innumerables capacidades de gestión y configuración existentes, proporciona simplificación de las operaciones y mejora la productividad de los empleados.

Además de colaborar con numerosos productos de seguridad de Cisco como los puntos de acceso inalámbricos, *Cisco Security Agent* para protección en los extremos y *Cisco Adaptive Security Appliance (ASA)*, el dispositivo NAC interopera con sistemas de otros proveedores de equipos de redes, por lo que puede aplicarse a una infraestructura de red heterogénea.

La solución de infraestructura NAC va dirigida a empresas cuya red esté basada totalmente en equipamiento Cisco, clientes especialmente preocupados por garantizar la interoperabilidad entre soluciones de seguridad multifabricante, clientes que precisen una solución de control de admisión compatible con el protocolo de gestión de identidades de usuarios en red 802.1x o clientes que quieran utilizar el servidor ACS como servidor donde se centralicen las políticas de seguridad. En el instante en el que los dispositivos de red detectan el

intento de acceso desde un dispositivo cliente a la red, contactan con el servidor de autenticación, denominado *Cisco Access Control Server* o ACS que, a su vez, y de forma opcional, puede contactar con el servidor de antivirus, el servidor de gestión de políticas de seguridad, el servidor de auditoría, etc. Así comprueban si el nuevo usuario y el dispositivo desde el que se conecta cumplen con la política de seguridad definida en la empresa. Cisco distribuye de forma gratuita el software cliente denominado *Cisco Trust Agent* que se instala, opcionalmente, en los ordenadores en los que se quiere activar el control de admisión. Si los dispositivos no tienen instalado este software cliente, se produce la colaboración del servidor de autenticación con las soluciones de auditoría que se basan típicamente en la utilización de herramientas de rastreo para comprobar el estado del ordenador antes de emitir un informe sobre su estado de salud.

## Más información

Cisco Systems: [www.cisco.com](http://www.cisco.com)