NAC, una solución REAL

NAC, a REAL solution

Samuel Bonete

Resumen

La implementación de sistemas de control de acceso en los entornos de Seguridad Física son habituales. Análogamente, el control de acceso en la Seguridad Lógica debería de ser visto con la misma naturalidad; de forma que el usuario se acostumbrará a ser detectado cuando accede a la red, autenticado, evaluado y autorizado según su nivel de permisos. Actualmente la tecnología pone a nuestra disposición las herramientas necesarias para realizar estos controles tanto en las fases de pre-conexión cómo de post-conexión. Por lo tanto, sólo nos hace falta conocer en detalle que nos aportan estas herramientas, así como la forma correcta de enfocar el despliegue de las mismas.

Palabras clave: control de acceso a la red, detección, autenticación, evaluación, remediación, autorización, 802.1x, políticas de seguridad, virtualización, monitorización, correlación de eventos, cumplimiento de normativa.

Summary

Implementing access control systems in Physical Security environments is common. Likewise, access control in Logical Security should be viewed just as naturally. The user must get used to being detected upon accessing the network, authenticated, evaluated and authorised according to the level of permissions. Technology today offers us the tools needed to carry out these controls, both in the pre-connection and the post-connection phases. All that is left, therefore, is to determine in detail what these tools have to offer and the right way to focus their implementation.

Keywords: Network access control, detection, authentication, evaluation, remediating, authorisation, 802.1x, security policies, virtualisation, monitoring, event correlation, compliance with standards.

Todos nosotros estamos acostumbrados a tener que identificarnos y ser escaneados múltiples veces a lo largo del día

1. Introducción

Todos nosotros estamos acostumbrados a tener que identificarnos y ser escaneados múltiples veces a lo largo del día. De hecho, antes de llegar a este evento muchos cogimos el avión. En el Aeropuerto nos hicieron identificarnos mostrando nuestro DNI y tarjeta de embarque, la autenticación fue satisfactoria. Esa autenticación habría bastado años atrás para volar, pero a día de hoy es necesario realizar también una validación de la integridad, de forma que nos aseguremos antes de permitirnos volar que no somos una amenaza. Por ello, el vigilante nos inspecciona el equipaje, hace que depositemos líquidos y otros posibles elementos peligrosos en contenedor e, incluso en algunas ocasiones, nos realiza un cacheo, o nos pide que nos quitemos los zapatos.

Las funciones de control de post acceso aplican monotorización, contención y remedio

Una vez dentro de la zona de embarque, cientos de cámaras, policías de paisano y otros agentes revolotean sobre nosotros monitorizando nuestros movimientos, con el fin de detectar alguna posible amenaza y registrar cualquier evidencia que pueda ser utilizada posteriormente.

Si nos fijamos con detalle, podremos identificar en esta descripción las cinco piezas claves que debe de tener cualquier **Sistema de Control de Acceso:**

Detección: Se detecta que una persona intenta conseguir acceso a la zona de embarque. Esta persona es interceptada en espera de…

Autenticación: El pasajero se autentica mostrando su tarjeta de embarque y DNI.

Evaluación: El pasajero es evaluado conforme a las políticas internacionales de seguridad en materia de aviación civil. Su equipaje es inspeccionado, se mira que no posea elementos peligrosos, etc.

Remedio: En caso de que la evaluación denotara que el pasajero es portador de algún elemento peligroso, es requerido a abandonarlo antes de entrar al área restringida.

Autorización: Una vez validado su acceso el pasajero puede entrar a la zona de embarque y moverse a unas zonas (p.e. salas VIP) o no en función de su perfil.

Pero, como comentábamos, el sistema no termina ahí… existe una monitorización post conexión sobre el viajero una vez dentro del área de embarque. Esta monitorización permite contener a aquel viajero que una vez dentro presente una amenaza. Detectamos pues varias funciones de control de post acceso que aplican:

Monitorización: Se supervisa la actividad de los viajeros con las medidas de detección de intrusiones que aplican en cada momento. El fin de esta supervisión es detectar anomalías o comportamientos sospechosos.
Contención: En el caso de detectar un viajero sospechoso se envía un grupo de vigilantes para detener al individuo.
Remedio: En caso de ser necesario, se corrige la actitud, y el viajero sigue circulando con normalidad.
Y claro está, a nadie ya le sorprende estas actuaciones que estamos describiendo. Las tomamos como medidas técnicas, en mayor o menor medida necesarias, para garantizar la seguridad e integridad dentro del entorno del aeropuerto.

En el ámbito de la Seguridad Informática, medidas técnicas similares son una realidad disponible para los responsables de seguridad y comunicaciones. Las medidas han ido evolucionando en los últimos años de forma que el Control de Acceso a la Red (Network Access Control - NAC) se ha convertido en una solución REAL, que se puede implementar y puede mitigar las brechas de seguridad de nuestra red.

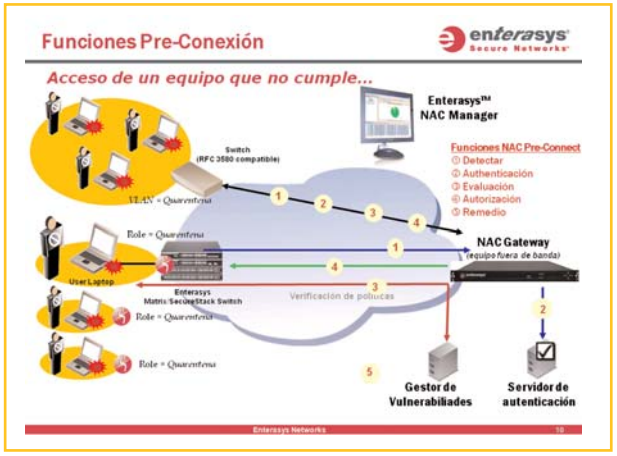
Las soluciones NAC de los sistemas de la información son similares a las anteriormente descritas para un aeropuerto o un edificio público. Su fundamento es tanto el control pre conexión como el post conexión. A grandes rasgos, los personajes son los mismos pero con actores diferentes.

Dicho esto, pasamos a presentar los actores típicos de un escenario NAC:

Las soluciones NAC de los sistemas de la información son similares a las anteriormente descritas para un aeropuerto o un edificio público

2. Actores de un escenario NAC

En primer lugar, un usuario desea acceder a su red corporativa. Para ello, conecta el equipo a la toma de red y lo enciende. La electrónica de red **(1) detecta** que existe un nuevo usuario intentando acceder a la red y realiza las funciones de **(2) autenticación**, actuando como intermediario en la validación de la identidad del usuario o del sistema que se conecta. La distinta naturaleza de los entornos en los que se puede aplicar NAC, obliga a que esta autenticación se pueda realizar de varias formas diferentes. Por ello, debemos poder autenticar el dispositivo final por su dirección MAC, podríamos necesitar realizar la autenticación mediante el uso de 802.1x con las credenciales del usuario (incluso aquellas que usó para intentar hacer login en el dominio de Microsoft), o bien podemos presentar al usuario un portal web en el que realizar la autenticación de forma interactiva.



Una vez validada la identidad del usuario final contra el servidor de autenticación de nuestro entorno, ya estamos en disposición de conocer qué tipo de **(3) evaluación** debemos aplicar al dispositivo que pretende acceder a la red. Esta evaluación deberá ser parametrizable en función tanto del dispositivo final (no podemos comparar el estado de salud de una cámara IP con el de un teléfono IP) como del usuario que intenta el acceso. Son las evaluaciones y el decidir qué y cómo evaluar durante el control de acceso uno de los temas más ásperos a la hora de poner en marcha un proyecto de NAC. Por ello, abordaremos este punto en detalle en las páginas siguientes.

Como norma general, verificaremos que el equipo remoto cumpla la política seguridad de nuestra corporación, de forma que nos aseguremos de que la entrada del equipo en la red no suponga un riesgo al resto de usuarios. Supongamos que el equipo en cuestión suspende la evaluación; entonces,

Verificaremos que el equipo remoto cumpla la política seguridad de nuestra corporación, de forma que nos aseguremos de que la entrada del equipo en la red no suponga un riesgo al resto de usuarios

a la vista de que su estado puede comprometer otros sistemas de la corporación, es conveniente aislarle. El aislamiento a aplicar debería ir más allá de situar el equipo en una red de cuarentena, siendo muy recomendable aplicar políticas de seguridad en el puerto en que conecta el usuario, a fin de controlar el uso de recursos que éste puede hacer.

En el caso de que existan varios dispositivos tras un único puerto de conmutación, es conveniente poder identificar a cada uno de esos dispositivos de forma separada y aplicar políticas acordes a cada uno de ellos. Supongamos el caso de un teléfono IP y un usuario tras el teléfono, autenticaremos al teléfono en base a su dirección MAC y aplicaremos una política generosa a nivel de calidad de servicio. Al usuario, que accede por el mismo puerto físico al switch, le aplicaremos autenticación 802.1x y políticas (protocolos permitidos, puertos de destino, calidad de servicio, etc.) en función de la evaluación que hagamos de su equipo.

Para que el usuario que hemos aislado sea capaz de conseguir acceso normal a la red, deberá corregir las deficiencias detectadas en su equipo. Para ello, la solución de NAC deberá contar con herramientas flexibles de **(4) remediación.** El remedio pasa por informar al usuario sobre cuál ha sido el motivo que le ha llevado a ser aislado con mediante una política de cuarentena. Así mismo, ha de contar con las herramientas necesarias que faciliten al usuario la información correspondiente para redirigir la situación anómala inicial a una situación de cumplimiento con las políticas de seguridad de la corporación. Esta remediación se puede hacer empleando portales web cautivos y redirigiendo en la infraestructura de red el tráfico web de los usuarios en cuarentena hacia los mismos.

Es necesario continuar prestando atención al usuario tras la conexión

Por último, una vez se han subsanado los motivos que llevaron al usuario a una política de cuarentena, se procede a **(5) autorizar** el acceso a la red con el perfil correspondiente al usuario. Este acceso se garantiza mediante la aplicación de las políticas de seguridad correspondientes, que garantizarán los niveles de calidad de servicio y servicios remotos alcanzables para cada usuario autenticado.

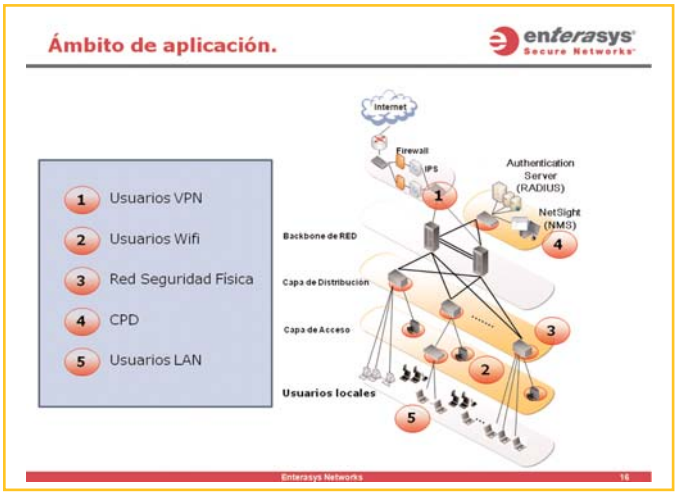
Siguiendo con el símil inicial, el usuario ya estaría dentro del área de embarque. Pero como comentábamos al principio, es necesario continuar **monitorizando** la actividad del usuario con el objetivo de detectar anomalías en su comportamiento. No vale con verificar pre-conexión, es necesario continuar prestando atención al usuario tras la conexión. Por ello, los sistemas de detección y prevención de intrusiones de la red, así como otros elementos de seguridad (cortafuegos, concentradoras vpn, servidores radius, etc.) pueden darnos información valiosa sobre la actividad del usuario. Esta información, proveniente de fuentes distintas, puede ser **correlacionada** en una herramienta diseñada para almacenar logs y generar alarmas de seguridad. Las herramientas de correlación de eventos, como el **Dragon Security Command Console (DSCC)** deben ser capaces de reducir el número de eventos que llegan a los departamentos de operaciones así como de actuar como contenedores de la información de cara a generar reportes o buscar evidencias cuando los departamentos de seguridad lo consideren necesario.

Nuestras experiencias en la implantación de soluciones NAC nos ha mostrado que muchos centros acometen el despliegue aplicando el control de acceso por bloques o diferentes áreas

Las alarmas generas por el **DSCC** podrán ser utilizadas para **contener** al usuario malicioso. De tal forma, una vez detectada una actividad anómala o de peligrosa para la red, se deberá proceder a localizar de forma automática el puerto de la electrónica donde está conectado ese usuario y se procederá a aplicar una política de seguridad al mismo, dándose así lugar a la contención comentada anteriormente. Esta contención deberá garantizar la trazabilidad del usuario, de forma que si éste cambia de puerto, la política siga aplicando al nuevo puerto en el que conecte. En caso de conectar a un puerto en el que ya hubiera más usuarios, la política deberá aplicar a él y sólo a él, no afectando el rendimiento del resto de usuarios.

Como se ha podido leer en los párrafos anteriores, la tecnología disponible hace que implementar NAC sea una realidad más que una posibilidad. El éxito está garantizado si realizamos el despliegue teniendo en cuenta los siguientes factores: **ámbito, evaluación, políticas a aplicar y monitorización.**

3. Ámbito



Nuestras experiencias en la implantación de soluciones NAC nos ha mostrado que muchos centros acometen el despliegue aplicando el control de acceso por bloques o diferentes áreas. Así pues, no es de extrañar que la implantación se aborde en diferentes fases actuando primero sobre los equipos que puedan presentar una amenaza mayor y dejando en último lugar las LANes internas. Un despliegue por fases podría ser acometido de la siguiente forma:

- **Usuarios VPN:** En primer lugar, aplicar el control de acceso a los usuarios que vengan desde ubicaciones remotas. Estos usuarios suponen siempre una amenaza dado que están fuera de nuestro control, ya sean teletrabajadores VPN o usuarios que lleguen vía una VPN Lan a Lan. Introduciendo un dispositivo en línea podremos verificar el estado del equipo desde el que el usuario remoto intenta ganar acceso a nuestra red, autenticando el usuario, evaluando la integridad del dispositivo, autorizando el acceso a sólo ciertos recursos y supervisando las actuaciones del usuario dentro de la red.
- En segundo lugar, podemos aplicar el control de acceso a los **usuarios Wifi** de la red. De igual forma que para el caso de usuarios VPN, se hará pasar su tráfico a través de un dispositivo NAC en línea.
- Otro lugar idóneo para los primeros despliegues son redes con pocas variaciones pero con elevadas exigencias en materia de seguridad, como pueden ser las redes dedicadas a los dispositivos de control de la seguridad física. Aplicando autenticación y políticas de seguridad a la electrónica que da conectividad a éstos dispositivos, mitigaremos el riesgo de que un usuario no autorizado conecte a esta red o que un dispositivo comportándose de forma anómala pueda afectar al resto de elementos de la red de **seguridad física**.
- Los **centros de procesos de datos** son también un buen lugar dónde aplicar las soluciones de Control de Acceso. Aplicando políticas basadas en MAC, y aplicando más de una política distinta dentro de un mismo puerto o una agregación de puertos, estaremos controlando el acceso a la red de diferentes máquinas virtuales emplazadas sobre un mismo servidor físico, pudiendo hablar de dominios de virtualización dónde se realiza el control de acceso.
- Por último, pero no necesariamente en último lugar, afrontar el control de acceso a la red dentro de los propios **usuarios LAN** de la corporación. La experiencia que hayamos ganado en los despliegues anteriores, tanto el personal de los departamentos de IT como los usuarios locales, facilitarán las labores de despliegue.

La experiencia que hayamos ganado en los despliegues anteriores, tanto el personal de los departamentos de IT como los usuarios locales, facilitarán las labores de despliegue

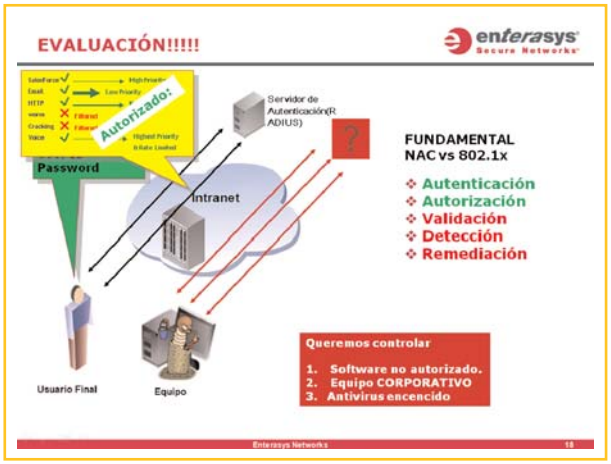
4. Evaluación

Si hay un factor realmente diferenciador dentro de NAC es la evaluación. La autenticación y asignación de una u otra política en función de la identificación del usuario era una realidad tiempo atrás. El problema radica en el decir ser alguien no debe de ser condición suficiente para garantizar el acceso, la integridad del equipo debe de ser evaluada. Esta evaluación de la integridad y la asistencia

La evaluación es un factor realmente diferenciador dentro de NAC

en la remediación es el factor diferenciador entre 802.1x y NAC.

La gráfica muestra una situación en la que tras una autenticación exitosa hemos facilitado el acceso a la red de gestión a un administrador que está usando un equipo comprometido. Como vemos la autenticación ha de ser condición necesaria pero no suficiente para garantizar el estado a la red.



A la hora de evaluar, hay que pensar cómo se quiere acometer esta acción

A la hora de evaluar, hay que pensar cómo se quiere acometer esta acción. Hay dos aproximaciones fundamentales: el uso de agentes o el uso de la red. Con el uso de agentes la información se obtiene directamente desde el equipo que se está evaluando. Es importante la capacidad de integración con los agentes nativos del SSOO (p.e. NAP de Microsoft). Estos agentes son capaces de controlar el estado de las aplicaciones, procesos y puertos que el usuario está usando en el equipo y notificarlos a un tercero para la toma de decisiones. El otro acercamiento está basado en el la realización de escaneos de vulnerabilidades al equipo que intenta el acceso. Ya se utilice una técnica u otra, una buena aproximación sería controlar la presencia de un software antivirus en el equipo, unas políticas de firewall mínimas, tener el sistema operativo actualizado y la no presencia de software malicioso en el host.

5. Conclusiones

Recopilando la información mostrada a lo largo de este artículo, a la hora de desplegar una solución de NAC deberemos fijarnos en que ésta cumpla tanto los requisitos de pre conexión (Detección, Autenticación, Evaluación, Remedio y Autorización) como en que sea capaz de monitorizar la actividad post conexión y contener a los usuarios que no tienen una conducta acorde a las políticas de seguridad corporativas.

NAC es una solución REAL que puede ser de utilidad en múltiples entornos en los que se desee controlar el acceso a la red que realizan los usuarios

De cara a realizar un despliegue de NAC, una buena aproximación puede ser empezar a trabajar con los segmentos de la red que puedan presentar mayor riesgo (tales como accesos remotos de usuarios VPN, segmentos Lan to Lan o redes wifi). Estas experiencias nos permitirán detectar posibles complicaciones y reducir los errores del despliegue de los usuarios de la red interna. Es también interesante contemplar las posibilidades que NAC nos ofrece en entornos de máquinas virtuales en los que podemos tener una agregación de enlaces desde los servidores físicos que corren diferentes máquinas virtuales a las que queremos aplicar diferentes políticas de seguridad y a las que queremos ser capaces de detectar de forma automática según se van moviendo por el datacenter.

Es también importante contar con la implicación de los responsables de seguridad de la información de corporación en el momento en que se definan los parámetros a evaluar y las acciones a tomar con los usuarios que no cumplan la política de seguridad. Este respaldo continuo permitirá aplicar las políticas de seguridad con confianza por parte del personal de seguridad.

Por último, NAC es una solución REAL que puede ser de utilidad en múltiples entornos en los que se desee controlar el acceso a la red que realizan los usuarios. La solución existe, la necesidad también.

Samuel Bonete

Consultor preventa de Seguridad para el Sur de Emea de ENTERASYS