

ForeScout: acceso NAC de última generación

En la actualidad, ForeScout es considerada una tecnología NAC de referencia, siendo su finalidad expresa proporcionar a los usuarios acceso a los recursos de la red corporativa, dónde, cómo y cuándo sea necesario sin comprometer la seguridad.

En los últimos años una de las mayores preocupaciones de las organizaciones es controlar el acceso a sus redes, es decir, quién es el usuario que se está conectando, cómo se está conectando, cuándo se está conectando, desde dónde se está conectando y qué tipo de dispositivo está usando.

Estas preguntas han ido creando en los departamentos de seguridad de las corporaciones cada vez mayor inquietud debido fundamentalmente a que la movilidad de los usuarios es cada vez mayor, el tipo de dispositivos que se utilizan para conectarse ha crecido exponencialmente, y el acceso puede ser desde cualquier sitio y por cualquier medio.

Así mismo las amenazas a las organizaciones se dan muchas veces por la conexión de un dispositivo que no cumple con una serie de normativas de seguridad, es decir, que no tiene los parches de seguridad instalados o actualizados y tiene aplicaciones potencialmente peligrosas instaladas que pueden provocar graves problemas a las corporaciones una vez que estos equipos entran en la red corporativa, así como usuarios invitados que se conectan a la red y sobre los cuales no se tiene control de sus dispositivos.

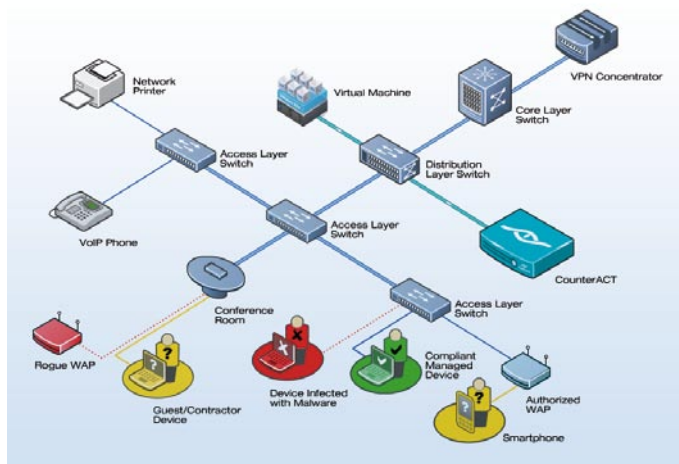
El mercado de la seguridad IT desde hace unos años ha ido perfilando una tecnología específica para dar respuestas a estos problemas, lo que conocemos como NAC. Muchos fabricantes han incorporado dentro de los dispositivos de seguridad que tenían funcionalidades de NAC y otros han nacido como puros fabricantes NAC. En estos años hemos visto como este nicho de seguridad ha evolucionado y se ha consolidado; muchos de los fabricantes iniciales que nacieron como pura tecnología NAC han desaparecido, otros se han quedado estancados en sectores y mercados verticales, y otros lo han incluido como una funcionalidad más.

Hay que destacar que una tecnología NAC no sustituye a otros elementos activos de seguridad de la red sino que se complementa con ellos para dar una respuesta pro-activa a cualquier amenaza aislando los elementos peligrosos en zonas de cuarentena donde se les obligará a tomar las medidas correctivas necesarias para volverles a dejar conectarse a la corporación automáticamente.

Uno de los actores que se considera líder de la tecnología NAC es ForeScout, siendo su finalidad expresa la de proporcionar a los usuarios acceso a los recursos de la red corporativa, dónde, cómo y cuándo

sea necesario, sin comprometer la seguridad. En la actualidad tiene una presencia muy considerable en todos los sectores, organizaciones gubernamentales y, así mismo, ha llevado a cabo grandes despliegues en empresas del Fortune 1000.

Conviene precisar que uno de los principales problemas al integrar una tecnología NAC en una organización, es que esta ya dispone de un parque de equipamiento multifabricante. En este sentido,



ForeScout es interoperable con cualquier fabricante, así como dispositivo IP; así mismo, muchos sistemas NAC en el mercado necesitan que los componentes utilicen 802.1x, en tanto que en ForeScout se permite su integración en arquitecturas mixtas; es decir: puede haber dispositivos que soporten 802.1x y otros no, lo que da una gran flexibilidad a la hora de implementar dicha tecnología.

ForeScout controla y monitoriza dispositivos IP, con lo cual su licenciamiento no se realiza por los usuarios que hay en la organizaciones, sino por dispositivos IP concurrentes que estén conectados desde cualquier medio, entendiendo como equipo IP no solo un ordenador, sino también un teléfono IP, un punto de acceso inalámbrico, una impresora, una cámara de video, cortafuegos, switch, router, etc.

ForeScout permite que cuando un usuario se conecta a la organización desde cualquier dispositivo se analice cualquier potencial amenaza que tenga ese equipo antes de permitirle el acceso, comprobando si tiene los parches de seguridad adecuados o cumple con la normativa de aplicaciones corporativas en caso de que fuera necesario; si esto no es así se le redirecciona a un portal cautivo donde se notifica el problema y se le proporcionan las acciones correctivas a los mismos; una vez solventadas dichas amenazas, se le da acceso a la

red. Una diferencia fundamental con ForeScout es que el análisis de dichas amenazas en los equipos no requiere la instalación de un agente en el mismo (puede funcionar con agente o sin agente).

Una vez que se ha dado acceso al usuario/equipo a la organización, se le sigue monitorizando y analizando, de tal manera que si cualquier componente de seguridad de la red que interopera con ForeScout detecta anomalías en los escaneos periódicos de los dispositivos, el usuario instala software no autorizado o se detecta una amenaza, se toman medidas correctoras automáticamente para aislar dicho equipo.

Igualmente, aunque no es la función propia de un dispositivo NAC, ForeScout permite inventariar todo el equipamiento de una organización, así como el software que se tiene instalado y los servicios que se están ejecutando en todos los equipos, con lo cual se podría detectar que un usuario está ejecutando un programa P2P y tomarse medidas correctoras desde la consola, notificando al usuario para que lo desinstale o 'matar' dicha aplicación desde ForeScout, incluso, aislar al equipo en una VLAN de cuarentena.

ForeScout se suministra como *appliance* físico (CounterACT para 100, 500, 1000, 2500 y 4000 dispositivos IP) o en versión virtualizada, teniendo una gran escalabilidad que permite satisfacer las necesidades desde pequeñas organizaciones hasta corporaciones globales que requieren control de acceso de múltiples ubicaciones; adicionalmente, se dispone del Counter ACT Enterprise Manager cuando se requiere controlar varios CounterACT, pudiendo soportar hasta 250.000 dispositivos.

Una de las funcionalidades destacables de ForeScout es el control en tiempo real de los dispositivos, su capacidad de funcionar sin agente y la monitorización dinámica de los endpoints; también permite poder dar acceso a los usuarios externos de la corporación de manera segura automatizando su registro, autenticación y cumplimiento de normativas de seguridad.

Otras de las características fundamentales de ForeScout es que se instala fuera de línea, realizándose con *portmirroring* o utilizando un TAP; es decir, que no es intrusivo en la red y no requiere un cambio de arquitectura. Una vez conectado en muy poco tiempo detecta todos los dispositivos IP instalados con sus características (tipo, modelo, sistema operativo, aplicaciones instaladas, parches de seguridad, antivirus, etc.). Por otra parte, es capaz de detectar dispositivos USB conectados y de qué tipo son, pudiendo bloquear los mismos o aislar el equipo hasta que dicho dispositivo no sea conectado. ■

ROBERTO MARTÍNEZ
 Director Técnico
INGECOM
 rmartinez@ingecom.net