NAC Inverso, un esquema optimizado de acceso a Internet

Nac Inverso, an optimised Internet access scheme

José Carlos González

Resumen

Dentro de las instituciones académicas existe una problemática muy concreta sobre al acceso a Internet para los usuarios internos. Llegar a un equilibrio entre las necesidades de los usuarios en el uso de los recursos de Internet y la seguridad de la red se complica cada día más. Políticas muy restrictivas evitan que los investigadores puedan desarrollar correctamente su trabajo, y políticas muy permisivas originan un auténtico quebradero de cabeza para los responsables TIC de las instituciones. La movilidad, la accesibilidad y el trabajo en la "nube" representan un cambio en el planteamiento de la seguridad.

Palabras clave: NAC, Internet, seguridad.

Summary

Within academic institutions there is a very specific problem relating to Internet access for internal users. Striking a balance between the needs of users using Internet resources and network security is becoming increasingly complicated. Highly restrictive policies prevent researchers from carrying out their work correctly and highly permissive policies are a real headache for the institutions' ICT managers. Mobility, accessibility and "cloud" work represent a change in approach to security.

Keywords: NAC, Internet, security.

La movilidad, la accesibilidad y el trabajo en la "nube" representan un cambio en el planteamiento de la seguridad

1. Introducción

Los administradores de la seguridad y la accesibilidad en las instituciones se ven cada día envueltos en continuas "peleas" por dar al usuario el servicio demandado sin poner en peligro las infraestructuras y recursos TIC internos. Los usuarios demandan un acceso libre a Internet culpando continuamente a los administradores de que no pueden realizar correctamente sus tareas. La institución aporta un parque importante de ordenadores (6.000 equipos) interconectados con redes de alta velocidad disponibles para Virus, Troyanos y Botnets que ponen continuamente en peligro su seguridad. La gestión de reglas en los firewalls degenera con una facilidad espantosa llegando en algunos momentos a hacerse una tarea realmente peligrosa y engorrosa. Todo esto unido se suma a una difícil identificación de los usuarios y las fuentes de ataques debido a lo heterogéneo y disperso de las infraestructuras de comunicaciones.asdf

La gestión de reglas en los firewalls degenera llegando a hacerse una tarea realmente peligrosa y engorrosa

2. Los flujos de información

Los usuarios y recursos se agrupan en 6 zonas de seguridad: servidores, usuarios rojos (profesores y alumnos), usuarios azules (gestión universitaria), usuarios wifi, usuarios vpn y usuarios de internet. Aparecen servicios y servidores en zonas mixtas como profesores que montan servicios en sus departamentos, recursos de internet que tienen que estar accesibles a todos, etc. El aumento en los flujos y combinaciones hace que la política de los sistemas firewall se parezca cada vez más a un "PERMIT ANY ANY", pues el tratamiento de cada uno de forma individualizada es imposible.

FIGURA 1

ºAl final los sistemas o barreras firewall se acaban convirtiendo en loggers de información que nos permitan tener algún dato más cuando se produce un ataque o se explota alguna vulnerabilidad. Es en este momento cuando el almacenamiento de los logs empieza a ser un problema y su tratamiento de una forma adecuada otro aún mayor.

3. Aproximación básica

Atacando el problema por partes se pueden arreglar bastantes cosas con un par de elementos básicos de seguridad. Para los usuarios externos que demandan recursos internos de la ULL se ha instalado un VPN-SSL de Juniper. El control de vulnerabilidades básicas se hace mediante un ISG/IDP en la entrada a las distintas zonas de seguridad. Para que la gestión de las configuraciones y seguimiento de los logs se una el Netscreen System Manager. Para seguir la movilidad y validación de los usuarios Wifi se ha implantado un Infranet Controler. Cubiertos estos aspectos queda pendiente como solucionar el acceso a recursos de Internet y a los recursos institucionales de una forma controlada y segura.

Las barreras firewall se acaban convirtiendo en loggers de información

4. NAC Inverso, una aproximación más versátil

La idea parte de considerar a Internet y los recursos existentes en Internet como un recurso más de nuestra institución al que los usuarios quieren conectarse. En ese caso parece que el NAC podría funcionar también para regular el acceso a los recursos de Internet. Al unificar este tipo de seguridad apareció también la idea de usar el NAC para las redes cableadas cuando intentan acceder a recursos de Internet y a recursos Institucionales.

FIGURA 2

El NAC podría funcionar para regular el acceso a los recursos de Internet

Una vez implementada la solución se ha de empezar a delegar la gestión de la seguridad en el NAC y el firewall pasa a ser lo que se denomina un "enforcer de seguridad", mientras que toda la lógica y diseño de la seguridad se descarga en el NAC.

Otra de las ventajas de este sistema está en el dinamismo que ofrece. Muchas veces, al ver las reglas del firewall que autorizan cosas, se detecta que durante muchas horas del día hay un gran número de reglas que no se utilizan pero que si intervienen en cargar más el firewall, consumir memoria, ocupar CPU. Al final el análisis de los paquetes pasa por un montón de reglas previas que en muchos instantes no tienen sentido. Al descargar la gestión de la seguridad en el NAC se muestra al usuario un menú de servicios de conexión. El usuario indica en cada sesión para que desea usar la "red" y el resto de reglas que estarían normalmente en el firewall nunca aparecerían.

Cuando una barrera, o doble barrera se coloca en el centro de todos los flujos de información, tiene una

principal problemática. Hay que replicar muchas veces los permisos para los distintos orígenes y destinos de la comunicación para lograr la movilidad de los usuarios. Esta es la forma manual de dar la sensación al usuario de la independencia del origen de la comunicación en el acceso a los recursos. Al basar ahora la seguridad y la política de seguridad en el NAC, es este el encargado de colocar de forma dinámica las reglas en el firewall en función del flujo que se está usando en cada momento sin necesidad de replicar su configuración.

5. Implementación, experiencia final al usuario

Una vez realizada la implantación e integración de toda la solución, la experiencia final al usuario queda de la siguiente forma:

1. El usuario se valida para acceder a la red.
2. Al validarse, el sistema sabe qué perfil tiene y en función de ese perfil le muestra los recursos y servicios que tendrá disponibles.
3. El usuario selecciona el servicio deseado.
4. El NAC inserta dinámicamente las reglas necesarias en el firewall para que ese servicio esté disponible en el flujo solicitado.
5. El propio navegador del usuario, que se ha usado para la validación en la red, será el encargado de mantener la sesión del usuario y garantizar su continuidad.
6. Una vez acabado, al cerrar el navegador, se eliminan las reglas dinámicas del firewall.

Al basar la política de seguridad en el NAC, éste se encarga de colocar las reglas en el firewall

6. La reducción drástica de las reglas estáticas en el firewall, primera gran ventaja

Si logramos agrupar los posibles servicios que demande un usuario por protocolos y utilidad, podemos tener un conjunto relativamente pequeño, 9 elementos: navegación web, mensajería instantánea, conexión a sistemas remotos, acceso a redes vpn, transferencia de ficheros, descargas p2p, etc.

Por cada usuario que solicita un acceso especial de esto nos veríamos obligados a suministrarle una IP fija, y dar de alta nueve reglas en el firewall para que estén disponibles para cuando el usuario quiera realizar una conexión. En un grupo de 2.000 usuarios (sólo profesores y personal de administración) tendríamos que introducir y mantener 18.000 reglas en nuestros sistemas de seguridad. En un esquema dinámico basado en NAC se comprueba que de estos 2.000 potenciales usuarios sólo coinciden como máximo 700 de forma simultánea en el sistema. Estos 700 seleccionarán uno de los 9 perfiles a la hora de conectarse a la red con lo que el número de reglas en el firewall se reduce a 700. Sobra decir las implicaciones que en cuanto a rendimiento e incluso consumo tiene una implementación de estas características.

De 2.000 usuarios potenciales, sólo coinciden como máximo 700 de forma simultánea en el sistema

7. Independencia del flujo, del origen y del destino de la comunicación, segunda gran ventaja

Una vez configurados todos los flujos de información para que basen su control de tráfico en el NAC, las políticas se aplican igual independientemente de que flujo se trate. Esto redunda rápidamente en la apreciación que tiene el usuario de la accesibilidad. Se logra una unificación total en el acceso del usuario

que ya no diferencia si se conecta por wifi, por cable o simplemente desde casa por vpn. Su interfaz es la misma, sus permisos los mismos y por consiguiente no tendrá un concepto diferente cuando usa uno u otro medio de comunicación.

Para poder garantizar esto es imprescindible que el tráfico sea autenticado. La autenticación va a ser la que nos diga cuál es el origen y el destino del flujo en cada momento y con esto mantendremos el control de las sesiones y los permisos asociados.

FIGURA 3

La utenticación nos dice cuál es el origen y destino del flujo

8. La correlación y federación de logs en tiempo real, un paso más hacia la seguridad y el control de uso real de los recursos

Cuando llega en algún momento un aviso del CERT indicando que alguna de nuestras ip's es origen de algún ataque, comienza la guerra. En ese momento corremos a nuestro firewall y vemos que esa ip pertenece a un pool de direcciones para hacer NAT de todas nuestras redes privadas. Entonces, corremos a los logs de tráfico del firewall y después de revisar varios gigabytes de ficheros de texto logramos encontrar la correlación entre la ip origen, el puerto de comunicaciones en cuestión y el destino que originó el NAT en cuestión. Pensando que ya lo tenemos, corremos al DHCP para ver las direcciones y observamos que pertenece a un pool dinámico de DHCP con un leasing bastante pequeño. Una vez más, tiramos del histórico y logramos más o menos encontrar la MAC del dispositivo y con un poco de suerte y documentación llegamos hasta el RACK y la roseta. Para que luego al final sea un switch en el despacho de la sala de profesores de algún departamento usado para que los alumnos hagan proyectos de fin de carrera.

Cuando llega un aviso del CERT indicando que alguna de nuestras ip's es origen de algún ataque, comienza la guerra

Con este sistema podemos tener un log único de los usuarios que usan nuestros recursos vinculados directamente con sus direcciones ip y el perfil de tráfico seleccionado para cada sesión en cuestión. Se simplifica mucho el control y el seguimiento de incidentes sin ir en decremento de la funcionalidad. La correlación en tiempo real da mucha información operativa y aprovechable de verdad.

9. Menú de servicios flexible, gestionable y con granularidad variable

Una diferencia importante de este sistema con respecto al resto es que la gestión de la asignación de perfiles de seguridad a los usuarios se puede basar en un LDAP. Esto hace que con una simple herramienta de gestión de atributos en un LDAP, el propio CAU pueda ser el que modifique, si fuera necesario los perfiles de tráfico que puede tener disponible cada usuario. En el momento en que el usuario entra en el sistema y se valida, el NAC busca los perfiles de tráfico que tiene disponible el usuario y los muestra en un menú para que pueda ser seleccionado por el propio usuario. Es en este momento cuando las reglas asociadas al perfil seleccionado van al firewall para permitir el tráfico solicitado.

Inherente a esta capacidad, está la forma de organizar los perfiles de tráfico. Podríamos tener dos tipos de organizaciones. En la primera de ellas se pueden hacer perfiles de tráfico por tipos de usuarios: alumnos, profesores, investigadores, doctorandos, etc. y en función del perfil del usuario mostrarle el menú de servicios asociados. Una segunda estructuración de la solución es hacer perfiles en función de servicios: navegación web, transferencia de ficheros, mensajería instantánea, videoconferencia, etc. Con esta segunda opción asociaríamos a cada usuario los perfiles que tiene disponibles para elegir en el sistema.

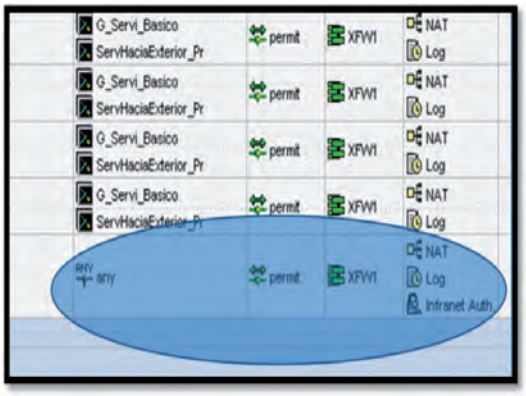
Otra ventaja del sistema es la granularidad del mismo. Podemos hacer una implantación de grano grueso: navegar, transferencia de ficheros, conexión a sistemas remotos. O bien ir a opciones de grano más fino: navegación estándar 80 y 443, navegación extendida (3128, 8080, 8083), transferencia de ficheros FTP, transferencia de ficheros SFTP, Jabber, Messenger, SSH, VNC, Telnet, etc. La ventaja de esta última opción es que aumenta la seguridad y la fiabilidad del sistema puesto que los logs de acceso son mucho más precisos. Tiene el inconveniente de dar pie a que existan combinaciones de perfiles incompatibles que no puedan ser activados de forma simultánea.

Una de las ventajas del sistema es la granularidad del mismo

10. Puesta en marcha de la solución, no hace falta tirarse a la piscina

La arquitectura de la solución planteada basa su gran potencial en los flujos de información. Estos flujos son gestionados en el firewall. Es en este dispositivo donde tenemos la llave para ir, poco a poco, indicando qué tráfico, con qué orígenes o destinos tiene que pasar por el NAC y estar correctamente autenticado antes de ser admitido.

FIGURA 4



En el caso de la ULL se optó por el siguiente método. Primero se puso para pasar por el NAC todo el tráfico de la última regla del firewall, la que típicamente hace el ANY ANY DENY. De esta forma si un usuario nos reclamaba un puerto de comunicaciones que no estaba abierto por defecto sólo teníamos que indicarle que para su uso sólo tenía que ir al NAC y validarse previamente seleccionando el perfil adecuado. Esto supuso un gran éxito debido a que ya podíamos cubrir unas demandas que se nos hacían muy engorrosas de incluir en nuestro firewall.

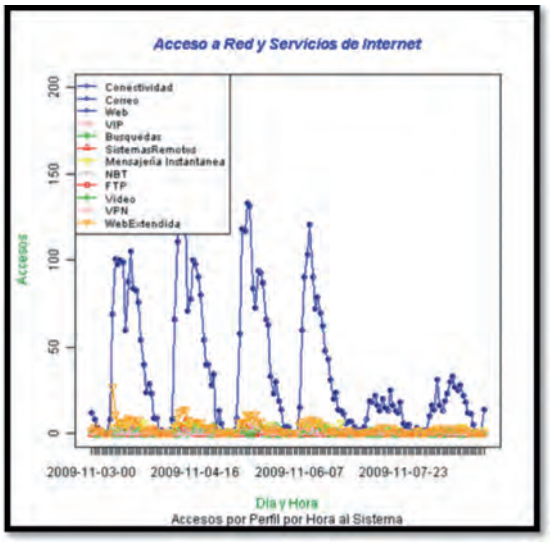
El usuario wifi tiene los mismos privilegios que el usuario cableado

En una segunda fase hicimos que todos los flujos de comunicación que tenían su origen en redes WIFI tuvieran que ser validados por el NAC antes de ser encaminados hacia su destino. Esto permitió dos cosas, que el usuario WIFI tuviera los mismos privilegios que el usuario cableado sin distinción del origen de la comunicación. El segundo efecto, sorprendente, fue el tema del roaming wifi-fijo-wifi. El profesor trabaja normalmente de forma cableada en su despacho en donde tiene su sesión abierta en el NAC para tener un cierto perfil de tráfico. Si cogía su portátil para ir a trabajar al laboratorio de forma inalámbrica no necesitaba volverse a validar, su sesión se actualizaba y sus permisos se mantenían. Esto ocurre también en sentido opuesto, si estaba dando una clase de teoría de forma inalámbrica con un perfil de tráfico autorizado, este se mantenía cuando volvía a su despacho para seguir trabajando de forma cableada. Este roaming es a nivel institucional funcionando también entre edificios.

11. Estadísticas complejas de una forma sencilla

El hecho de tener toda la seguridad de la red centralizada e integrada aporta una gran ventaja. El estudio de uso es mucho más fiable y didáctico, permitiendo tomar unas decisiones más adecuadas optimizando el uso de los recursos y las funcionalidades de los sistemas.

FIGURA 5



Tener toda la seguridad de la red centralizada e integrada aporta una gran ventaja

Cosas como qué perfiles de tráfico son los más usados, en qué franjas horarias se demandan más o desde qué ubicaciones son más utilizados tienen ahora una respuesta sencilla y clara. ¿Desde dónde se conectan los usuarios?, ¿a dónde? y ¿para qué? Tienen ahora una respuesta sencilla.

Normalmente si un perfil de tráfico se ve que demanda mucho podemos aumentar su granularidad para que la información obtenida sea más clara. Un ejemplo claro está en la conexión a los sistemas remotos. Si existe inicialmente un perfil de tráfico que es Conexión a Sistemas Remotos e incluye todos los protocolos típicos (telnet, ssh, Terminal Server, VNC, Cytrix, PCAnywhere, etc.) podemos registrar un uso muy elevado de este perfil que no nos aporta una información interesante de su uso. Con un simple análisis podemos decidir subdividir esta opción del menú en 6 opciones de menú, una por cada tipo de conexión a sistemas remotos. De esta forma sabremos qué usuarios hacen ssh, cuáles hacen VNC, etc. una estadística más precisa sin desmejorar el servicio ni las funcionalidades.

12. ¿Cómo actúan los usuarios ante un menú totalmente abierto?

Sólo un 10% de los usuarios ha elegido un perfil de tráfico distinto de la navegación web estándar

En la ULL hemos hecho una prueba, ¿qué pasaría si dejamos que a todos los usuarios, incluidos alumnos, les aparezca el menú con todos los posibles perfiles de tráfico? Algo que era impensable hasta hace unos meses, y era el hecho de dejar que incluso los alumnos tuvieran un acceso libre a Internet, es ahora una realidad.

Entre los usuarios, sólo un 10% ha elegido un perfil de tráfico distinto de la navegación web estándar. Y si quitamos a los que elegían un perfil de navegación web extendida con los perfiles de tráfico para 3128, 8080, 8083 nos quedamos en que menos de un 5% de los usuarios son los que eligen perfiles de tráfico especiales.

La conclusión de este análisis es clara, no merece, de momento, la pena eliminar perfiles de tráfico de los distintos tipos de usuarios. El tener que autenticarse es suficiente para garantizar que van a hacer un uso correcto de los recursos.

13. VPN, ¿Doble validación para el acceso a los recursos?

En cuanto se pone en funcionamiento una solución de este tipo surge la gran pega. Normalmente los profesores se conectan desde casa por VPN para obtener una "IP" válida de la ULL que le permita acceso a recursos bibliográficos externos a la misma, licenciados sólo para las IP's de la Institución.

En cuanto se mira el esquema de montaje aparece el problema. El usuario se valida una vez para conectarse por VPN, luego cuando su conexión intenta atravesar el firewall para salir a Internet por algún puerto especial tendrá que volver a validarse para seleccionar el perfil de tráfico deseado en la conexión. Aunque el sistema funciona, es muy poco operativo y da sensaciones raras en los usuarios.

Se hace obligado integrar el servidor VPN con el NAC y el firewall. Cuando un usuario se valida en el VPN se ha de sincronizar su sesión con el NAC para que cuando sus paquetes intenten atravesar el firewall en una conexión que requiera autenticación, estos sean válidos y no se exija una nueva autenticación. Para ello es necesario un protocolo que permita federar la seguridad entre los dos dispositivos. En este caso el NAC actuaría como servidor de seguridad para el firewall y para el VPN. Cuando el usuario entra por VPN y es validado, se almacena en el NAC su sesión y sus roles. Al intentar atravesar el tráfico ya está autenticado y si tiene permiso para acceder a donde desea todo funcionará de forma transparente. Al fin y al cabo, lo que se está buscando es extender el Roaming que existe ya entre wifi y cableado al mundo VPN de forma transparente.

FIGURA 6

La sesión se inicia en la VPN, se almacena en el NAC y se consulta y aplica desde el firewall de forma transparente para el usuario

Para la federación de seguridad existe ya un estándar elaborado por el Trusted Computing Group. Es el protocolo IF-MAP y está disponible desde Mayo de 2008. Ya empiezan a aparecer varios fabricantes que lo implementan en sus equipos de seguridad. Este es el caso de Juniper Networks, que lo incluye ya en varios de sus elementos de seguridad. Configurando este protocolo entre el VPN y el NAC se obtiene el efecto deseado. La sesión se inicia en el VPN, se almacena en el NAC y se consulta y aplica desde el firewall de forma totalmente transparente para el usuario.

14. ¿Seguimos federando e integrando?

La aparición de IF-MAP ha supuesto una revolución en la gestión de la seguridad en redes heterogéneas. Está claro que merece la pena poner en marcha en entorno de seguridad basado en este estándar que permita poco a poco que los distintos elementos que intervienen en las comunicaciones vayan alimentando el estado de seguridad de los usuarios y sus conexiones.

Para una correcta implantación de IF-MAP es necesario montar el MAP server

Como proyecto a corto plazo, para una correcta implantación de IF-MAP, es necesario montar el MAP server. Va a ser el gran cerebro de la organización. Simplemente, y nada menos, va a ser un repositorio central de metadatos donde todos los dispositivos van a volcar o recoger la información de seguridad que necesitan o recogen. En el caso de la ULL esto se plantea de dos formas, usar las funcionalidades de MAP server de los servidores de DHCP/DNS de Infoblox o bien usar las funcionalidades de MAP server de los Infranet Controler de Juniper. Se están estudiando las opciones para ver cuál encaja mejor.

Una vez esté el MAP Server, se tiene todo lo necesario para ir vinculando cada elemento de la red de comunicaciones (DNS, DHCP, Firewalls, VPN, Routers, NAC, Wifi, etc.) para pasar de un funcionamiento de modo StandAlone a un funcionamiento coordinado e integrado con el resto. Todo esto se hará a través del MAP Server mediante el protocolo IF-MAP. Toda esta comunicación se realiza mediante XML usando SOAP sobre conexiones seguras en https con certificados.

FIGURA 4

Toda esta comunicación se realiza mediante XML usando SOAP, sobre conexiones seguras en https con certificados

Referencias

[1] Universidad de La Laguna [*http://www.ull.es*]

[2] CCTI - Centro de Comunicaciones y Tecnologías de la Información de la Universidad de La Laguna [*http://www.ccti.ull.es*]

[3] 'NAC 2.0' Takes Shape Under Networking Giants. Microsoft, Cisco and TCG converge on standards as broader network access control standards emerge. [*http://www.internetnews.com/infra/article.php/3743346/NAC+20+Takes+Shape+Under+Networking+Giants.htm*]

[4] NAC 2.0, UN MODELO PARA UNA MAYOR SEGURIDAD DE LAS REDES CORPORATIVAS *[http://www.computing.es/Informes/200809290025/NAC-20-un-modelo-para-una-mayor-seguridad-de-las-redes-corporativas.aspx]*

[5] New IF-MAP enables coordinated Network Security. A Fundation for NAC 2.0 and Other Applications [*http://www.infoblox.com/solutions/if-map.cfm*]

[6] Interop New York 2009. *[http://www.interop.com/newyork/]*

[7] Trusted Network Connect: Open Standars for Integrity-bases Network Access Control *[http://www.trustedcomputinggroup.org/files/resource_files/38BA4157-1D09-3519-AD08262A419DA3B9/Open%20Standards%20for%20Integrity-based%20Network%20Access%20Control.pdf]*

[8] Overview of Trusted Network Connect (TNC) IF-MAP *[http://www.trustedcomputinggroup.org/files/resource_files/AA9CF85D-1D09-3519-ADC31E1BEA407646/TNC_IF-MAP%20Overview%2004-2009.pdf]*

[9] About the Statement of Health (SoH) in Network Access Protection *[http://technet.microsoft.com/en-us/library/bb680833.aspx]*

[10] Meeting Today's Security Challenges with End-to-End Network Access Control [*http://www.juniper.net/us/en/local/pdf/whitepapers/2000266-en.pdf*]

José Carlos González
(jgonzal@ull.es)
Universidad de La Laguna