Endurecimiento (hardening) en dispositivos de red: Routers y switchs

Jensy Leonardo Martínez Cruz
jensyleo@gmail.com
Universidad Piloto de Colombia

Resumen—Presentación de lo más indicado para un proceso de endurecimiento en los dispositivos de networking mas importantes (routers y switchs) que constituyen la columna vertebral de toda infraestructura de TI ya sea local o en la nube. Estos dispositivos siempre estarán presentes debido a que son fundamentales para la comunicación entre sistemas.

Abstract— Introducing the most suitable for a hardening process in major networking devices (routers and switches) and are the backbone of any IT infrastructure either locally or in the cloud. These devices will always be present because they are essential for communication between systems.

Índice de Términos—TI, convergencia, resiliencia, lockdown, lockup

I. INTRODUCCIÓN

Las infraestructuras de TI en Colombia se encuentran apoyadas por iniciativas como gobierno en línea, que han evolucionado de manera exponencial en los últimos años, además, han surgido nuevos conceptos como: virtualización, consolidación, convergencia, BYOD, escritorios virtuales, Cloud etc.

Dicha evolución ha llevado a una disminución considerable del hardware en muchos dispositivos tradicionales, pero no ha ocurrido así para los dispositivos de red por excelencia como los son routers y switchs, la realidad, es que estos dispositivos no son tan fáciles de reducir o consolidar ya que continúan siendo la *espina dorsal* de una infraestructura de TI.

Por esta razón se hace muy importante ver cuáles deben ser los mínimos aceptables para el endurecimiento de estos dispositivos enfocados en la realidad Colombiana, donde las infraestructuras no son tan grandes, no se utilizan todos los servicios de convergencia y los presupuestos para TI son limitados, pero la necesidad de seguridad está latente, adicionalmente las empresas en su necesidad de mantenerse competitivas buscan certificaciones de seguridad como la ISO 27001 que implementa una serie de con controles y/o normativas. El fortalecer estos dispositivos puede ayudar con su cumplimiento.

II. ENDURECIMIENTO (HARDENING)

Este es un proceso mediante el cual se trata de *disminuir al máximo la superficie de ataque* de un sistema (tecnológico para el caso que nos atañe) a través de una serie de actividades que para los dispositivos de red se condensan en tres.

A. Instalación segura del sistema operativo

Consiste en realizar la instalación del sistema operativo con unos requisitos mínimos que garanticen (hasta cierto punto) que el sistema se aloje en un lugar seguro y que además, que se cuente con suficiente espacio para almacenar archivos de servicio como lo son: los temporales, la memoria de intercambio y logs (aunque estos últimos se recomienda almacenarlos en un servidor dedicado para ello)

En el caso de los routers y switchs, la gran mayoría de fabricantes (por no decir todos) *no instalan sus sistemas operativos* en sus dispositivos, lo que hacen es volcar un archivo que se almacena en la memoria flash de estas máquinas, entonces surge una pregunta: ¿cómo se configuran estos dispositivos si no se les instala el sistema operativo?, la respuesta se basa en su filosofía de funcionamiento: La información de configuración de estos elementos de red se almacena aparte, a veces en la misma porción de memoria flash donde se coloca el sistema operativo o en otro dispositivo de almacenamiento de estado sólido. Cuando el

router o el switch arrancan, se carga el sistema operativo y acto seguido, el archivo de configuración, con base en este último el dispositivo activa o desactiva las funciones que necesita del sistema.

Por esta razón en routers, switchs y firewalls la instalación segura del sistema operativo es el paso más sencillo en el proceso de hardening, ya que lo que se debe hacer es descargar la última versión liberada por el fabricante desde su portal, verificar su hash después de su descarga y volcar mediante la utilización de algún protocolo seguro como lo sería SFTP (o vía USB con una memoria previamente esterilizada) dicha versión a la memoria flash. La mayoría de fabricantes publican estos procedimientos en sus portales. Cabe anotar que actualmente en Colombia no es común utilizar SFTP para este procedimiento, se prefiere usar TFTP que no es un protocolo seguro, sin embargo esto es válido si el volcado se realiza fuera de línea (offline) y por un segmento de red que solo permita conexión punto a punto.

Actualmente los fabricantes líderes en estas tecnologías colocan en sus máquinas dos memorias flash independientes para poder volcar dos sistemas operativos, de esta manera en caso que falle una de las memorias, la otra entrará como respaldo, lo mismo ocurre con el archivo de configuración. Esta característica es deseable y se debe buscar para nuevas adquisiciones tecnológicas y para infraestructuras de misión crítica.

B. Eliminar lo que no se necesita (Lockdown)

Consiste en eliminar todo aquello que no es necesario para el cumplimiento de los objetivos funcionales que se esperan de la máquina. Los dispositivos de red modernos ofrecen una amplia gama de servicios y están activos por defecto, los cuales si no van a ser utilizados deben ser desactivados, de esta manera, también se elimina la posibilidad que se pueda ingresar a estos elementos a través de estos servicios utilizándolos como *puertas traseras*, por ejemplo: si el dispositivo trae activo por defecto protocolos multicast como PIM pero no se piensa utilizar videoconferencia en la red o algún otro servicio que requiera multicast esta funcionalidad debe desactivarse, lo mismo ocurre para servicios tales como DHCP, DNS entre otros. Respecto a estos últimos cabe anotar que las buenas prácticas de TI (y la experiencia) nos recomiendan no colocar este tipo de servicios en routers, switchs ni en firewalls, lo que se recomienda es colocarlos en dispositivos aparte que ofrezcan mayor robustez y versatilidad.

La ejecución de estas actividades en routers, y switchs no conlleva ningún proceso de desinstalación, el procedimiento a seguir consiste en *desactivar las funcionalidades* que estos elementos poseen a través de sus archivos de configuración.

Para ayudar en este proceso, los grandes fabricantes y grupos de seguridad independientes publican una serie de recomendaciones, las cuales pueden servir como guía para esta labor, pero es muy importante resaltar que este material no es para seguir al pie de la letra, más pensando en Colombia, con lo diversas que son las infraestructuras de redes y lo diferentes que son las necesidades de seguridad en cada ambiente.

C. Proporcionar lo que se necesita (Lockup)

Consiste en colocar todo aquello que sea necesario no solo para el cumplimiento de los objetivos funcionales de la máquina, sino para que preste los servicios de manera segura. Análogamente al proceso de lockdown, la ejecución de esta actividad no conlleva ningún procedimiento de instalación, lo que se debe hacer es *activar las funcionalidades* que estos elementos poseen a través de sus archivos de configuración.

Se pueden usar los mismos documentos de recomendaciones publicadas por los fabricantes y grupos de seguridad independientes para el proceso de lockdown, teniendo en cuenta lo ya explicado sobre este tipo de documentos.

Adicionalmente, pensando un poco en la continuidad de los servicios, la alta disponibilidad (HA) es también una necesidad de seguridad y por esta razón es recomendable agregar un cuarto paso al proceso de hardening (aunque técnicamente no está contemplado) que consiste en tener redundancia, no solo en equipos sino en conexiones obteniendo un buen nivel de resiliencia en la red.

Tener elementos de red que se respalden entre si

es recomendado para lo que se ha llamado las redes de nueva generación (NGN), las cuales se están imponiendo como un nuevo modelo estándar.

Cuando se coloca redundancia en configuración activo-activo, no solo se tienen 2 maquinas respaldándose una a la otra, sino que además están trabajando para un objetivo común, lo que teóricamente aumenta el desempeño al doble.

III. ENDURECIMIENTO DE ROUTERS

Actualmente en Colombia, los grandes proveedores de telecomunicaciones poseen la mayor parte de la autonomía sobre los routers instalados, debido a que cuando ellos proveen el enlace también entregan el dispositivo de enrutamiento, esto ha resultado ventajoso para los clientes que ven como entregan la administración de sus dispositivos de networking que van hacia la WAN a un tercero y no se preocupan por la depreciación ni actualización, ya que esto normalmente está ligado a un contrato de prestación del servicio, incluso esto también ocurre con los proveedores de internet para el hogar.

Esto hace que no sea posible para la mayoría realizar un proceso de hardening por propia mano, pero si es posible exigirle al proveedor que haga esta tarea y entregue evidencia de ello.

En un router se deben hacer mínimo estas tareas en el proceso de hardening:

A. Asegurar el acceso

Una de las primeras tareas es lograr que el acceso para la administración del router se realice garantizando la confidencialidad, autenticidad y trazabilidad sobre él, para ello y sin importar la marca o modelo del router se pueden hacer las siguientes tareas:

1) Desactivar protocolos inseguros y activar los seguros: Este es el típico caso de eliminar TELNET y HTTP que no cifran sus comunicaciones y remplazarlos por SSHv2 y HTTPS que si lo hacen. Es recomendable utilizar certificados digitales no auto firmados para las comunicaciones HTTPS.

2) A pesar que HTTPS es un protocolo seguro se recomienda no activarlo, ya que estos elementos gráficos suman vulnerabilidades a los routers y su concepción siempre ha sido gestionarlos, administrarlos y configurarlos por línea de comandos (CLI), si se desean utilizar interfaces gráficas, es preferible utilizar una consola remota para ello. Existen muchos fabricantes que ofrecen estas consolas con una amplia gama de funciones que pueden suplir el uso de HTTPS.

3) Restringir el acceso desde cualquier parte a través de ACL o un mecanismo equivalente: La gestión solo debe estar disponible para un limitado rango de direcciones IP, las cuales deben ser exclusivas de las maquinas del personal de administración.

4) Autenticar el acceso a través de servidores remotos redundantes: Configurar el acceso a través de un servidor remoto y dedicado nos ofrece aparte de la autenticación, niveles de autorización y auditoría sobre los administradores, de esta manera, se obtiene trazabilidad y segregación de funciones, aumentando el control sobre el router.

5) A través del servidor de acceso remoto implementar políticas de password fuerte, con longevidad y número de intentos limitados.

6) Configurar un usuario de recuperación de desastres: Se debe configurar uno y solo un usuario local en el router para que en caso de un desastre se pueda acceder al mismo y recuperarlo.

7) El usuario local para recuperación de desastres debe tener una política de password fuerte, longevidad, límites de acceso y mantenerse en sobre sellado con cadena de custodia.

8) Configurar límite de intentos y conexiones: Esto es fundamental para evitar ataques de fuerza bruta y abandonos de sesión abierta.

9) Configurar un servicio de logs remoto: De esta manera se pueden tomar acciones proactivas elevando los niveles de seguridad.

B. Asegurar los protocolos y servicios

Un router solo debe hacer las tareas para las cuales fue diseñado y debe hacerlas de manera segura. Otras funciones adicionales deben ser eliminadas, el único servicio suplementario que se acepta y solo en situaciones particulares, son las VPN, igualmente es muy importante tener un monitoreo seguro.

Para lograr estos objetivos se puede hacer lo

siguiente:

1) Eliminar las configuraciones por defecto innecesarias: Normalmente las configuraciones por defecto no son recomendables, sin embargo, pueden existir algunas dependiendo del diseño de la red que pueden ser deseables y quizás sea necesario mantenerlas, pero las demás, deben ser eliminadas.

2) Eliminar cualquier otro servicio de red aparte del enrutamiento: Esto puede tener una excepción a la regla en redes pequeñas donde servicios como DHCP, DNS y hasta de firewall son aceptables.

3) Minimizar la cantidad de protocolos de enrutamiento que procesa el router concurrentemente: Esto ahorra consumo de procesamiento y memoria.

4) Maximizar en la medida de lo posible el enrutamiento estático: Esto ayuda a disminuir el consumo de procesamiento.

5) Optimizar los protocolos de enrutamiento dinámico de tal manera que la tabla de enrutamiento se mantenga lo más pequeña posible (sumarizada) y que las métricas estén correctamente configuradas para que el router tome las mejores decisiones de enrutamiento y lo haga de la manera más óptima posible.

6) Asegurar los protocolos de enrutamiento: Esto se logra autenticando las comunicaciones de actualizaciones de estado y enrutamiento entre los *routers de confianza*. Sin importar el protocolo de enrutamiento implementado, se debe garantizar que las actualizaciones de enrutamiento sean legítimas y de esta manera evitar ataques de spoofing que puede conllevar a loops.

7) Activar los servicios antispoofing que cada fabricante ofrece.

8) Limitar el tráfico broadcast.

9) Limitar o eliminar las respuestas a los paquetes de control.

10) No permitir el paso de paquetes no estándar (fragmentados, jumbofarmes, etc.)

11) Configurar el NTP oficial de Colombia.

12) Activar logs de auditoría.

13) Enviar los logs de auditoría a un servidor syslog.

14) Definir a nivel de configuración exactamente por donde y a que servidor enviar los logs de auditoría.

15) Preferir Netflow sobre SNMP: En Colombia el monitoreo por SNMPv1 es el más utilizado pero Netflow posee características funcionales y de seguridad muy interesantes, además, es el preferido para las redes de próxima generación (NGN).

16) Si no es viable utilizar Netflow, utilizar SNMP versión 3, asegurándolo a través de ACL y si es posible, utilizarlo en una red de gestión solo alcanzable por los servidores de monitoreo.

17) A través del monitoreo configurar umbrales de alarma para los recursos del router: CPU, memoria, tráfico en los puertos, etc.

18) Colocarlos en configuración de alta disponibilidad a través de protocolos abiertos como VRRP: De esta manera se tiene redundancia en equipos, también se recomienda redundancia en conexiones tanto la hacia la WAN como hacia el firewall ubicado en la LAN.

C. Asegurar la trazabilidad

Este elemento es prácticamente inexistente en Colombia, donde la documentación no forma parte del proceso de implementación, soporte y mantenimiento de los sistemas tecnológicos por diversas razones, sin embargo, con las nuevas exigencias que solicitan las certificaciones destacándose la ISO 27001 como una de las más apetecidas en Colombia, hace que poder tener trazabilidad en los dispositivos de red sea muy importante como elemento colaborativo para obtener dichas certificaciones, además, la documentación es fundamental en toda infraestructura de networking, que si se mantuviera actualizada y correcta colaboraría bastante en la reducción y resolución de problemas.

Los elementos a tener en cuenta para asegurar la trazabilidad son:

1) Tener hoja de vida del dispositivo.

2) Tener ingeniería de detalle de la solución de networking.

3) Tener documentada la configuración del router.

4) Generar un programa de respaldo del sistema operativo y configuraciones, acorde con el programa de actualización de software de la compañía.

Existen otra serie de actividades de hardening

para estos dispositivos y dependiendo del fabricante hay unas puntales según la marca y modelo, sin embargo, las presentadas en el presente artículo, aplican para la gran mayoría de modelos de router y para la realidad de TI en Colombia.

IV. ENDURECIMIENTO DE SWITCHS

Es el dispositivo de red más cerca al usuario y uno de los más descuidados en temas de seguridad. Este es el núcleo de una red LAN y normalmente no está administrado por un proveedor de telecomunicaciones, lo que permite tener más oportunidad de realizar hardening de propia mano.

Las redes de siguiente generación (NGN) traen nuevas exigencias dada la llegada de la convergencia, donde voz, datos y video ahora viajan de manera indistinta por el mismo canal, las redes SAN ahora con el protocolo iSCSI que se está empezando a preferir sobre fiberchannel, han convertido los sistemas de almacenamiento en parte integral de la red, los protocolos abiertos han desplazado los protocolos propietarios, los enlaces de 100Gb/s ya se están imponiendo a pesar de su alto costo, la redundancia con estándares como LACP, IRF y VRRP ahora son una exigencia.

Todos estos elementos hacen que el hardening de los switchs ahora cobre mayor importancia dado que prestan muchos más servicios que antes y deben ser prestados de manera segura.

En los switchs se deben hacer mínimo estas tareas en el proceso de hardening:

A. Asegurar el acceso

Al igual que en los routers, una de las primeras tareas es lograr que el acceso para la administración del switch se realice garantizando la confidencialidad, autenticidad y trazabilidad sobre él, para ello y sin importar la marca o modelo se pueden hacer las siguientes tareas:

1) Desactivar protocolos inseguros y activar los seguros: Este es el típico caso de eliminar TELNET y HTTP que no cifran sus comunicaciones y remplazarlos por SSHv2 y HTTPS que si lo hacen. Los certificados digitales auto firmados son aceptados si la administración se va a realizar de manera local a través de HTTPS.

2) A pesar que HTTPS es un protocolo seguro, se recomienda no activarlo, ya que estos elementos gráficos suman vulnerabilidades a los switchs, sin embargo, a diferencia de los routers, los switchs por su gran cantidad de puertos y su elevado número en la red LAN, hace que gestionarlos, administrarlos y configurarlos por línea de comandos (CLI) no sea eficiente, por lo tanto, las interfaces graficas son deseables, pero deben ser utilizarlas a través una consola remota. Existen muchos fabricantes que ofrecen estas consolas con una amplia gama de funciones que pueden suplir el uso de HTTPS.

3) Si en el modelo de administración se tiene que hacer gestión remota (desde internet), la conexión debe hacerse vía VPN ya sea IPSec o SSL; sin importar que ya estén SSHv2 y HTTPS activados. Gestionarlos desde internet conlleva a publicar estos dispositivos, los cual no es deseable ya que los expone a ataques desde internet. Como regla general *no es recomendable publicar un elemento de red solo para gestionarlo* ya que ese no es el objetivo de una publicación, *la publicación tiene por objetivo prestar servicios hacia internet*.

4) Restringir el acceso desde cualquier parte de la LAN a través de ACL y utilizar una VLAN exclusiva para administración solo alcanzable por el personal de autorizado: La gestión solo debe estar disponible para las maquinas del personal de administración.

5) Autenticar el acceso a través de servidores redundantes: Configurarlo a través de un servidor remoto y dedicado, nos ofrece aparte de la autenticación, niveles de autorización y auditoría sobre el personal autorizado, de esta manera, se obtiene trazabilidad y segregación de funciones, aumentando el control sobre los switchs de la red.

Pensando en protocolos abiertos, para la implementación de este servidor redundante, es recomendable hacerlo con tecnología RADIUS e integrándolo con el directorio activo de la red.

6) A través del servidor de acceso remoto implementar políticas de password fuerte, con longevidad y número de intentos limitados o utilizar las mismas políticas del directorio activo.

7) Configurar un usuario de recuperación de desastres en todos los switchs de la red: Se debe configurar uno y solo un usuario local en todos los

switchs para que en caso de un desastre se pueda acceder a los mismos y recuperarlos.

8) El usuario local para recuperación de desastres debe tener una política de password fuerte, longevidad, límites de acceso y mantenerse en sobre sellado con cadena de custodia.

9) Configurar límite de intentos y conexiones: Esto es fundamental para evitar ataques de fuerza bruta y abandonos de sesión abierta.

10) Configurar un servicio de logs hacia un servidor syslog: De esta manera se pueden tomar acciones proactivas elevando los niveles de seguridad.

B. Asegurar los protocolos y servicios

Un switch ahora presta más servicios por la nueva tendencia de redes convergentes, pero debe ofrecerlos de manera segura y otras funciones adicionales deben ser eliminadas, igualmente es muy importante tener un monitoreo seguro

Para lograr estos objetivos se puede hacer lo siguiente:

1) Eliminar las configuraciones por defecto innecesarias: Normalmente las configuraciones por defecto no son recomendables, sin embargo, pueden existir algunas dependiendo del diseño de la red que pueden ser deseables y quizás sea necesario mantenerlas, pero las demás, deben ser eliminadas.

2) Eliminar cualquier otro servicio de red aparte del de enrutamiento, QoS, Spaning Tree y otros necesarios para el cumplimiento de sus funciones misionales: Esto puede tener una excepción a la regla en redes pequeñas donde servicios como DHCP, DNS son aceptables.

3) A pesar que los grandes fabricantes lo ofrecen, no se recomienda consolidar servicios adicionales en los nuevos switchs CORE que tienen la capacidad para instársele módulos de firewall, IPS, controladora wireless etc. esto conllevaría a un punto único de falla y en un análisis de riesgos, esto se vería claramente como un riesgo alto, muy alto o inaceptable dependiendo de la métrica que se utilice y aunque se coloquen en alta disponibilidad, las actualizaciones, y migraciones serian dependientes de un único chasís el cual cuando se haga obsoleto hará obsoletos todos los otros módulos que posee.

4) Minimizar la cantidad de protocolos de enrutamiento que procesa : Actualmente los switchs son capaces de hablar protocolos de enrutamiento dinámico como RIP y OSPF entre otros, sin embargo, antes de activarlos se debe hacer un diseño de red muy estricto para analizar la necesidad de activarlos, ya que hay que recordar que *los protocolos de enrutamiento dinámico están pensados para redes de gran tamaño* y en Colombia hay muy pocas redes con un tamaño que justifique el uso de estos protocolos en la red LAN.

5) Maximizar en la medida de lo posible el enrutamiento estático: Esto ayuda a disminuir el consumo de procesamiento.

6) Si en el diseño de la red se optó por usar enrutamiento dinámico se recomienda optimizar dichos protocolos de tal manera que la tabla de enrutamiento se mantenga lo más pequeña posible (sumarizada) y que las métricas estén correctamente configuradas para que el switch tome las mejores decisiones de enrutamiento y lo haga de la manera más óptima posible.

7) Asegurar los protocolos de enrutamiento: Esto se logra autenticando las comunicaciones de actualizaciones de estado y enrutamiento entre los switchs. Sin importar el protocolo de enrutamiento implementado, se debe garantizar que las actualizaciones de enrutamiento sean legítimas y de esta manera evitar ataques de spoofing que puede conllevar a loops.

8) Activar los servicios antispoofing que cada fabricante ofrece.

9) Permitir el uso de Jumboframes únicamente hacia los dispositivos que lo utilizan como es el caso de algunos modelos de servidores de almacenamiento iSCSI que los usan para optimizar la transferencia de la información.

10) Configurar el NTP hacia un servidor NTP local, el cual a su vez debe estar sincronizado con el servidor NTP oficial de Colombia.

11) Activar logs de auditoría.

12) Enviar los logs de auditoría a un servidor syslog.

13) Definir a nivel de configuración exactamente por donde y a que servidor enviar los logs de auditoría.

14) Preferir Netflow sobre SNMP: En Colombia el monitoreo por SNMPv1 es el más utilizado pero

Netflow posee características funcionales y de seguridad muy interesantes, además, es el preferido para las redes de próxima generación (NGN).

15) Si no es viable utilizar Netflow, utilizar SNMP versión 3, asegurándolo a través de ACL y si es posible, utilizarlo en una red de gestión solo alcanzable por los servidores de monitoreo.

16) A través del monitoreo configurar umbrales de alarma para los recursos del switchs: CPU, Memoria, tráfico en los puertos, etc.

17) Colocarlos en configuración de alta disponibilidad a través de protocolos abiertos como IRF o VRRP entre otros: De esta manera se tiene redundancia en equipos, también es deseable redundancia en conexiones por medio de LACP tanto entre switchs como hacia otros dispositivos.

18) Configurar en los puertos troncales únicamente las VLANs que se debe propagar: De esta manera se evita que el tráfico broadcast viaje por las troncales sin ninguna necesidad.

19) Activar Spanning Tree: Muy importante para evitar los tan temidos *loops de conmutación* que en algunas marcas pueden dejar toda la red fuera de operación,

20) Asegurar el Spanning Tree: Se recomienda escoger claramente entre los modos de Spanning Tree según convenga en el diseño de red (STP, RSTP, MSTP, PVSTP), acto seguido, definir claramente la raíz del árbol de conmutación, luego, definir claramente los puertos que se van a utilizar para interconectar switchs (troncales) y los que se van a utilizar para conectar dispositivos terminales (de borde), una vez definido esto, se les debe configurar protección de BPDU. De esta manera el árbol de conmutación se mantendrá estable y no consumirá procesamiento recalculando el árbol de conmutación cada vez que se conecta o desconecta un puerto y se previenen ataques de BPDU.

21) Apagar administrativamente los puertos que no se van a utilizar y eliminarles toda configuración: Esto aumenta la carga administrativa pero aumenta los niveles de seguridad.

22) Definir claramente una VLAN de administración y a través de filtrado ACL u otro método, configurar que solo sea posible administrar estos dispositivos desde esta VLAN.

23) Configurar seguridad en los puertos: A pesar que es una queja en Colombia el hecho que implementarlo aumenta la carga administrativa, la verdad es que en contraposición aporta mucho a la seguridad.

Limitar al mínimo las propagaciones broadcast por puerto colabora bastante cuando hay malware en los equipos de cómputo, lo mismo cuando solo se permite el paso de jumboframes en los puertos donde están conectadas maquinas que realmente lo necesitan (Servidores, NAS, SAN, troncales, etc.), de igual manera solo permitir el paso de una cantidad limitada de direcciones MAC en los puertos de acceso, evita que se puedan colocar dispositivos intrusos (HUBS, accespoints etc.), activar la opción que solo permita una(s) MAC(s) autorizada(s), evita que se conecten maquinas en puntos nos autorizados de la red y que trasladen de manera indiscriminada los equipos.

C. Asegurar la trazabilidad

Este elementos está un poco más presente en la parte LAN pero sigue siendo una gran falencia en Colombia, donde la documentación pocas veces forma parte del proceso de implementación, soporte y mantenimiento de los sistemas tecnológicos LAN por diversas razones, sin embargo con las nuevas exigencias que solicitan las certificaciones destacándose la ISO 27001 como una de las más apetecidas en Colombia, en este momento hace que poder tener trazabilidad en los dispositivos de red sea muy importante como elemento colaborativo para obtener dichas certificaciones, además, la documentación es fundamental en toda infraestructura de networking y si se tuviera actualizada, colaboraría bastante en la reducción y resolución de problemas.

Los elementos a tener en cuenta para asegurar la trazabilidad son:

1) Tener hoja de vida del dispositivo.

2) Tener ingeniería de detalle de la solución de networking.

3) Tener documentada la configuración.

4) Generar un programa de respaldo del sistema operativo y configuraciones, acorde con el programa de actualización de software de la compañía.

Un elemento adicional que si no fuera por su elevado costo sería un complemento ideal, es la *implementación de inteligencia en la capa física,* a través de sistema de *patch panel inteligente*. En la gran mayoría de cableados de Colombia, el patch panel no es más que un sistema de conexión física sin ningún tipo de monitoreo, el cual se deja a los switchs, pero estos lo hacen en la capa de enlace, por ejemplo: En un proceso de aprovisionamiento o reorganización de dispositivos en la red si hay un switchs con un puerto desactivado administrativamente, no hay manera de saber si tiene conectado un cable o no, habría que *utilizar trucos* para obtener esta información. Los patchs panels inteligentes ofrecen: Seguridad, documentación automatizada, administración de activos, administración remota de la capa física, alarmas proactivas y aprovisionamiento más eficiente.

Existen otra serie de actividades de hardening para estos dispositivos y dependiendo del fabricante hay unas puntales según la marca y modelo, sin embargo, las presentadas en el presente artículo, aplican para la gran mayoría de modelos de switch y para la realidad de TI en Colombia.

V. CONCLUSIONES

1. Un proceso de hardening en routers y switchs debe ajustarse a las necesidades de una compañía y a la realidad del entorno, sin embargo, hay unos mínimos a cumplir que son comunes para la mayoría de ambientes en Colombia.

2. A pesar de existir múltiples fabricantes los procesos de hardening dado el objetivo tecnológico y funcional de los routers y switchs son similares entre ellos.

3. Después de hacer un proceso de hardening el siguiente paso debe ser una auditoría para verificar los resultados.

4. Después de una auditoría exitosa a routers y a switchs una prueba de penetración sobre los mismos es recomendable.

5. La situación actual de conectividad en Colombia con el descontrolado boom de la nube hace que cobren más importancia los routers y switchs porque ahora se necesita más conectividad que nunca.

6. Por la razona anterior hay que hacer de manera responsable y metodológica el hardening en estos dispositivos colocándolos en el clico de planeación diseño, implementación, operación, optimización de la compañía.

REFERENCIAS

[1] *Cisco, Cisco Guide to Harden Cisco IOS Device [En línea]* http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.pdf. *[Última actualización: Junio 2014]*

[2] Grupo Smartekh *[En línea]*. http://blog.smartekh.com/%C2%BFque-es-hardening/

[3] *Camilo Andrés Forero Velandia, Auditoría en routers y switchses [En línea]* http://es.slideshare.net/jcfarit/auditora-de-routers-y-switchses. *[Última actualización: octubre 2003]*

[4] *HP, Hardening Procurve switchses [En línea]* http://www.hp.com/rnd/pdfs/Hardening_ProCurve_Switchses_White_Paper.pdf *[Última actualización: febrero 2007]*

[5] *HP, HP Networking guide to hardening Comware based devices [En línea]* http://h20564.www2.hp.com/hpsc/doc/public/display?docId=c03536920. *[Última actualización: octubre 2003]*