Buenas prácticas de seguridad en redes de almacenamiento

La aparición y posterior proliferación de las redes de almacenamiento ha supuesto, aparte de las ventajas competitivas y operativas para las que fueron ideadas, una serie de cambios en la manera en que se accede y administra el almacenamiento de los sistemas de información, con nuevas implicaciones de seguridad, que trataremos de enumerar, así como una serie de buenas prácticas que pueden complementar las técnicas y mecanismos de protección que estas nuevas tecnologías incorporan.

Antonio Requejo / Javier Zamorano

El papel que están tomando las redes de almacenamiento como herramientas para consolidar, virtualizar y hacer accesibles los dispositivos físicos de almacenamiento las convierte en punto de interés corporativo. En este artículo nos referiremos a las redes de almacenamiento en un sentido muy laxo, englobando tecnologías como NAS, SAN y las últimas tendencias en almacenamiento sobre tráfico IP.

La evolución tecnológica de las redes de almacenamiento parte del escenario básico del almacenamiento directamente conectado al sistema que hace uso de él (DAS, Direct Attached Storage).

Con la llegada de las redes de ordenadores se hizo posible el acceso remoto al sistema. De esta forma, mediante sesiones remotas, se habilitaba el consumo, aún local, del almacenamiento, pero aumentando las posibilidades de acceso, y por tanto, los riesgos.

El salto cualitativo comienza cuando se habilita la utilización local de recursos de almacenamiento remotos, mediante protocolos como NFS (Network File System), dando lugar a los sistemas NAS (Network Attached Storage), que ofrecen un sistema de ficheros definido (con sus permisos, cuotas, gestión de asignación de espacio…) visibles y accesibles, como si de unidades locales se tratara.

Las limitaciones de los sistemas NAS se sobrepasaron con la aparición del protocolo Fibre Channel (FCP) y el despliegue de redes basadas en él, SAN (Storage Area Network), que ofrecían acceso de baja latencia y alto ancho de banda a dispositivos en modo bloque ("sin formatear"). Posteriormente, hemos visto aparecer soluciones mixtas NAS+SAN, pasarelas SAN para unión de "islas SAN", y por último, protocolos que encapsulan este acceso al almacenamiento sobre tráfico IP, abaratando los costes que acarreaba el equipamiento propio de las SAN.

Algunos fabricantes de equipamiento SAN incorporan diversos métodos para autenticar dispositivos (secreto compartido, certificados…) pero son de aplicación incipiente y opcional (no forman parte de ningún estándar).

Desde el punto de vista de seguridad, todas estas posibilidades conforman un escenario cambiante y por tanto complejo, agravado por la aparición de diferentes modelos de seguridad y riesgo/confianza que introducen estas tecnologías, cada una de las cuales acarrea distintas formas de acceso y administración de los dispositivos de almacenamiento.

En la mayoría de los casos, los protocolos contienen una mínima funcionalidad embebida de seguridad, que es necesario complementar (con diseño topológico, gestión de tráfico, cifrado) para conseguir seguridad extremo a extremo. Estos dos factores, junto con el diferente enfoque de los mundos del almacenamiento y la seguridad, que tradicionalmente manejan conceptos y prioridades diferentes, dificulta la tarea de 'securización' de las redes de almacenamiento, que se está encomendando en primera instancia a administradores de sistemas especializados en almacenamiento.

Las buenas prácticas complementan las posibilidades y técnicas que cada solución ofrece, por lo que repasaremos tales herramientas para enumerar ciertas recomendaciones que ayudarán a mitigar los riesgos de nuestra red de almacenamiento.

Los riesgos a los que se ve sometida una red de almacenamiento (considerando el escenario de forma global) no son muy diferentes a los que se presentan en otros escenarios TI:

– Acceso no autorizado/no autenticado a los dispositivos o repositorios (lectura, modificación)

– Ataques al tráfico en tránsito

• Modificación de paquetes, tanto de datos como de información de control

• Inyección de información

• Robo de sesiones/conexiones

– Ataques de denegación de servicio, rotura de conexiones

– Disrupción de la negociación de los niveles de seguridad

– Disrupción del servicio de descubrimiento de sistemas de almacenamiento

– Suplantación de identidades

Todo ello con sus consecuencias derivadas (impacto en los procesos de negocios, incumplimiento de obligaciones legales…) igualmente conocidas

Soluciones de almacenamiento basadas en NAS

En las soluciones NAS, (basadas en NFS, CIFS/SMB y similares) la seguridad se aplica en el servidor, con las técnicas de control de acceso

que proporcione el SO y/o sistema de ficheros, y en el protocolo de comunicación cliente-servidor, combinadas con medidas de seguridad IP convencionales para controlar/autorizar el tráfico.

El principal problema ha venido tradicionalmente de las carencias en el protocolo, específicamente, por:

– La autenticación poco robusta de los clientes

– La utilización de protocolos de comunicación no orientados a conexión (UDP)

– El flujo de datos en claro (sin cifrar)

Actualmente los protocolos han evolucionado en distinto grado para subsanar en parte o en la totalidad dichos problemas, aunque la gran variedad de implementaciones hace necesario extremar las precauciones.

¿Que recomendaciones específicas para estas redes se pueden ofrecer? Para las que se basen en CIFS:

– Evite usar la autenticación según recurso (frente a la autenticación por usuario).

– Active la transmisión de contraseñas cifradas por la red, frente al envío de las mismas en claro.

– Habilite la autenticación de ambas partes, servidor y cliente.

– Utilice exclusivamente protocolos de autenticación robustos (NTLMv2 frente a LM o NTLM).

Para redes NFS:

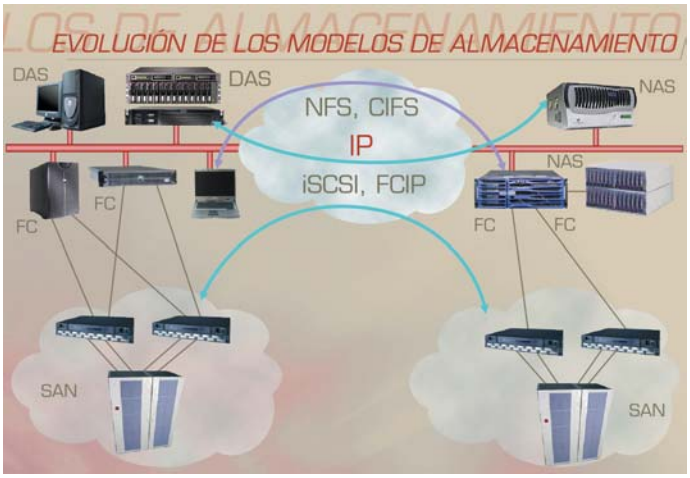
– Elija una implementación de NFS que haya resuelto los problemas tradicionales del protocolo (comunicación en claro a ficheros, envío de contraseñas sin cifrar por la red, dificultades para autenticar fehacientemente al usuario)

– Deshabilite el acceso en base al nombre o IP del cliente

– Utilice protocolos de autenticación como Kerberos v5

Redes FC-SAN

Los distintos mecanismos con los que cuenta la arquitectura SAN para reforzar la seguridad no son robustos. La base, que es el protocolo FCP, no es un protocolo seguro, ya que la seguridad no era un requisito en su diseño original. Por otro lado, las técnicas que se pueden aplicar en la infraestructura propia de los *fabric* SAN (zoning soft/hard, LUN masking) son relativamente fáciles de vulnerar. Finalmente, la granularidad en el control de acceso que se consigue es básicamente binaria (se accede con total privilegio o no se accede).



Como parte de los recursos de la organización, las redes de almacenamiento deben cumplir con la Política de Seguridad corporativa y, por tanto, antes de desplegar una, es imprescindible analizar detalladamente qué requisitos de seguridad tenemos y qué tecnología nos los puede proporcionar.

Algunos fabricantes de equipamiento SAN incorporan diversos métodos para autenticar dispositivos (secreto compartido, certificados…) pero son de aplicación incipiente y opcional (no forman parte de ningún estándar).

Las buenas prácticas en estas redes se limitan a aplicar, lo más exhaustivamente posible, las citadas técnicas de *masking* y *zoning*, así como procurar que todos los dispositivos dispongan de capacidad de autenticación entre las partes y configuración de ACLs.

Almacenamiento basado en IP

Las soluciones basadas en IP (iSCSI, FCIP) siguen sin ofrecer una solución global para la información almacenada, ya que están exclusivamente orientadas a habilitar el acceso a dispositivos de almacenamiento a través de redes IP. Lo único es que, al habilitarse esta tecnología como portadora, aparecen como aplicables en principio los mecanismos de seguridad IP tradicionales, para complementar las limitaciones de las SAN basadas en FC, especialmente la autenticación de los extremos y el cifrado de la conexión.

En cualquier caso, ha de tenerse en cuenta que, si bien se dispone en estos casos de herramientas de seguridad maduras, las velocidades y latencias requeridas en las redes SAN (redes en todo caso gigabit, con gran cantidad de tráfico) sobre IP, hacen de dudosa aplicación ciertas herramientas de seguridad IP convencionales (FW, IDS). Están apareciendo aplicaciones específicas que hacen uso de soluciones como SSL o IPSec, de momento centrándose en el cifrado de la comunicación y la autenticación. Nótese además que esta utilización de redes IP, muchas veces compartiendo medio con otras redes, exponen los recursos en mayor grado, generalizando su acceso.

Nuestras recomendaciones, aparte de las que sean aplicables genéricamente en las redes SAN, pasan por la aplicación de mecanismos de seguridad de IPSec/FC-Sec (más específico) para asegurar los datos en tránsito y reforzar la autenticación de las partes. Aparte, además, se recomienda cautela en la aplicación de soluciones de seguridad IP tradicionales por el potencial impacto en la funcionalidad y rendimiento.

Buenas prácticas generales

Las buenas prácticas generales no sorprenderán a nadie, pues son la adaptación de las de "obligado cumplimiento" en redes y sistemas genéricos:

– Cumpla con los niveles de seguridad definidos en la Política de Seguridad de la organización. No permita que la red de almacenamiento rebaje su nivel de seguridad.

– Cree procesos y procedimientos para la gestión de la solución de almacenamiento.

– Separe físicamente los elementos, como primera medida de seguridad, deshabilitando puertos e interfaces no utilizadas.

– Aplique la "defensa en profundidad" (en capas), combinando el control del tráfico con el reforzamiento de los equipos.

– Proteja los datos en tránsito (IPSec, FCSec) y en el almacenamiento (si es pertinente, utilizando soluciones de cifrado).

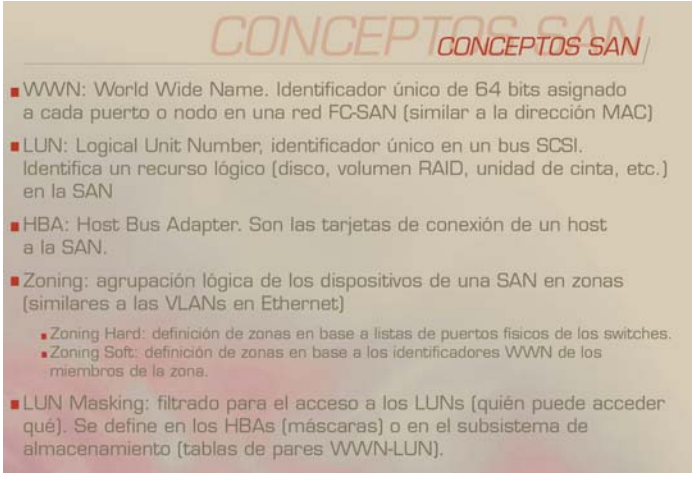
– Implemente soluciones basadas en estándares (ANSI/T11, IETF). Seleccione soluciones maduras, estables e interoperables.

– Audite, y habilite la auditoría, activando la emisión y recogida de trazas de información.

– Securice convenientemente la gestión de la solución, separando la red de gestión de la red corporativa y cifrando las comunicaciones en dicha red, usando mecanismos de autenticación fuerte en el control de acceso a las consolas de gestión, y deshabilitando aquellas interfaces poco seguras (telnet, HTTP, SNMP).

Conclusiones

Actualmente las redes de almacenamiento son un recurso insustituible, ya que ofrecen un entorno escalable con el que satisfacer la creciente y continua demanda de almacenamiento de las empresas. Considerando, por tanto, indispensable su despliegue, debemos pues centrarnos en la mitigación de los riesgos asociados a su implantación.



Como parte de los recursos de la organización, las redes de almacenamiento deben cumplir con la Política de Seguridad corporativa. Por tanto, antes de desplegar una, es imprescindible analizar detalladamente qué requisitos de seguridad tenemos (tanto autoimpuestos, como por la normativa vigente de aplicación) y qué tecnología nos los puede proporcionar, seleccionando productos y tecnologías que, de partida, ofrezcan una correcta implementación de los protocolos y estándares de seguridad aplicables.

Los mecanismos de seguridad de las redes de almacenamiento son actualmente limitados, y es por ello que debemos complementarlos con:

– Unos correctos procedimientos y documentación del despliegue, operación y mantenimiento del sistema.

– Técnicas tradicionales de seguridad, como el cifrado, la seguridad en profundidad o los sistemas de alerta.

– Integración en el plan de contingencia de la organización

– La correcta formación de los responsables de O&M de los sistemas.

Siendo como es un campo emergente y en rápida evolución es de esperar importantes adiciones y mejoras a los mecanismos de seguridad actualmente disponibles. ■

Como los mecanismos de seguridad de las redes de almacenamiento son actualmente limitados, hay que complementarlos con una correcta procedimentación y documentación del despliegue, operación y mantenimiento del sistema, con técnicas tradicionales de seguridad, integrándolas en el plan de contingencia de la organización, y con una correcta formación de los responsables de O&M de los sistemas.

Antonio Requejo Novella
Director de la División de Seguridad
arequejo@germinus.com
Javier Zamorano Sáiz
Director de la División de Infraestructuras
jzamorano@germinus.com
GERMINUS

REFERENCIAS

– "Securing Storage Networks", @Stake, Abril 2003
– "Storage Security Handbook", Neoscale Systems
– "Best Practices for Managing a Secure Enterprise Storage Network" EMC2
– "The Emerging Storage Security Challenge", Yankee Group, Septiembre 2003
– IP Storage Working Group, Internet Engineering Task Force
– "Using SANs and NAS", W. Curtis Preston
– "The Best Practices for Ensuring Enterprise Storage Security", Storage Security Industry Forum SSIF/SNIA, febrero 2003 ssifchair@snia.org
– «Securing Block Storage Protocols over IP», IP Storage Working Group, Internet Engineering Task Force, [http://www.ietf.org/internet-drafts/draft-ietf-ips-security-19.txt]
– Storage Networking Industry Association [http://www.snia.org]
– Association of Storage Networking Professionals [http://www.asnp.com]
– ANSI T11.3 Security Working Group [http://www.t11.org]
– [http://www.sansecurity.com]
– Fabricantes:
  • HBAs: Qlogic, Emulex, JNI
  • Switches: Brocade, McData
  • Software: Veritas, TAS, Legato (EMC)
  • Almacenamiento: EMC, Sun, HP, IBM, Storagetek