GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-408)

SEGURIDAD PERIMETRAL
(CORTAFUEGOS)

MARZO 2010

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

© Editor y Centro Criptológico Nacional, 2010
NIPO: 076-10-072-4

Tirada: 700 ejemplares
Fecha de Edición: marzo de 2010
Jess García con la colaboración de Carlos Fragoso han participado en la elaboración del presente documento.
Luis Pedro Fabián ha participado en la revisión del documento.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el **Centro Criptológico Nacional** puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Febrero de 2010

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 1
2. OBJETO 1
3. ALCANCE 1
4. CORTAFUEGOS: CONCEPTOS GENERALES 2
4.1. ¿QUÉ ES UN CORTAFUEGOS? 2
4.2. CLASES DE CORTAFUEGOS 3
4.3. ENRUTADORES Y CORTAFUEGOS 3
5. FUNCIONALIDADES DE LOS CORTAFUEGOS 6
5.1. CONTROL DEL TRÁFICO DE RED 6
5.2. REGISTRO DE EVENTOS Y ALERTAS 9
5.3. TRADUCCIÓN DE DIRECCIONES (NAT) 10
5.3.1. NAT Estático 12
5.3.2. NAT Dinámico 12
5.3.3. NAT de Ocultamiento 13
5.3.4. Redirección de Puertos 14
5.3.5. Compatibilidad NAT-Protocolos 14
5.4. FILTRADO DE CONTENIDOS 15
5.5. PREVENCIÓN DE INTRUSIONES 17
5.6. NORMALIZACIÓN DE PAQUETES 17
5.7. DHCP 18
5.8. ALTA DISPONIBILIDAD 18
5.9. BALANCEO DE CARGA 19
5.10. TRANSPARENCIA 19
5.11. SEGURIDAD EN EL ACCESO REMOTO 20
5.11.1. Control de acceso 20
5.11.2. Control de admisión a la red 22
5.11.3. Seguridad en el Acceso: Redes Privadas Virtuales (VPN) 23
6. TIPOS DE CORTAFUEGOS 28
6.1. FILTRADO BÁSICO DE PAQUETES 28
6.2. FILTRADO DE PAQUETES CON ESTADO 29
6.3. FILTRADO DE PAQUETES CON ESTADO E INSPECCIÓN 29
6.4. CORTAFUEGOS A NIVEL DE APLICACIÓN 30
6.5. CORTAFUEGOS TRANSPARENTES 31
6.6. CORTAFUEGOS A NIVEL SISTEMA 31
6.6.1. Sistemas UNIX 31
6.6.2. Sistemas Windows: Cortafuegos personales 31
6.6.3. Buenas Prácticas 32
6.7. CORTAFUEGOS VIRTUALES 32
6.8. SISTEMAS DEDICADOS (APPLIANCE) Y DE PROPÓSITO GENERAL 33
7. DISPOSITIVOS ADICIONALES 34
7.1. SISTEMAS DE DETECCIÓN DE INTRUSIONES 34
7.1.1. IDS a nivel de red 34
7.1.2. IDS a nivel de sistema 35
7.2. SISTEMAS DE PREVENCIÓN DE INTRUSIONES 35
7.3. CONCENTRADORES DE VPN 36
8. CICLO DE VIDA DEL CORTAFUEGOS 36
8.1. DISEÑO 36

8.1.1. Parámetros de Diseño **36**
8.1.2. Elementos de la Arquitectura **39**
8.1.3. Procedimiento de Diseño **40**
8.1.4. Diseños Básicos **42**
8.1.5. Arquitecturas de VPN **46**
8.1.6. Ejemplo de Arquitectura de Seguridad Perimetral Multicapa **48**
8.2. DESPLIEGUE 52
8.2.1. Instalación y Configuración de Sistemas y Dispositivos de Red **52**
8.2.2. Seguridad Física **53**
8.2.3. Configuración de los Cortafuegos **53**
8.2.4. Evaluación de la Configuración del Cortafuegos **54**
8.3. GESTIÓN 54
8.3.1. Administración Remota **54**
8.3.2. Actualizaciones de Software **54**
8.3.3. Procedimientos y Documentación **55**
8.3.4. sUBCONTRATAS **56**
8.3.5. Recuperación ante Incidentes **56**
8.3.6. Seguridad Perimetral a Largo Plazo **58**
8.4. RETIRADA/SUSTITUCIÓN 59
9. RESUMEN DE BUENAS PRÁCTICAS 59

ANEXOS

ANEXO A. CRITERIOS DE ELECCIÓN DE CORTAFUEGOS 62
ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS 64
ANEXO C. REFERENCIAS 69

FIGURAS

Figura 1. Traducción de direcciones (NAT) 11
Figura 2. Traducción de direcciones estática 12
Figura 3. Traducción de direcciones dinámica 13
Figura 4. Traducción de direcciones de ocultamiento 14
Figura 5. Redirección de puertos 14
Figura 6. Filtrado de contenidos en correo electrónico entrante 15
Figura 7. Filtrado de contenidos en acceso web saliente 16
Figura 8. Filtrado de contenidos en correo electrónico entrante con proxy dedicado 16
Figura 9. Filtrado de contenidos en acceso web saliente con proxy dedicado 17
Figura 10. Autenticación mediante un servidor RADIUS 22
Figura 11. Cortafuegos a nivel de aplicación (proxy) 30
Figura 12. Ejemplo de cortafuegos virtual 33
Figura 13. Intranet, DMZ, Internet, Extranet 40
Figura 14. Diseño de red doméstica o de pequeña oficina típica 43
Figura 15. Diseño en tres zonas, con una DMZ 43
Figura 16. Diseño multizona con varios cortafuegos 44
Figura 17. Diseño con dos DMZ y un sólo cortafuegos 44
Figura 18. Diseño con dos DMZ multicapa 45
Figura 19. Arquitectura con dos DMZ en modo "service leg" 46
Figura 20. Cortafuegos sobre VLAN 46
Figura 21. Configuración típica de acceso VPN 47
Figura 22. Concentrador VPN externo 48
Figura 23. Arquitectura de seguridad perimetral multicapa 50

1. INTRODUCCIÓN

1. Asegurar el perímetro es una de las estrategias defensivas más eficaces comúnmente utilizadas desde antaño en el campo de la seguridad. Baste para ello recordar las fortificaciones medievales en las que existía tan sólo un número restringido de puntos de entrada en los que se aplicaba un fuerte control de acceso.

2. Reducir la superficie de exposición, crear puntos controlados de acceso y centrar las defensas en esos puntos permite optimizar la capacidad defensiva. Para reforzar la eficacia de la fortificación existían asimismo, elementos añadidos de seguridad como guardias, fosos, barreras naturales, puertas falsas o perímetros internos a la propia fortificación. También han sido muchas las puertas traseras o poternas construidas por comodidad, y que cuando no fueron debidamente mantenidas en secreto supusieron la caída de fortalezas.

3. El mundo de las tecnologías de la información y las comunicaciones (TIC) ha adoptado estas ideas a lo largo de los últimos años, creando arquitecturas y dispositivos que permitieran realizar las mismas tareas con idéntica eficacia. En el centro de estas tecnologías se encuentran los cortafuegos: **puntos controlados de acceso**.

2. OBJETO

4. El objeto de esta guía es familiarizarse con las distintas tecnologías y estrategias existentes actualmente en el campo de la seguridad perimetral, muy especialmente en el de las tecnologías de cortafuegos, y a partir de aquí ser capaz de seleccionar cuáles de ellas se adaptan mejor a las necesidades concretas de una Organización para poder posteriormente realizar un diseño e implementación que sea lo más óptima posible en términos de arquitectura y procedimientos y que a la vez asegure la perdurabilidad en el tiempo de la seguridad obtenida inicialmente.

3. ALCANCE

5. El presente documento presta especial atención a las tecnologías de cortafuegos, consideradas como la piedra angular de la seguridad perimetral, dejando el estudio del resto de tecnologías para futuras guías de referencia.

6. Queda fuera del propósito de este documento el estudio en profundidad de cada uno de los campos tratados. En cada caso, se hará una breve introducción y se indicará cuáles son los puntos más importantes a tener en cuenta. Al final de este documento se podrá encontrar la bibliografía necesaria para poder abundar en el estudio de cada uno de esos campos.

7. El contenido de esta guía está dirigido a personal técnico o de gestión que necesite tener un conocimiento técnico de las tecnologías de cortafuegos existentes, de las posibilidades de uso de las mismas o de las distintas estrategias para introducirlas de forma conveniente en una Organización.

8. El presente material tratará de forma muy somera temas puramente teóricos tales como protocolos de red, criptografía o conceptos básicos de seguridad por lo que se recomienda un conocimiento previo de los mismos.

9. La referencia a cualquier producto comercial específico, proceso o servicio con nombre comercial, marca fabricante, o de otro modo, no constituye ni implica su respaldo comercial. Los puntos de vista y las opiniones de los autores expresadas en este documento no se utilizarán para fines publicitarios ni de respaldo.

10. La información aquí recopilada puede estar obsoleta en el momento de la lectura del documento.

4. CORTAFUEGOS: CONCEPTOS GENERALES

11. El cortafuegos ha sido considerado tradicionalmente el dispositivo central de protección perimetral. Es importante conocer su papel en la seguridad de las tecnologías de la información y las comunicaciones (STIC) para poder elegir correctamente soluciones que se ajusten a nuestras necesidades y así poder realizar implantaciones que mejoren el estado global de la seguridad dentro de la Organización.

12. Los cortafuegos son el equivalente a las murallas de la antigüedad, dispositivos que separan distintas áreas con distintos requisitos de seguridad o niveles de riesgo y que controlan el flujo de tráfico entre ellas.

13. Además de los cortafuegos, y al igual que sucedía en el caso de las fortificaciones que mencionábamos anteriormente, se han incluido elementos adicionales para hacer posible el incremento de la seguridad proporcionada, ya sea aumentando la “inteligencia” de los cortafuegos en sí mismos o a través de nuevas tecnologías y procesos como el cifrado, los certificados digitales, los sistemas de detección y prevención de intrusiones, los sistemas de análisis de contenidos, etc.

4.1. ¿QUÉ ES UN CORTAFUEGOS?

14. Un cortafuegos (*firewall*) es aquel sistema formado por aplicaciones, dispositivos o combinación de éstos encargado de hacer cumplir una política de control de acceso en las comunicaciones entre dispositivos de red según una política de seguridad existente.

15. Se entiende por políticas de control de acceso las primitivas de "permitir" o "denegar" a determinados clientes el acceso a los recursos de red, expuestos como servicios, según unos privilegios de autorización. Estos privilegios a los recursos u objetos se definen habitualmente mediante listas con entradas secuenciales llamadas juegos de reglas (*rulesets*).

16. Se pueden encontrar muchos tipos de cortafuegos determinados por su ámbito, función, nivel de actuación en la torre de protocolos, inteligencia en la inspección del tráfico, etc. También suelen diferenciarse cualitativamente y cuantitativamente por los servicios o funcionalidades añadidas que proporcionan, tales como traducción de direcciones, redes privadas virtuales, integración de mecanismos de autenticación, etc.

17. Además de la tecnología de filtrado utilizada por un determinado cortafuegos, deben tenerse en cuenta, entre otros, los siguientes parámetros o criterios para su elección dentro de la arquitectura de red:

    – Rendimiento.
    – Disponibilidad.
    – Seguridad.

- Flexibilidad.
- Facilidad de uso y gestión.

18. Es imprescindible que el cortafuegos proporcione trazas de registro (*logs*) lo más completas posible para poder auditar en cualquier momento dicha información y mejorar proactivamente la seguridad perimetral.

4.2. CLASES DE CORTAFUEGOS

19. Se pueden distinguir distintas clases de cortafuegos según el criterio a seguir.
20. Según el ámbito de aplicación encontramos dos tipos:
    - **Cortafuegos de red**: su objetivo es el control del tráfico en tránsito de la red y por ello participa como dispositivo activo en ésta. Permite la gestión centralizada de la seguridad.
    - **Cortafuegos a nivel sistema**: forma parte de una estación de la red, normalmente como aplicación local, e implementa el control del tráfico con origen o destino a dicha estación. Aunque su uso en aproximaciones de seguridad multicapa es una buena práctica de protección, no ha sido ampliamente utilizado. La tendencia está cambiando ya que en el escenario actual de las comunicaciones existe una mayor diversidad y movilidad en la conectividad haciendo la definición del perímetro cada vez más difusa. Es posible realizar una gestión centralizada con el despliegue y las herramientas necesarias.
    -
21. Según su nivel de participación dentro de la torre de protocolos OSI, se realiza una de las principales clasificaciones entre los cortafuegos existentes. Aunque encontramos inevitablemente soluciones híbridas, a grandes rasgos podemos diferenciar los tipos:
    - **Nivel de enlace de datos** (nivel 2). Permite filtrar por direcciones MAC. Hasta hace poco era extraño encontrar filtros basados en este nivel, pero han ido ganando popularidad al mejorar las prestaciones de seguridad de los dispositivos de red basados en esa capa, como por ejemplo los conmutadores Ethernet.
    - **Nivel de red** (nivel 3). Permite filtrar por direcciones IP.
    - **Nivel de transporte** (nivel 4). Permite filtrar por protocolo (TCP, UDP) y puertos. Estos cortafuegos también suelen permitir realizar NAT, lo que supone otra capa de defensa.
    - **Nivel de aplicación** (nivel 7). Permite filtrar por características propias de un protocolo, bloqueando o cambiando el resultado, por ejemplo, determinadas peticiones DNS o URL en la navegación web. Pueden realizar tareas de *Proxy*.

4.3. ENRUTADORES Y CORTAFUEGOS

22. Gracias al aumento de potencia de las plataformas hardware actuales, a menudo se entremezclan las funciones de los enrutadores (*routers*, *switches*) y de los cortafuegos. No obstante, las capacidades de los enrutadores están orientadas a realizar su función característica (enrutar) de forma eficiente y puede verse seriamente afectada si se les

fuerza a realizar tareas demasiado exhaustivas como las típicamente realizadas por un cortafuegos (filtrado excesivo o excesivamente complejo).

23. Los enrutadores por su localización dentro de la infraestructura, especialmente los de perímetro o *border routers*, son un punto privilegiado donde filtrar tráfico claramente malicioso. Es por tanto recomendable, y aliviará a los siempre sobrecargados cortafuegos, utilizar los enrutadores para realizar un filtrado simple de tráfico (a nivel de red, por ejemplo) o incluso explotar las características más avanzadas que pueda proporcionar siempre y cuando estas tareas no perjudiquen su labor fundamental de enrutar eficientemente los paquetes.

24. Siempre que sea posible, el grueso de la tarea de control del tráfico debe recaer de forma natural en los cortafuegos, dado que habitualmente tienen la posibilidad de analizar el tráfico en más profundidad.

25. A la hora de proteger el tráfico propio es imprescindible conocer su tipología: protocolos permitidos, rangos de direccionamiento permitidos, etc. Suele ser habitual implantar equipos de enrutamiento en entornos de producción sin este conocimiento previo y ello implica un esfuerzo de corrección posterior.

26. Hay dos estrategias fundamentales para proteger la red utilizando enrutadores:
    - **Filtrado**: permitir o denegar el tráfico.
    - **Conformado/Limitado**: mecanismos de calidad de servicio consistentes en la definición de umbrales de tolerancia a partir de los cuales se aplican medidas sobre el tráfico como puede ser descartarlo.

27. Para el filtrado de tráfico podemos combinar los siguientes mecanismos:
    - **Listas de acceso** (*ACL*): permiten realizar el filtrado de tráfico con una alta granularidad. Es un filtrado basado en direcciones IP de origen y de destino, y en protocolo.
    - **Filtrado de camino inverso** (*Reverse Path Filtering – RPF*): permite verificar todo el tráfico de entrada de un interfaz, comprobando que las direcciones de origen son conocidas mediante la tabla de enrutamiento (*Routing Information Base – RIB*). Es un filtrado basado en direcciones IP de origen.
    - **Rutas de descarte** (*null routes*): permite enviar el tráfico especificado a una interfaz virtual de descarte. Se implementa modificando la tabla de enrutamiento. Es un filtrado basado en la dirección IP de destino.

28. En los dispositivos de enrutamiento perimetral suele aplicarse un filtrado conocido como **de entrada/salida** (*ingress/egress*) de manera que sean el primer punto de control del tráfico. Para un rendimiento óptimo, lo habitual es filtrar en el interfaz más cercano, es decir, el tráfico de salida hacia Internet filtrarlo en el interfaz interno y el tráfico de entrada de Internet filtrarlo en el interfaz externo.

29. Es habitual filtrar el tráfico dirigido a las direcciones de interfaz de los equipos de red, conocidas como direcciones de “infraestructura”, permitiendo sólo el tráfico de control necesario:
    - Listas de acceso de tránsito:
        - Denegar la entrada y salida de direcciones marcianas (*martians*) de uso especial. Son direcciones marcianas todas aquellas que por su asignación no

pueden generar tráfico Internet válido (y, por lo tanto, seguramente enmascaran tráfico ilícito), incluyendo:

- **RFC 3330** ([Ref.- 39]): Direcciones reservadas por IANA. (0.0.0.0/8, 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.0.2.0/24, 192.88.99.0/24, 198.18.0.0/15, 192.168.0.0/16, 224.0.0.0/4, 240.0.0.0/4)
- **RFC 3232** ([Ref.- 40]): Este documento sustituye a la RFC 1700 ([Ref.- 37]) y establece una base de datos online y en continuo cambio como referencia obligada para la asignación de los rangos de direcciones IP por IANA ([Ref.- 44]).
- Otras RFC cuyo contenido está incluido en las anteriores, como la RFC 1918 ([Ref.- 38]) sobre Espacio privado de direcciones (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16) y la RFC 3927 ([Ref.- 41]) sobre direcciones para enlace dinámico local (169.254.0.0/16).

- Denegar la entrada y salida de tráfico originado en direcciones válidas pero que no están en uso (no asignadas o *unallocated*).
- Denegar la entrada de tráfico con nuestras direcciones y la salida de tráfico no originado con nuestras direcciones RFC2827, es decir tráfico cuya IP de origen no se corresponde del segmento de red del que procede (técnicas *anti-spoofing*).
- Permitir explícitamente el tráfico de retorno hacia nuestras direcciones y de salida originado con nuestras direcciones.
- Denegar explícitamente el tráfico restante.

– Listas de acceso de protección de infraestructura:
  - Permitir el tráfico de gestión y monitorización necesario
  - Permitir el tráfico de los protocolos de enrutamiento y de red necesarios.

30. Jamás deberían verse en Internet IP marcianas o no asignadas, lo que se conoce por el nombre de *bogons*[1]. Es importante mantener esta lista, ya que IANA, repetidamente durante el año, asigna nuevos rangos a los registros regionales para que puedan ser utilizados.

31. Es habitual protegerse limitando el máximo tráfico de tipo UDP e ICMP a transitar. Esto es muy dependiente del entorno, pero habitualmente la distribución de tráfico suele ser de un 85% TCP, 10% UDP y el restante 5% ICMP. Los umbrales suelen dimensionarse en función de la capacidad del enlace.

32. Las listas de acceso necesarias para dar transito a las redes propias serían:

– Filtro de entrada en interfaz externo:
  - Denegar direcciones de origen marciano o no asignado (*bogon*).
  - Denegar tráfico originado con nuestras direcciones.

[1] Consultar la sección "*Bogon Reference Page*" de la página web del Team Cymru ([Ref.- 42]) para obtener información actualizada o suscribirse a una lista de notificación de cambios. También se puede encontrar información al respecto en las bases de datos de registro de routing como la de RADB (*Routing Assets DataBase*) de la red americana MERIT ([Ref.- 43]) accesible mediante "whois": whois.radb.net fltr-bogons / fltr-martians / fltr-unallocated.

- Denegar puertos habitualmente atacados/escaneados (alivia al cortafuegos del ruido de la red) teniendo la precaución de no bloquear ningún puerto crítico para la Organización.
- Permitir tráfico TCP, UDP, ICMP y resto de protocolos que se utilicen en la Organización con destino a nuestras direcciones.
- Denegar el tráfico restante.

– Filtro de entrada en interfaz interno:
  - Permitir tráfico de gestión hacia el equipo desde nuestras direcciones.
  - Permitir tráfico TCP, UDP e ICMP y resto de protocolos que se utilicen en la Organización originado desde nuestras direcciones.
  - Denegar el tráfico restante.
  - No es necesario filtrar las direcciones *bogon* de destino debido a que será realizado por las rutas estáticas de descarte y tampoco se filtran los puertos más explotados/escaneados ya que se realiza mediante política en el cortafuegos.

5. FUNCIONALIDADES DE LOS CORTAFUEGOS

33. Ya se ha mencionado que el cortafuegos es el principal elemento en la estrategia de seguridad perimetral. En sus orígenes, la labor del cortafuegos se centraba simplemente en el control del tráfico de red de una forma muy simple.

34. Sin embargo, con el tiempo fueron adquiriendo más funciones, ya fuera porque entraban dentro de los cometidos de seguridad que le correspondían (autenticación y autorización) o porque el cortafuegos era el lugar adecuado para su implementación debido a su posición en la infraestructura de red, aunque se tratara de funcionalidades no relacionadas directamente con la seguridad (como NAT o traducción de direcciones).

35. A continuación se enumeran las principales funcionalidades presentes en los cortafuegos.

5.1. CONTROL DEL TRÁFICO DE RED

36. El control del tráfico de red es una de las principales funciones de los cortafuegos. De acuerdo con el papel que le corresponde dentro de la seguridad perimetral, el cortafuegos es el encargado de controlar el flujo de tráfico entre dos entornos con niveles de seguridad distintos, ya sea internamente a la Organización o entre la Organización y el mundo exterior.

37. Llevar a cabo este control puede ser algo bastante complejo. En el caso más simple, el de filtro de paquetes, el cortafuegos analizará cada paquete que llega hasta él y verificará su cabecera analizando varios parámetros, típicamente los siguientes:

– Dirección de origen.
– Dirección de destino.
– Protocolo.
– Puerto de origen.
– Puerto de destino.

38. Una vez obtenida esta información se aplica la política de seguridad, habitualmente en forma de reglas de filtrado, y se determinará si se debe permitir o denegar el paso del paquete en cuestión.

39. Esta aproximación tan sencilla, basada tan sólo en unos pocos parámetros de la cabecera de los paquetes, resulta insuficiente a la hora de tratar determinados protocolos de red complejos (como FTP o H.323) en los que se establecen varias conexiones en paralelo relacionadas y en los que no es posible determinar toda la información acerca de las mismas a partir de sólo la cabecera.

40. También resulta insuficiente a la hora de detener ataques que se aprovechen de la falta de conocimiento del cortafuegos sobre el estado de la conexión para destruirla, o aún peor, para introducirse en medio de la misma o incluso secuestrarla.

41. Como respuesta a estos problemas se ha ido dotando paulatinamente a los cortafuegos de la capacidad de poder almacenar el estado de las conexiones y de intervenir el contenido de los paquetes y no tan sólo de su cabecera, para así "entender" la situación y poder actuar en consecuencia. Todo esto ha dado lugar a distintas generaciones y tipos de cortafuegos que serán tratados más adelante en este documento.

42. En cualquiera de los casos, para poder llevar a cabo el control del tráfico de red se utilizan reglas como las que mencionábamos anteriormente. Un ejemplo de regla que permitiera el tráfico de correo (tcp/25) a un servidor de la Organización (1.2.3.4) sería:

Protocolo	*Dir. Origen*	*Puerto Origen*	*Dir. Destino*	*Puerto destino*	*Acción*
tcp	cualquiera	Cualquiera	1.2.3.4	25	aceptar

43. Pero las reglas no se presentan de forma aislada sino como un conjunto de ellas, conocido a menudo como "juego de reglas", que actúan como un todo para implementar la política de seguridad. Volviendo al ejemplo anterior, el siguiente juego de reglas permitiría el tráfico al servidor de correo, así como tráfico web HTTP (tcp/80) y HTTPS (tcp/443) al servidor web (1.2.3.5) y denegaría el resto del tráfico

Protocolo	*Dir. Origen*	*Puerto Origen*	*Dir. Destino*	*Puerto destino*	*Acción*
tcp	cualquiera	cualquiera	1.2.3.4	25	aceptar
tcp	cualquiera	cualquiera	1.2.3.5	80	aceptar
tcp	cualquiera	cualquiera	1.2.3.5	443	aceptar
tcp	cualquiera	cualquiera	cualquiera	cualquiera	denegar

44. Con este ejemplo tan simple se puede observar que los juegos de reglas pueden llegar a ser muy complejos, lo que puede dar lugar a errores de configuración. Por tanto, resulta vital ser extremadamente cuidadoso y ordenado e introducir comentarios sobre qué función tiene cada regla en el conjunto del juego.

45. Los juegos de reglas son la forma de plasmar la política de seguridad en lo que a tráfico se refiere. Hay una serie de reglas que normalmente se recomiendan para cualquier configuración:

    – Acceso administrativo al cortafuegos (Bloqueo del Cortafuegos).

      Ningún Sistema debería tener acceso al cortafuegos principal o *gateway* salvo el utilizado para su administración. Dado que el *gateway* es un elemento crítico a

proteger, debemos estar plenamente seguros de que ningún paquete no deseado llegará al mismo como resultado de un error de configuración.

Con esta regla, a menudo conocida como Bloqueo del Cortafuegos o *Firewall lockdown*, prohibiremos expresamente todo tráfico al *gateway* salvo el proveniente de los puestos administrativos, desde los cuales admitiremos el tráfico relacionado con los protocolos necesarios para la gestión del cortafuegos, ya sean los propietarios del producto cortafuegos en cuestión u otros generales como SSH.

– Tráfico sin registro.

A menudo hay un conjunto de tráfico del que no interesa guardar registro. Es el caso de algunos tipos de tráfico asociados a la actividad normal de la red y que pueden resultar especialmente ruidosos para las trazas de registro (*logs*).

Este tipo de tráfico no aporta, en general, información interesante acerca de la actividad del cortafuegos y sin embargo puede hacer que los ficheros de registro se llenen rápidamente. Con esta regla, en ocasiones conocida como *No Logging*, conseguiremos mejorar la eficiencia de las capacidades de registro.

Algunos ejemplos de este tipo de tráfico son:

- *Broadcast*. Este tráfico es preferible dejarlo pasar.
- *identd* hacia servidores de correo o proveniente de servidores IRC. Tras una conexión smtp a un servidor de correo, es habitual en numerosos paquetes populares de software de correo que el MTA remoto inicie una conexión al puerto identd de nuestro servidor. No es deseable tirar (*drop* en las reglas) los paquetes de identd dado que esto introduce un retraso apreciable en el despacho del correo. Es más recomendable por tanto rechazar (*reject* en las reglas) este tráfico.

– Registro del tráfico denegado.

Es muy conveniente garantizar que se guarda registro del tráfico que el cortafuegos deniega, excepto en el caso de algunos tipos de tráfico "ruidoso". Se aconseja al final del juego de reglas se incluya una regla que deniegue el resto del tráfico y que guarde un registro del mismo. Esta regla es conocida en ocasiones como *Log Denied*.

– Tráfico desde la *DMZ*.

La DMZ es una red de servidores desde la cual no se debería originar ningún tráfico. Si este tráfico se produce podría ser un claro indicio de intrusión. Se recomienda introducir una regla, en ocasiones conocida como *Sneaky Rule*, que alerte en caso de que se produzca esa situación.

Esto es aplicable también a cualquier otra red, DMZ o no, desde la cual no esperemos recibir tráfico hacia otras redes y que no sea particularmente "ruidosa", en especial redes expuestas o especialmente sensibles.

46. Muchos productos de cortafuegos incluyen de fábrica una serie de reglas implícitas que suelen permitir determinado tráfico, por ejemplo administrativo, y que no aparecen claramente definidas en el juego de reglas por defecto. Es importante que el administrador se familiarice con las características de cada cortafuegos en uso, investigar si existen este tipo de reglas y en último término hacer una verificación de los puertos que

son accesibles desde cada uno de los interfaces utilizando un programa rastreador de puertos.

47. El juego de reglas estándar deberá de plasmar claramente la política de seguridad en el *gateway*. Es importante seguir un proceso cuidadoso para no cometer errores, dado que la correcta selección de todas las propiedades de las reglas, así como su orden, es un trabajo delicado. Es también especialmente importante documentar claramente la utilidad de cada una de las reglas, muy en particular aquellas que no sean evidentes, utilizando tanto comentarios como documentación externa.

48. El juego de reglas de un cortafuegos en producción puede llegar a tener decenas de reglas, y suele dar lugar a fallos de configuración. Para luchar contra esto, el orden, la documentación y las inspecciones son las mejores armas.

49. Es importante también ser lo más escrupuloso posible con el juego de reglas definido, restringiendo origen y destino según sea estrictamente necesario. Esto puede aumentar la cantidad de trabajo administrativo, pero sin duda es la mejor aproximación de cara a garantizar la seguridad de las redes.

50. Obtener la mejor eficiencia posible es importante en un cortafuegos, tanto más importante cuanto mayor sea la carga que soporte. Las reglas más usadas deben ser situadas lo más al principio posible según el orden de ejecución, y análogamente situar las menos usadas al final. Esto mejorará claramente la eficiencia dado que el cortafuegos tendrá que procesar menos reglas.

5.2. REGISTRO DE EVENTOS Y ALERTAS

51. Un aspecto fundamental de la seguridad perimetral consiste en verificar los mensajes registrados por los distintos componentes de la misma, en especial los cortafuegos. El principal papel de los cortafuegos es garantizar que la política de seguridad de la Organización se cumple, por lo que los mensajes emitidos por los mismos indican violaciones de dicha política de seguridad[2].

52. Es fundamental revisar periódicamente los *logs* o registros de todos los sistemas que conforman la seguridad perimetral. La periodicidad dependerá de las capacidades de la Organización, pero es recomendable hacerlo al menos una vez al día, aunque en Organizaciones con altos requisitos de seguridad se puede tener un equipo dedicado a esta función en tiempo real o se puede considerar la externalización.

53. La información obtenida de las interfaces expuestas a Internet sirve en ocasiones para poco más que realizar estadísticas de ataque, debido el elevado "ruido de fondo" existente (gusanos, ataques indiscriminados, barridos de red, etc.) y la cantidad de mensajes que se generan.

54. Los mensajes procedentes de zonas controladas, como la DMZ o las redes internas, sí deben vigilarse, prestando especial atención a las zonas particularmente sensibles o expuestas de la Organización. Con una configuración adecuada, un cortafuegos puede hacer una excelente labor de detección de intrusiones. La detección a tiempo de un compromiso en un Sistema puede evitar que el incidente llegue a ser crítico para la Organización.

[2] Una referencia para interpretar algunas de las entradas típicas en los registros de eventos (*logs*) de un cortafuegos se puede encontrar en: http://www.robertgraham.com/pubs/firewall-seen.html

55. El volumen de mensajes de registro generados por un solo cortafuegos es enorme. Además, una Organización típica suele contar con varios cortafuegos y demás elementos de seguridad perimetral, en ocasiones un gran número. Para resolver este problema, se deben establecer los siguientes mecanismos:

    – **Centralización de los registros de eventos**: La mayor parte de los sistemas y dispositivos de hoy en día, cortafuegos incluidos, permiten la redirección de los eventos a un sistema remoto, además de guardar los mismos localmente. El estándar para este registro remoto es del mundo UNIX, *syslog*, y la mayor parte de los dispositivos de red y sistemas operativos suelen poder ser configurados de un modo u otro para enviar las alertas remotamente utilizando este sistema

    – **Análisis automatizado de los registros**: Existen tanto en el mundo del código abierto como en el mundo comercial diversos sistemas para la clasificación y el análisis de los eventos de registro, y algunos de ellos especialmente orientados al análisis de los registros de los cortafuegos. Un caso particular de los mismos son los sistemas de gestión de eventos de seguridad (*SEM - Security Event Managers*). Estos sistemas suelen tener un precio elevado pero están diseñados para aceptar, gestionar y correlar un elevado volumen de eventos de multitud de dispositivos distintos, por lo que suelen resultar muy útiles en Organizaciones de gran tamaño.

    – **Generación automática de alertas** para eventos que representen ser un claro indicio de un incidente de seguridad.

56. Otras buenas prácticas en la gestión de logs son:

    – Almacenarlos fuera del propio cortafuegos. Si el equipo es comprometido, pueden ser eliminadas las trazas que permitan identificar el incidente y reaccionar adecuadamente. En el caso de centralizar los logs, este problema queda resuelto.

    – Asegurar que se use un canal seguro (cifrado o fuera de línea) para transmitir los logs. Los mensajes de registro del cortafuegos contienen habitualmente información sensible, desde información de autenticación hasta información sobre violaciones de la política de seguridad (información que eventualmente puede ser usada por ejemplo para hacer ingeniería inversa del juego de reglas del cortafuegos).

    – Definir una política adecuada de rotación, análisis y archivo de los registros.

    – Aplicar a los registros de eventos las correspondientes medidas de seguridad física y copias de seguridad. Muchas Organizaciones están obligadas por ley a guardar sus logs durante un período variable de tiempo, en ocasiones para siempre.

57. Aunque algunos dispositivos de seguridad perimetral lo permiten, no se recomienda programar medidas automáticas reactivas tras la detección de un incidente de seguridad, tales como bloquear el tráfico a la dirección de origen. Este tipo de medidas son habitualmente más perjudiciales que beneficiosas, dada la facilidad con que se puede falsificar el origen del incidente, pudiendo resultar en una denegación de servicio a sistemas no hostiles.

5.3. TRADUCCIÓN DE DIRECCIONES (NAT)

58. La traducción de direcciones, habitualmente conocida como *NAT* (*Network Address Translation*) o enmascaramiento IP, nació con la principal motivación de paliar los efectos de la escasez de direccionamiento que sufre la Internet actual (basada mayoritariamente en IPv4) tras su crecimiento explosivo, hasta que se implemente con una solución a largo plazo como IPv6.

59. La traducción de direcciones consiste en utilizar un dispositivo de red, típicamente un cortafuegos o un *router*, para modificar la dirección de IP de origen o destino de los paquetes.

60. Esta técnica se puede utilizar por diferentes motivos:

- Traducción de direccionamiento privado a direccionamiento público (NAT estático y dinámico).
- Facilidad en la gestión del espacio de direccionamiento, incluyendo:
  - Balanceo de IP entre distintos servidores y alta disponibilidad.
  - Proveimiento de varios servicios en distintos servidores y puertos a través de una sola IP (Redirección de puertos).
- Ocultación del direccionamiento interno y conexión de múltiples servidores o estaciones clientes a una red externa a través de una sola IP (NAT de ocultamiento).

61. En la **Figura 1** , se indica un ejemplo típico de traducción de direcciones conocido como "ocultamiento" o Hide NAT que se tratará en detalle más adelante. Se observa cómo los paquetes generados por los sistemas de la red 10.0.0.0/8 son traducidos a la dirección 1.2.3.4. Tanto el enrutador como el cortafuegos serían posibles candidatos para realizar la traducción de direcciones.

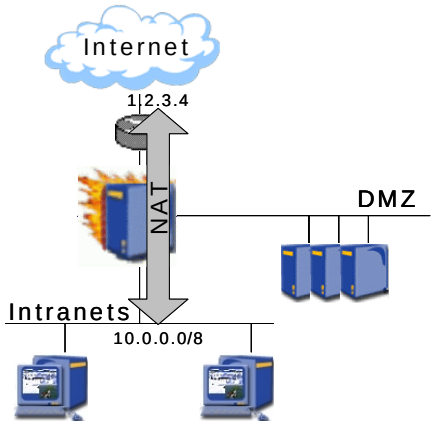

Figura 1. Traducción de direcciones (NAT)

62. **No se debe considerar al NAT como un mecanismo de seguridad**, aunque se obtengan ciertos beneficios derivados de la ocultación del espacio de direcciones interno. Además, al ser un mecanismo que modifica las cabeceras, se está rompiendo uno de los principales beneficios de las comunicaciones IP en la red: “comunicación extremo a extremo”.

63. Debe garantizarse que el dispositivo inmediatamente anterior Si el dispositivo que realiza NAT en la cadena de enrutamiento (normalmente un *router*), es capaz de hacer llegar al mismo los paquetes destinados a las IP traducidas. En una configuración estándar, localizará dinámicamente al dispositivo que realiza NAT usando las peticiones ARP correspondientes. Si el dispositivo que realiza NAT utiliza una dirección IP distinta de las que tiene asignadas en sus interfaces, no podrá concluirlo de forma satisfactoria, al no estar configurado para responder a esas peticiones ARP.

64. Las dos formas más habituales de resolver este problema son:

- Introducir una ruta estática en dicho dispositivo para indicarle que el siguiente paso en la cadena de enrutamiento para llegar a la dirección traducida es el cortafuegos. Suele ser la más recomendable si se posee control sobre el dispositivo inmediatamente anterior en la cadena de enrutamiento.
- Configurar el cortafuegos para que haga *proxy-arp*, es decir, para que responda a esa dirección IP como si fuera suya.

65. A continuación se describen los distintos tipos de NAT existentes que podemos combinar para abordar diferentes situaciones o suplir ciertas carencias.

5.3.1. NAT ESTÁTICO

66. Este tipo de traducción de direcciones permite realizar un mapeado predefinido y permanente entre dos direcciones IP, una interna y una externa, creando una correspondencia unívoca entre ambas.

67. El mecanismo de traducción estático permite una mayor flexibilidad en la gestión del espacio de direcciones ya que podemos fácilmente cambiarlas y dirigirlas, en cada momento, a los sistemas que por conveniencia o disponibilidad deban ser "visibles".

68. El NAT estático, menos potente que la Redirección de Puertos que se explica más adelante, se suele utilizar con algunos protocolos que experimentan problemas con la redirección de puertos siempre que se cuente con las suficientes IP externas..

69. En la **Figura 2**, se ve un ejemplo de traducción estática de direcciones. El tráfico generado por un sistema que en la red interna tiene la dirección privada no enrutable 10.1.2.3, que tras atravesar un cortafuegos que realiza NAT se convierte en la dirección enrutable 1.2.3.4. Este ejemplo, se podría corresponder con la situación típica en la que se dispone de un servidor con direccionamiento privado (web, correo, etc.) cuyos servicios deben exponerse en Internet.

Figura 2. Traducción de direcciones estática

5.3.2. NAT DINÁMICO

70. El NAT dinámico, también conocido como *Pool NAT*, consiste en la traducción de una dirección IP interna (privada) a una dirección IP externa (pública) seleccionada dinámicamente dentro de un grupo de direcciones disponibles (pool) reservadas para este propósito, creando una correspondencia temporal una a una. Esa correspondencia suele liberarse cuando no hay tráfico en ninguno de los dos sentidos durante un tiempo pre-establecido. Una vez liberada, una nueva petición generaría una nueva relación.

71. Este tipo de traducción de direcciones permite dar una conectividad total extremo a extremo de manera temporal a dispositivos cliente que utilizan direcciones privadas. No tiene sentido aplicar ésta modalidad a servidores, ya que la relación IP pública-IP-privada se establece cuando hay comunicación, y ésta nunca se produciría al no poder acceder los clientes de IP pública a la IP pública del servidor.

72. El NAT dinámico, menos potente que el NAT de ocultamiento que se explica más adelante, se suele utilizar con algunos protocolos que experimentan problemas con el NAT de ocultamiento.

73. En la **Figura 3**, se puede señala un ejemplo en el que un servidor interno con dirección 10.1.2.3 accede al exterior a través de un cortafuegos que realiza NAT dinámico. Este cortafuegos dispone de tres direcciones externas para ser asignadas a clientes internos que necesiten alcanzar el exterior. En este caso la primera dirección (1.2.3.4) se encuentra asignada a algún otro sistema, por lo que el cortafuegos le asigna la siguiente dirección disponible (1.2.3.5) con la cual el sistema interno accederá al exterior.

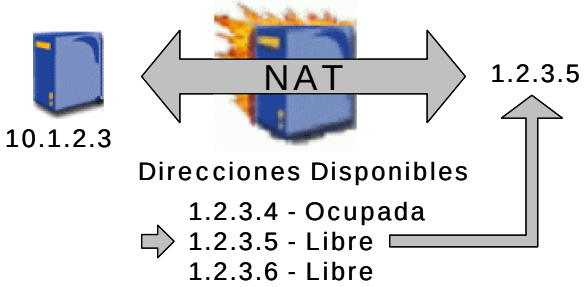

Figura 3. Traducción de direcciones dinámica

5.3.3. NAT DE OCULTAMIENTO

74. El NAT de ocultamiento, conocido también como NAT de sobrecarga o *Hide NAT*, consiste en la multiplexación de las comunicaciones de un grupo de direcciones IP privadas en tan sola una dirección IP, estableciéndose de esta forma una correspondencia de N direcciones a una. Una explicación simplificada consiste en describirlo como un NAT dinámico que, en vez de establecer relaciones IP a IP, establece relaciones IP-puerto a IP-puerto, mapeando el puerto origen del sistema interno a uno nuevo, tanto sobre TCP como UDP.

75. Este proceso es muy utilizado pues permite ahorrar direcciones públicas al ser compartidas por varias estaciones de trabajo,

76. Desde el momento en que el paquete atraviesa el dispositivo hacia el exterior se sustituyen las direcciones privadas por una única pública y el puerto origen por uno asignado dinámicamente. Cuando llega un paquete de respuesta, se verifica cuál es el puerto de destino, se consulta la tabla de traducciones para saber qué sistema inició esa conexión y desde qué puerto originalmente, y se realiza una traducción de manera inversa a como se realizó anteriormente, enviando el paquete así generado al sistema en cuestión.

77. Para evitar los problemas que pueden sufrir algunos protocolos que necesitan mantener el puerto o que distintas comunicaciones compartan IP, algunos dispositivos disponen de la posibilidad de funcionar con NAT dinámico y sólo activar el NAT de ocultamiento en caso de que en algún momento se agote el rango de direcciones de traducción.

78. En la **Figura 4**, se puede observar un ejemplo de NAT de ocultamiento en el que la red interna 10.0.0.0/8 saldrá al exterior con la dirección 1.2.3.4.

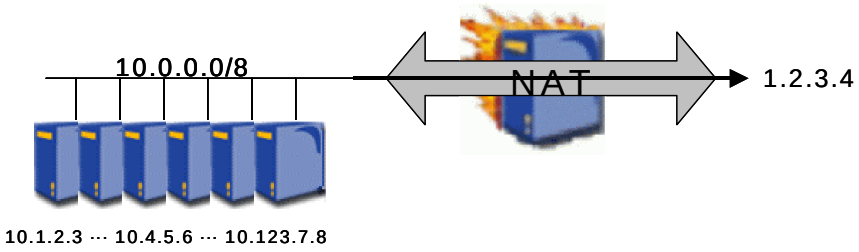

Figura 4. Traducción de direcciones de ocultamiento

5.3.4. REDIRECCIÓN DE PUERTOS

79. La redirección de puertos (*port forwarding*) es una versión estática del NAT de ocultamiento que permite dar visibilidad exterior a servicios concretos. Para ello se realiza el mapeo estático de un puerto de transporte TCP o UDP en el sistema hacia el mismo u otro puerto en la dirección IP pública utilizada para el NAT de ocultamiento.

80. Este tipo de NAT ofrece la ventaja de permitir exponer servicios concretos sin tener que sacrificar totalmente una dirección IP para ello.

81. En la **Figura 5**, se ilustra un ejemplo en el que dos sistemas internos que ofrecen servicios de correo y web respectivamente en sus puertos estándar (TCP/25 y TCP/80) son sometidos a redirección de puertos al atravesar un cortafuegos, de manera que el servidor de correo es accesible en el puerto TCP/25 de la dirección externa 1.2.3.4 y el servidor web es accesible a través del puerto no estándar TCP/8080.

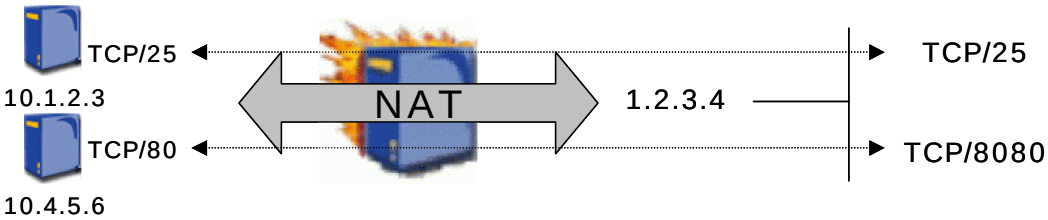

Figura 5. Redirección de puertos

5.3.5. COMPATIBILIDAD NAT-PROTOCOLOS

82. Existen muchos protocolos y aplicaciones que se ven afectados seriamente por el mecanismo de traducción de direcciones, como en el caso en que la dirección IP del sistema original está incluida no sólo en la cabecera sino también en el cuerpo de los paquetes y el protocolo hace uso de esa información.

83. Una solución ampliamente utilizada consiste en la utilización de **proxies de protocolo**. Se trata de programas que actúan de intermediarios a nivel 7 de aplicación, de tal manera que cuando reciben una petición de conexión desde un cliente realizan una nueva petición al servidor, estableciendo en la práctica dos conexiones independientes y actuando de pasarela en lo que a peticiones y respuestas se refiere. Dado que en este punto existen dos conexiones y ninguna de las dos está sometida a NAT, no se presentan los problemas descritos anteriormente.

84. Otra solución que se está asumiendo pasa por la definición de **protocolos que se adaptan dinámicamente** si detectan que se encuentran tras un dispositivo NAT, como es el caso de Simple Transversal of UDP through NATs (STUN).

5.4. FILTRADO DE CONTENIDOS

85. Cuando las Organizaciones empiezan a perfilar su política de seguridad con respecto al uso aceptable de sus sistemas y redes, surgen necesidades acuciantes, entre las que se encuentran:

– la necesidad de establecer un control para verificar que la política es respetada o incluso para hacerla cumplir de forma obligada.

– la necesidad de filtrar el posible contenido malicioso que pudiera introducirse en la Organización debido a la acción del usuario, como la apertura de adjuntos de correo electrónico o la visita de sitios web con contenido activo malicioso o prohibido.

86. Fruto de estas dos necesidades nacieron los sistemas de filtrados de contenidos. Gracias a la posición estratégica que ocupan los cortafuegos en la red, muchas veces se utilizan para llevar a cabo dicho filtrado. Estamos hablando, como se especificó en el apartado 4.2. CLASES DE CORTAFUEGOS, de filtrado a nivel de aplicación (nivel 7).

87. La tarea de filtrado puede ser altamente intensiva, por lo que en general es deseable descargar el peso de su procesado en un servidor paralelo al que el cortafuegos pueda recurrir cuando necesite verificar el contenido de alguna transacción.

88. Existen productos que se encargan de llevar a cabo de forma especializada dicha función en colaboración con el cortafuegos: antivirus que verifican el tráfico de correo, web, FTP, P2P, etc.; *antispam* y *spyware*; filtrado de contenido de web activo (ActiveX, Java, etc.); o filtrado de URLs que puedan ir en contra de la política de seguridad de la Organización.

89. Dado que el contenido está en continua evolución, este tipo de funcionalidades sólo son realmente eficaces si se cuenta con actualizaciones periódicas, por lo que debe contarse con un contrato de soporte.

90. En la **Figura 6** se puede observar cómo el cortafuegos intercepta la recepción de un correo electrónico para verificar, con la ayuda de un servidor de seguridad de contenidos, que el mismo no contiene contenido malicioso en forma de virus, enlaces a sitios web maliciosos, spam, etc.

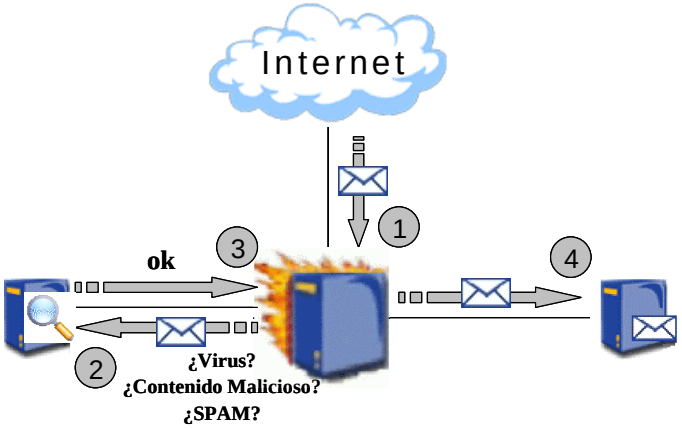

Figura 6. Filtrado de contenidos en correo electrónico entrante

91. De forma análoga pero en sentido inverso, la **Figura 7** muestra cómo el cortafuegos intercepta el intento de conexión de una estación de trabajo a un sitio web prohibido por la política de seguridad de la Organización.

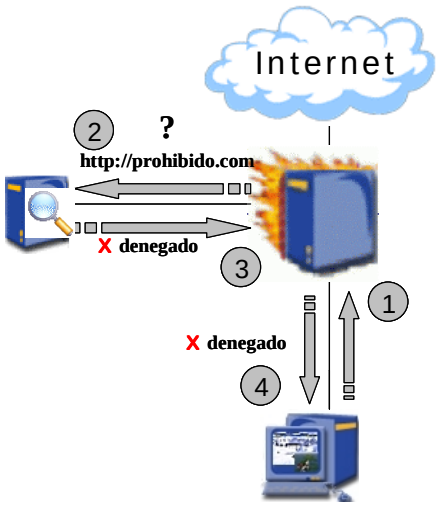

Figura 7. Filtrado de contenidos en acceso web saliente

92. Siempre que sea posible, es más recomendable liberar al cortafuegos de esa tarea añadida y utilizar un *proxy* dedicado del servicio en cuestión que cuente con las capacidades de filtrado de contenidos requeridas. Además de mejorar la eficiencia, simplifica la administración tanto del cortafuegos como del resto de servicios.

93. En las **Figura 8** y **Figura 9** se pueden observar esquemas equivalentes a los anteriores utilizando un *proxy* dedicado en lugar del cortafuegos

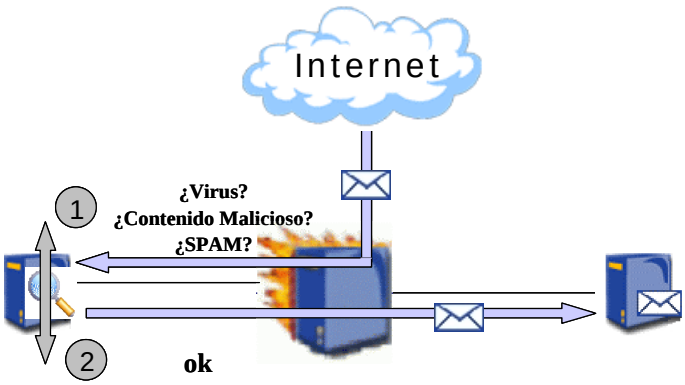

Figura 8. Filtrado de contenidos en correo electrónico entrante con proxy dedicado

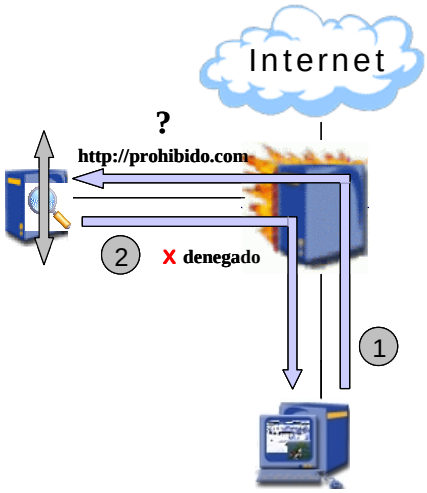

Figura 9. Filtrado de contenidos en acceso web saliente con proxy dedicado

5.5. PREVENCIÓN DE INTRUSIONES

94. Un sistema de prevención de intrusiones (IPS) y un cortafuegos realizan tareas de filtrado de tráfico similares, a pesar de que ambos lo realizan de un modo distinto.

95. Esta similitud ha provocado que algunos cortafuegos incluyan algunas de las funcionalidades de filtrado de tráfico características de los IPS. Mucho antes de la aparición de los IPS, el filtrado de ataques conocidos como *LAND attack*[3], ping de la muerte[4], etc. ya estaban presentes en algunas soluciones de cortafuegos.

96. Cada vez se incluyen más funcionalidades de este estilo en los cortafuegos, lo que en el futuro o en algunos entornos puede provocar que sea el propio cortafuegos el que asuma esas tareas.

97. Al igual que sucedía con el contenido activo, para asegurar la efectividad de la funcionalidad de IPS en el cortafuegos es necesario que **se actualicen periódicamente las reglas** del mismo, recurriéndose a menudo a contratos de mantenimiento externos.

5.6. NORMALIZACIÓN DE PAQUETES

98. Aunque la definición de los protocolos suele estar claramente definida en los RFCs siempre quedan algunas variables con cierto grado de libertad, las cuales cada fabricante implementa como considera adecuado. Por eso, las características de los paquetes vienen definidas por la pila TCP/IP que los generó, que depende del sistema operativo y su versión utilizado (suelen introducirse cambios entre distintas versiones). Algunas pilas TCP/IP son menos robustas en términos de seguridad que otras, siendo susceptibles a ataques de distintos tipos.

99. Para evitar ataques basados en esta premisa, algunos cortafuegos permiten llevar a cabo la normalización de los paquetes que lo atraviesan. Cuando un paquete lo atraviesa, se

[3] Land Attack es un tipo de ataque de Denegación de Servicio (DoS) que se basa en paquetes TCP SYN corruptos que las máquinas receptoras no procesan correctamente, colapsándose ([Ref.- 54]).
[4] El Ping de la Muerte o *Ping of Death* se basa en el envío de paquetes ICMP corruptos, generalmente con un tamaño excesivo, lo que produce el llenado de los buffer y colapso de las máquinas receptoras ([Ref.- 55]).

modifican algunos parámetros de los paquetes de forma que, sin perder funcionalidad, resulten más seguros a su salida del cortafuegos. Asimismo, se descartan aquellos paquetes que son considerados anómalos por no cumplir con las especificaciones concretas de su protocolo.

100. El uso de este tipo de funcionalidad es recomendable, especialmente cuando detrás del cortafuegos existen versiones de sistemas operativos antiguas, con pilas de red poco robustas, con una excepción: existen situaciones en las que debido a una anomalía en la implementación de un protocolo concreto en algún sistema operativo pueden generar paquetes con características anómalas como parte del tráfico operacional. Estos paquetes serían adecuadamente rechazados por el cortafuegos si la normalización de paquetes está en uso, produciendo un daño potencial del servicio para este caso concreto.

5.7. DHCP

101. El protocolo DHCP (*Dynamic Host Configuration Protocol*) se usa para configurar automáticamente la red en sistemas y dispositivos. Cuando un elemento establece su configuración de red, típicamente al iniciarse el mismo, lanza una petición a la red solicitando dicha configuración. El servidor DHCP responde a dicha petición devolviendo la configuración pedida, que normalmente incluye su dirección IP, máscara de subred, ruta por defecto y servidor DNS, entre otros datos.

102. Algunos cortafuegos cuentan con la funcionalidad extra de servidor DHCP. Aunque puede resultar útil para redes de tipo doméstico o pequeñas oficinas, no se recomienda activarlo; de existir una vulnerabilidad en el protocolo DHCP o en la implementación del mismo por parte del fabricante, el cortafuegos y con él toda la arquitectura de seguridad perimetral estarían en peligro.

103. Es recomendable, siempre que sea posible, evitar que los elementos críticos de la infraestructura de red ofrezcan servicios que no sean exclusivamente los que le corresponden por la propia función de seguridad que desempeñan. Todos los demás servicios serán ubicados en servidores externos configurados para tal fin.

5.8. ALTA DISPONIBILIDAD

104. Una de las necesidades más importantes desde el punto de vista funcional de una empresa u organismo es la redundancia de todos sus sistemas productivos, incluyendo los dispositivos críticos de seguridad perimetral y, entre ellos, aquellos puntos que representan la posibilidad de un fallo traumático como son los cortafuegos.

105. Existen dos soluciones extendidas para esta necesidad:

- **Activo-pasivo:** En cada momento existe un sólo dispositivo activo y el resto de los dispositivos supervisan que funciona adecuadamente para en caso contrario tomar el control. La gran desventaja de esta aproximación es que el dispositivo o dispositivos que se encuentran en espera están siendo desaprovechados.
- **Activo-activo:** Todos los dispositivos disponibles están activos en todo momento hasta que alguno falla, distribuyéndose la carga entre todos. La ventaja, al revés que en el supuesto anterior, es que se optimiza la inversión.

106. Contar con un esquema de alta disponibilidad es útil incluso en el caso de que no se produzcan incidentes. Permite poder garantizar la continuidad y estabilidad a la hora de

llevar a cabo periódicas actualizaciones de *software* o *firmware*, aplicar parches o hacer cambios drásticos de configuración.

107. Uno de los requisitos para poder llevar a cabo de forma adecuada la transferencia de control entre el dispositivo activo y el pasivo es que el nuevo dispositivo posea toda la información necesaria del estado en que estaban las conexiones, autenticación, etc. en el dispositivo maestro justo antes de fallar.

108. En relación con lo anterior, hay dos puntos importantes a tener en cuenta:

- ¿Cómo monitoriza el sistema pasivo averiguar que el sistema activo ha fallado o no?
- ¿Qué método utilizar para realizar la transferencia de la información de estado entre el dispositivo activo y el pasivo?

109. Existen protocolos abiertos y propietarios que definen como se lleva a cabo este proceso (HSRP, VRRP, CARP, etc.). Se recomienda restringir este tráfico de transferencia de información sensible a una subred compartida entre ambos dispositivos para evitar que pueda interceptado o modificado. También es posible que la activación/desactivación de los dispositivos se haga desde los propios cortafuegos o de forma externa, con productos específicos para ello.

5.9. BALANCEO DE CARGA

110. El balanceo de carga (*load balancing*) enlaza, en cierto modo, con la alta disponibilidad (modelo activo-activo) en los cortafuegos. Existen muchos modelos que pueden operar en paralelo uniendo toda la capacidad operativa de varios elementos.

111. El balanceo de carga permite que determinados servicios puedan ser atendidos por distintos servidores. Se suele implementar en el cortafuegos por su situación en la entrada a la Organización, así como por sus capacidades de inspeccionar, modificar y direccionar el tráfico,

112. Un caso de ejemplo consiste en una "granja" de servidores web. El cortafuegos, al realizar el balanceo, reparte las peticiones entre distintos servidores web de forma transparente

5.10. TRANSPARENCIA

113. Se entiende por cortafuegos transparente (*transparent firewalls*) aquel que es "invisible" a los clientes y servidores que intervienen en la comunicación. Esto se consigue gracias a que el dispositivo funciona en la capa 2 (enlace de datos) del modelo OSI, pero sin embargo es capaz de modificar los paquetes en tránsito.

114. Su principal ventaja reside en que su introducción en una red no implica la reconfiguración (propiedades de enrutamiento) de los sistemas existentes como típicamente ocurre con los cortafuegos de nivel 3 (red, IP).

115. Dadas sus características, los cortafuegos transparentes no requieren tener asignada una dirección IP para su operación nominal, aunque suele ser necesario fijarle una si se desea poder gestionarlos remotamente. Se recomienda utilizar un interfaz de gestión dedicado únicamente a este propósito para realizar la gestión "fuera de banda".

116. La transparencia no vuelve a un cortafuegos invulnerable, aunque complica los ataques contra él debido a la imposibilidad de utilizar una dirección IP para un ataque remoto. Pueden ser vulnerables a diversos tipos de ataques desde las redes a las que están directamente conectados o incluso remotamente si la implementación de las reglas del cortafuegos o de su pila de protocolos tuviera algún tipo de vulnerabilidad que pudiera ser explotada simplemente a través de los paquetes en tránsito.

5.11. SEGURIDAD EN EL ACCESO REMOTO

117. Actualmente el perímetro de seguridad se está difuminando en muchos entornos debido principalmente a:

– la integración con redes de socios o colaboradores externos.

– la implantación de tecnologías móviles en auge, que permiten el acceso de usuarios remotos a los recursos de la Organización desde cualquier origen.

118. Para satisfacer estas necesidades y mantener la seguridad hay que garantizar tres aspectos importantes:

– **Control de acceso:** garantizar que sólo acceden los usuarios autorizados y a los recursos permitidos.

– **Control de admisión:** garantizar que sólo se accede desde un entorno seguro.

– **Seguridad en el acceso:** garantizar que los datos son accedidos con confidencialidad.

119. La gestión del acceso remoto se puede realizar en el cortafuego o en otros elementos centralizadores, como servidores especializados o de aplicaciones. En los siguientes apartados se va a tratar esta problemática desde el punto de vista del cortafuegos.

5.11.1. CONTROL DE ACCESO

120. Las medidas de control de tráfico reseñadas resultan insuficientes en la mayoría de los casos. Es necesario posibilitar la utilización de mecanismos más potentes de autenticación y control de acceso.

121. Existen distintas aproximaciones que permiten resolver este problema. Las más comunes, sin utilizar otros elementos de seguridad como VPN (que son tratadas más adelante), son las siguientes:

– Autenticación de usuario.

Un cortafuegos de nivel 7 puede interpretar la comunicación de determinados servicios (típicamente telnet, ftp, http/https y rlogin), y solicitar interactivamente autenticación al usuario, normalmente, en forma de nombre de usuario y contraseña. Una vez autenticado el usuario y autorizado su acceso al servicio, el usuario tiene acceso transparente al mismo.

– Autenticación de sesión.

La autenticación de sesión se lleva a cabo habitualmente a través de un agente, un programa específico que se ejecuta en el sistema remoto y que permite al usuario introducir sus credenciales, usualmente en forma de nombre de usuario y contraseña.

Tras autenticar adecuadamente al usuario, el cortafuegos permite el acceso transparente desde la dirección IP de origen al servicio o servicios que hayan sido definidos previamente para ese usuario.

– Autenticación de cliente.

La autenticación de cliente se puede llevar a cabo a través de un agente, como en el caso anterior, o directamente a través de una autenticación directa en el cortafuegos (por ejemplo vía telnet o http/https). La autenticación de cliente suele ser más flexible que la de sesión, permitiendo definir a que sistema y/o servicio se desea acceder y durante que período de tiempo o número de accesos.

122. Algunos de los métodos de autenticación mencionados anteriormente pueden contribuir a aumentar ese riesgo. Si se utiliza un servicio no cifrado (como http) para la autenticación, tanto usuario como contraseña viajarán en claro por la red, siendo susceptibles de ser interceptados y reutilizados por un potencial atacante. Para servicios no cifrados (telnet, rlogin, http) se deben usar como alternativa servicios cifrados o agentes de autenticación, que suelen utilizar cifrado y a menudo autenticación de tipo "desafío-respuesta" (*challenge-response*), en la cual no es la propia contraseña la que viaja por la red sino un "testigo" que ha sido cifrado con ella.

123. Existen distintas estrategias para llevar a cabo el proceso de autenticación contra el cortafuegos. Los cortafuegos modernos son capaces de permitir un amplio rango de métodos como usuario/contraseña, *S/KEY*, *SecureID* o incluso sistemas biométricos.

124. Tanto la autenticación de sesión como la de cliente cuentan con la ventaja de poder permitir el acceso a cualquier servicio, no encontrándose limitadas a los servicios soportados por los *proxies*. La gran desventaja de utilizar estos dos tipos de autenticación se presenta en los casos en los que el sistema remoto es un sistema multiusuario o está sometido a traducción de direcciones (NAT). En esos casos, el cortafuegos no es capaz de distinguir unívocamente de qué usuario o sistema final concreto proviene la petición, corriendo el riesgo potencial de permitir acceso a usuar*ios o s*istemas no autorizados que comparten la misma dirección IP desde el punto de vista del cortafuegos. En los casos en que ninguna de estas opciones sea suficiente se podría recurrir al uso de redes privadas virtuales (VPN) u otras tecnologías.

125. Algunos productos de cortafuegos permiten integrar las reglas de autenticación en el juego de reglas estándar. No se recomienda, puesto que las reglas de autenticación tienen una naturaleza distinta a las reglas de filtrado de tráfico. Si este fuera el caso, se deberán situar siempre tras las reglas concretas que puedan aplicarse a ese servicio. Por ejemplo, si a un sistema concreto sólo se quiere permitirle acceso al puerto 443 “https” y además exigirle autenticación, la regla de autenticación debería ser posterior a la regla que restringiera el acceso a dicho puerto. En cualquier caso, es muy importante consultar la documentación y familiarizarse con el funcionamiento del sistema de autenticación del producto en cuestión.

5.11.1.1 DIRECTORIOS DE USUARIOS

126. En caso de que la organización cuente con directorios centralizados de usuarios y autenticación (*RADIUS*, *TACACS+*, *LDAP*, *Active Directory*) es conveniente integrar la autenticación a nivel de cortafuegos con el resto de la autenticación corporativa. Esto permite gestionar centralizadamente a nivel corporativo los usuarios y sus privilegios lo

que suele representar una ventaja desde el punto de vista de la seguridad y redunda en una mayor comodidad de cara al usuario.

127. En determinados entornos sensibles, el uso de directorios de usuarios puede suponer un riesgo. Si las contraseñas son eventualmente comprometidas, no sólo sería posible autenticarse frente al cortafuegos sino que además se ganaría acceso a otros sistemas de la infraestructura de la Organización. En ese caso, se recomienda el uso de usuarios distintivos en los servicios más sensibles.

128. También hay que cuidar la transmisión de la autenticación dentro de la propia red, desde el cortafuegos hasta el servidor de autenticación. Aproximaciones como Kerberos, con un robusto sistema de autenticación, son bastante resistentes a este tipo de problemas, así como puede serlo LDAP si se combina con el uso de SSL. En el caso de utilizar RADIUS y los métodos de autenticación CHAP o PAP, el esquema final podría ser vulnerable a la intercepción de la contraseña y a otros tipos de ataques dependiendo de la implementación final y del método elegido, especialmente en el caso de PAP (un protocolo considerado poco seguro).

129. En la **Figura 10**, se puede observar el intento de acceso a la Organización por un usuario a través de un mecanismo usuario/contraseña. Tras recibir las credenciales, el cortafuegos consulta con el servidor centralizado de autenticación (en este caso un servidor *RADIUS*) para verificar si dicha combinación usuario/contraseña es aceptada. En caso positivo, el cortafuegos permitirá el acceso al usuario en los términos definidos en la política de acceso.

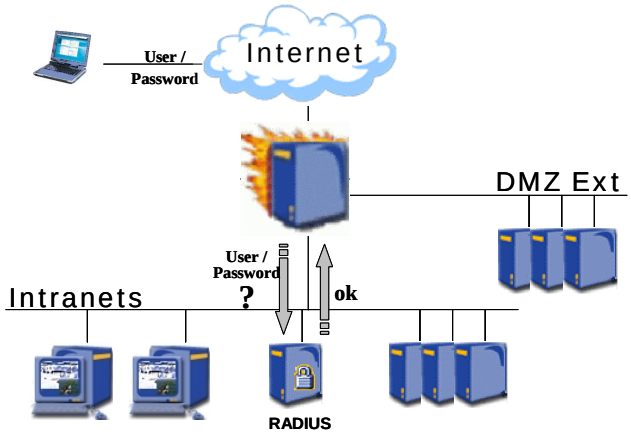

Figura 10. Autenticación mediante un servidor RADIUS

5.11.2. CONTROL DE ADMISIÓN A LA RED

130. En ese escenario, resulta cada vez más importante verificar que el sistema remoto cuenta con las debidas condiciones de seguridad antes de permitírsele el acceso a los recursos internos de la Organización.

131. La comprobación de las redes de socios o colaboradores debe ser garantizada de manera manual y a través de un compromiso de éstas, que debe renovarse y verificarse periódicamente. Pero ése método no es válido para las conexiones móviles, que deben ser verificadas automáticamente.

132. Esta verificación, cuyo punto natural de aplicación es el cortafuegos o el sistema de control de acceso, debe garantizar que el sistema remoto cumple con la política de seguridad establecida por la Organización respecto a:

- versiones y nivel de actualización del sistema operativo y aplicaciones,
- actualización de antivirus,
- sistemas de detección y prevención de intrusos,
- en general, cualquier tecnología que pueda influir en la integridad del sistema remoto y que sea capaz de informar al cortafuegos de su estado.

133. Si dicha verificación de integridad no es completada con éxito pueden tomarse diversas acciones, cómo denegar al sistema remoto el acceso a la red o permitir un acceso limitado que le proporcione la oportunidad de corregir los problemas detectados a través del acceso a un servidor de actualizaciones de seguridad, actualización de antivirus, etc. y así poder intentar de nuevo superar con éxito los diversos chequeos necesarios.

134. Como ejemplo, se podría pensar en un sistema remoto que intentara acceder a la Organización. El sistema de control de admisión a la red establecería comunicación con los distintos componentes del sistema remoto, como por ejemplo con el sistema de antivirus, quien sería interrogado acerca del grado de actualización del motor de búsqueda y de las firmas. Posteriormente, podría entablar una conexión con el sistema de detección de intrusos y verificar si se han producido eventos relevantes. También podría verificar si el nivel de parcheado del sistema es el adecuado. En base a toda esta información y a la política definida en respuesta a cada uno de estos parámetros, el sistema podría ser o no admitido a la red.

5.11.3. SEGURIDAD EN EL ACCESO: REDES PRIVADAS VIRTUALES (VPN)

135. El concepto de red privada virtual (Virtual Private Network - VPN) intenta dar solución al problema de cómo establecer una comunicación segura y flexible entre dos nodos, entre un nodo y una red o entre dos redes cuando dicha comunicación ha de atravesar un medio potencialmente inseguro, como puede ser Internet.

136. El grado de flexibilidad y seguridad proporcionado por la VPN dependerá de la tecnología concreta seleccionada y puede incluir:

- Garantizar la integridad de la comunicación.
- Garantizar la confidencialidad de la información.
- Proporcionar resistencia limitada al análisis del tráfico cifrado.
- Requerir la autenticación robusta de las partes involucradas.
- Requerir distintos tipos de control de acceso.

5.11.3.1 CRIPTOGRAFÍA

137. Las VPN se apoyan fuertemente en la criptografía para asegurar la integridad y confidencialidad de las comunicaciones. Es habitual que el administrador tenga la capacidad de modificar los parámetros criptográficos que se utilizarán en una VPN. El administrador debe estar, por tanto, familiarizado con los algoritmos criptográficos más habituales para poder determinar cuál es la configuración idónea para una VPN concreta

y no terminar estableciendo parámetros criptográficos débiles que pongan en peligro la seguridad de la VPN.

138. En lo que respecta al cifrado utilizado para garantizar la confidencialidad de las comunicaciones, se pueden utilizar cualquiera de los dos grupos establecidos de algoritmos:

5.11.3.1.1. Cifrado simétrico

139. El cifrado simétrico se basa en el conocimiento de una clave compartida que ambas partes conocen, con la cual se cifrarán las comunicaciones. Algunos de los algoritmos de cifrado simétrico más populares son DES, 3DES, Blowfish y AES.

140. DES (Data Encryption Standard) que durante muchos años constituyó el estándar de cifrado y que suele aparecer como una opción en casi todas las implementaciones de VPN hace largo tiempo que puede ser descifrado en tiempo real, por lo que se desaconseja altamente su uso. La opción aconsejada es el nuevo estándar AES (Advanced Encryption Standard).

5.11.3.1.2. Cifrado asimétrico

141. El cifrado asimétrico se diferencia del simétrico en que no es necesario conocer una clave común para intercambiar información cifrada. La clave se compone de dos partes, la clave pública y la clave privada, que son complementarias y obtenidas en el mismo proceso de generación. Algo que es cifrado con la clave pública sólo puede ser descifrado con la clave privada, y viceversa. Por tanto, la clave pública puede ser distribuida públicamente sin por ello comprometer la seguridad del conjunto.

142. El cifrado asimétrico implica un mayor consumo de procesador que el cifrado simétrico, por lo que no ralentiza las comunicaciones. Suele emplearse para el intercambio seguro de de la clave utilizada para el cifrado simétrico.

143. El protocolo de intercambio de claves, llamado también IKE (RFC 2409, [Ref.- 45]), se basa en un cifrado asimétrico para intercambiar la clave simétrica. Puede utilizar distintos algoritmos asimétricos, entre los cuales se distinguen:

- **Diffie-Hellmann** (DF): uno de los más conocidos y utilizados. Utilizándolo es posible llegar a un secreto compartido común sin que la información intercambiada entre las partes sea suficiente, en caso de ser interceptada, para poder averiguar dicho secreto. En cambio, Diffie-Hellmann es vulnerable a ataques *man-in-the-middle*, lo que puede ser resuelto utilizando algoritmos de clave pública para asegurar la integridad de los mensajes del intercambio.
- RSA,
- **Método Oakley** (RFC 2412, [Ref.- 48]): Basado en DF, añade una serie de garantías de que no se va a sufrir un ataque y aumentar la seguridad, incluyendo:
    - *Cookies* para evitar ataque DoS.
    - El cálculo de los exponenciales usados en el cifrado está relacionado con la idenatidad de los nodos que se comunican.
    - Opción de seleccionar los métodos de cifrado, derivación de clave y autenticación a elegir entre los grupos Oakley de 3 tipos: de Módulo de Exponencial (MODP: *MODular exPonential group*), de Cúrva Elíptica

sobre Campo Finito 2^N (EC2N) y de Curva Elíptica sobre Campo Finito Primo (ECP). Los usuarios pueden definir sus propias estructuras matemáticas, lo que reduce aún más las posibilidades de suplantación de identidad. IANA ha predefinido numerosos grupos con distintas longitudes de clave y configuraciones, numerados e identificados con números del 1 al 32767 (RFC 2409 [Ref.- 45], RFC 3526 [Ref.- 46], RFC 4753 [Ref.- 47], etc.).

144. Se recomienda elegir, siempre que sea posible, un grupo Oakley de valor lo mayor posible, para garantizar que sea reciente y seguro, y al menos superior al 5.

5.11.3.1.3. Funciones de Hash

145. Las funciones de *hash* son algoritmos que, a partir de un mensaje de entrada de longitud arbitraria, son capaces de producir una salida de longitud fija llamada firma (*message hash*, *digest* o *fingerprint*). Estas funciones suelen ser utilizadas para verificar la integridad de los mensajes ya que si un mensaje es modificado, su firma varía y se puede comparar el *hash* del mensaje enviado con el *hash* generado del mensaje recibido.

146. Hay dos propiedades que deben tener los algoritmos de *hash*:

- Por muy pequeña que sea la diferencia entre el mensaje original y el modificado, aunque sea de un sólo bit, el *hash* generado en uno y otro caso serán completamente distintos.
- Los algoritmos de hashing han de tener una probabilidad de colisión mínima. Esto quiere decir que la posibilidad de que dos mensajes distintos tengan el mismo *hash* es extremadamente remota y no puede ser, en principio, conseguido ex profeso.

147. Ejemplos típicos de algoritmos de *hashing* son, entre otros:

- MDC-2
- GOST
- SHA-1
- HAS-1 (derivado de SHA-1)
- SHA-2

148. Se ha demostrado que otros algoritmos como MD2 ([Ref.- 53]), MD4 ([Ref.- 52]), MD5 ([Ref.- 50]), HAVAL-128, MD4, RIPEMD y SHA-0, LM-HASH, N-Hash, no son seguros y no deben usarse. Siempre que sea posible deberá utilizarse el más robusto, por lo que el algoritmo más recomendable en el momento de la redacción de este documento es el **SHA-2**. Está en marcha un concurso para seleccionar el algoritmo SHA-3, cuyo resultado se anunciará en 2012 ([Ref.- 51]).

149. Un caso particular de los algoritmos de *hashing*, lo constituyen los conocidos como HMAC (*Hash Message Authentication Code*), que son fundamentalmente modificaciones de los anteriores de tal forma que se introduce una clave compartida en el proceso de generación del *fingerprint*. De esta manera, la clave compartida asegura la integridad del *hash* y el *hash* asegura la integridad del mensaje. Un ejemplo típico de este tipo de *hashing* es HMAC-SHA-1.

5.11.3.2 Tipos de VPN

150. Los tipos de VPN más populares son los siguientes:

– PPTP.

PPTP (*Point-to-Point Tunneling Protocol*) fue durante largo tiempo la única opción para establecer VPN en sistemas Windows. A pesar de haberse subsistido a lo largo del tiempo y haber sufrido varias actualizaciones sigue siendo vulnerable a ataques del tipo *man-in-the-middle* relacionados con la integridad de los datos y su origen.

El mayor problema que presenta este protocolo es la poca flexibilidad en la autenticación ya que sólo soporta contraseñas. Por estas razones, no resulta aconsejable utilizar PPTP para el establecimiento de redes privadas virtuales y en su lugar, es recomendable utilizar opciones alternativas como L2TP o IPSec.

– L2TP.

L2TP (*Layer 2 Tunneling Protocol*) es una extensión del protocolo PPP (*Point-to-Point Protocol*) que permite a proveedores de servicio la posibilidad de establecer VPN. L2TP funciona a nivel 2 (enlace de datos), teniendo la capacidad de tunelizar cualquier tráfico de nivel 3 (red).

L2TP adolece de un problema y es que no soporta el cifrado de mensajes, por lo que habitualmente se suele combinar con IPSec si se requiere confidencialidad.

– SSH tunneling.

SSH es un protocolo estándar, en modo línea de comando, para conexiones remotas. SSH tiene la capacidad de tunelizar tráfico TCP (nivel 4) a través de un canal cifrado, creando en términos prácticos una VPN. Este protocolo establece correspondencias entre puertos locales y remotos que permiten el acceso sencillo a servicios activos en el sistema remoto o incluso en la red remota.

El único requisito para establecer este tipo de VPN es tener un cliente y un servidor de SSH a ambos lados de la comunicación.

– SSL.

Las VPN basadas en SSL han ido ganando poco a poco terreno a las basadas en IPSec debido a su sencillez y no necesidad de instalación de software en la máquina cliente. Estas VPN utilizan una conexión SSL a través de un navegador web estándar para alcanzar un dispositivo que se encuentra en el perímetro de la Organización.

Este dispositivo servirá de interfaz con los servidores de la Organización para proporcionar acceso a través del propio navegador a aplicaciones clásicas (correo, calendario, etc.), a sistemas de ficheros en servidores remotos o incluso acceso directo a través de línea de comando o compartición de escritorio a sistemas internos.

En las versiones más elaboradas también se permite tunelizar puertos o incluso redes enteras. A todas estas capacidades se añade un fuerte y flexible control de acceso y detallado registro de eventos (auditoría).

– IPSec.

IPSec (*Internet Protocol Security*) es un conjunto de protocolos que permite establecer VPN a nivel 3 (transporte) entre dos nodos, un nodo y un *gateway* o dos *gateways*. IPSec es optativo en IPv4 pero parte del estándar IPv6. Desde 2005, fecha en la que sufrió una serie de vulnerabilidades, cuenta con su tercera versión que aún se considera segura, detallada en las RFC 4301 ([Ref.- 57]) y 4309 ([Ref.- 58]).

Muchas veces se utiliza el término VPN para hablar exclusivamente de aquellas basadas en IPSec, debido a la ubicuidad de esta tecnología. Por este factor, por su importancia de cara a la implantación de IPv6 y por la cierta complejidad que encierran, se incluye más adelante un apartado específico sobre su funcionamiento básico.

– MPLS.

A pesar de que una de las capacidades de IPSec es la posibilidad de establecer túneles entre dos *gateways* para conectar redes, lo cierto es que MPLS (*MultiProtocol Label* Switching) se ha convertido en la opción más utilizada para llevar a cabo esta tarea debido, entre otras cosas, a su mayor sencillez y transparencia.

El funcionamiento de MPLS ([Ref.- 59]) es conceptualmente simple y está basado en etiquetas que se añaden a las tramas de nivel 2 (enlace de datos). Los paquetes de nivel 3 (red) viajan de origen a destino y en un punto concreto entran en la red MPLS a través del *Ingress Label Switched Router* (*Ingress LER*).

Los paquetes son encapsulados en tramas MPLS de nivel 2 (enlace de datos) y debidamente etiquetados. Dichas tramas viajarán hacia su destino utilizando un túnel que ha sido previamente establecido entre el punto de entrada (*Ingress LER*) y el punto de salida (*Egress LER*) atravesando los distintos enrutadores MPLS intermedios, conocidos como *Transit Label Switched Routers* (*TLSR*).

Posteriormente, los paquetes serán desencapsulados y seguirán su enrutamiento normal de nivel 3 (red) dentro de la Organización remota hacia su destino final.

5.11.3.3 IPSEC

151. IPSec está formado por un conjunto de protocolos que permiten establecer túneles entre dos sistemas, entre un sistema y un *gateway* o entre dos *gateways*.

152. Las dos partes implicadas establecen una comunicación previa y se ponen de acuerdo en qué parámetros se van a utilizar durante la comunicación. En el caso más común, dicha negociación se realizará utilizando el protocolo IKE (*Internet Key Exchange*). IKE funciona en dos fases, en la primera se negocian unos parámetros iniciales para crear un canal de cifrado previo que sirva para proteger una segunda negociación. En esta segunda fase se acordarán los parámetros de la red privada virtual, constituyendo lo que se denomina Asociación de Seguridad (*Security Association - SA*), permaneciendo para referencias futuras en la Base de Datos de Asociaciones de Seguridad (*Security Associations Database - SAD*) que contendrá en cada momento las entradas para las SA activas.

153. Las SA tienen la característica de ser unidireccionales, por lo que se necesitarán dos juegos de SA para tráfico saliente y entrante. Para cada juego de SA, se almacenan, entre otros, los siguientes datos:

- protocolo IPSec
- modo de operación
- claves criptográficas
- algoritmos criptográficos
- tiempo de vida de las claves.

154. IPSec contempla dos posibles **protocolos**:

- **Authentication Header - AH**: proporciona autenticación del origen e integridad de datos, pero no proporciona cifrado.
- **Encapsulating Security Payload - ESP**: proporciona confidencialidad (cifrado simétrico), protección limitada frente a análisis de tráfico, autenticación de origen, integridad y servicio *anti-replay* opcional.

155. Tanto AH como ESP pueden ser utilizados en dos **modos de operación**:

- **Transporte**: sólo puede ser utilizado entre dos sistemas o dispositivos. No es compatible con NAT en AH, ya que autentica los campos inmutables de la cabecera, entre los que se encuentran la dirección IP de origen y la de destino. Sí es compatible con NAT en ESP.
- **Túnel**: los *gateways* crean una nueva cabecera IP y encapsulan dentro el datagrama original.

156. Un elemento crucial en todo este proceso es la Base de Datos de Políticas de Seguridad (*Security Policy Database - SPD*). En ella se almacenan las políticas de seguridad de la Organización en lo que respecta al tráfico intercambiado vía IPSec, especificando entre qué red o redes se permite el intercambio de tráfico, qué protocolos específicos y bajo qué condiciones de cifrado y autenticación.

6. TIPOS DE CORTAFUEGOS

157. A continuación se describen las diferentes tecnologías de cortafuegos que se pueden encontrar disponibles en gran parte de los productos o soluciones existentes.

6.1. FILTRADO BÁSICO DE PAQUETES

158. El filtrado básico de paquetes, también conocido como *stateless packet filtering*, se basa en una lista de control de acceso sobre la información de cabecera de las capas de red y transporte (direcciones IP origen/destino, protocolos IP, puertos TCP/UDP, banderas TCP, etc.) de manera individual e independiente para cada uno de los paquetes.

159. Se trata de la forma más simple y ligera de filtrado. Sólo evalúa las cabeceras y no memoriza el estado de las conexiones a nivel de transporte permitidas con anterioridad. Es habitualmente utilizado como control básico de acceso en dispositivos de encaminamiento de perímetro, siendo la primera línea de filtrado en una aproximación multicapa para proporcionar filtrado de entrada/salida (*ingress/egress filtering*). Su configuración recomendada incluye:

- Permitir el tráfico saliente sólo originado con direcciones propias.

- Permite el tráfico entrante sólo destinado hacia direcciones propias.
- Denegar el tráfico saliente a direcciones de tipo *bogon*:
  - No asignadas (*unallocated*).
  - Reservadas o de uso especial (S*pecial Use Addresses* - *SUA*).
- Limitación de exposición y acceso global:
  - Denegar los servicios no permitidos por política en ambos sentidos.
  - Denegar los puertos asociados a código malicioso (gusanos, troyanos, etc.).

6.2. FILTRADO DE PAQUETES CON ESTADO

160. El filtrado de paquetes con estado, también conocido como *stateful packet filtering*, es un filtrado más completo que el filtrado de paquetes estándar ya que le añade la capacidad de mantener información de estado de las conexiones establecidas.

161. Esto permite una mayor flexibilidad y seguridad porque se evalúa la situación en función de la información ya permitida y memorizada (puertos TCP/UDP, banderas TCP, números de secuencia TCP) con anterioridad al juego de reglas definido. Los paquetes no son tratados ya de manera individual sino como iniciadores de una nueva comunicación o participantes de una existente.

162. A efectos prácticos, esta "memoria" del cortafuegos se traduce en una tabla de conexiones establecidas, mantenidas durante la comunicación y olvidadas al finalizar o tras un tiempo máximo de inactividad (*timeout*). No puede mantenerse información de estado para todos los protocolos de transporte sino sólo para algunos de ellos.

163. Disponer de la información de sesión es la principal ventaja de este tipo de cortafuegos ya que su mayor granularidad los hace menos vulnerables a la falsificación de paquetes. Sin embargo, suelen ser más lentos al tener una carga de proceso más alta debido al mantenimiento de la tabla de estados y a la evaluación de los paquetes con las conexiones existentes.

164. De la misma manera que el filtrado básico de paquetes, no inspecciona el contenido de los paquetes ni, por tanto, evita ataques de protocolo o de nivel de aplicación.

6.3. FILTRADO DE PAQUETES CON ESTADO E INSPECCIÓN

165. El filtro de paquetes con estado e inspección, también conocido como *stateful inspection packet filtering*, es un filtrado todavía más completo que los dos anteriores. Añade la capacidad de inspeccionar el contenido de los paquetes, interpretando los protocolos o aplicaciones que viajan dentro de los datagramas de la capa de transporte.

166. Posee un mayor grado de "inteligencia" y conocimiento de la torre del modelo OSI, de manera que puede interpretar el protocolo de alto nivel y adaptar las reglas para permitir los diferentes flujos generados.

167. Esto es especialmente útil en protocolos con comportamientos dinámicos, donde se negocia a nivel de aplicación, durante la sesión, las características de la comunicación a nivel de transporte y posteriormente establecen varias comunicaciones en distintos puertos.

168. Su ventaja reside en la capacidad de gestionar dinámicamente el filtrado gracias al conocimiento de los protocolos. Sin embargo, esto supone una alta carga de proceso al

sistema al tener que inspeccionar el contenido de los paquetes decodificando los protocolos y memorizando consecuentemente la información.

6.4. CORTAFUEGOS A NIVEL DE APLICACIÓN

169. Los cortafuegos a nivel de aplicación, también conocidos como *proxies*, no sólo se sitúan en un punto intermedio de la comunicación sino que actúan totalmente como intermediario en ésta: aceptan las peticiones de los clientes y actúan en su nombre ante los servidores.

170. Actúan en la capa 7 del modelo OSI y por ello históricamente han sido considerados los cortafuegos más seguros. Se puede decir que enmascaran totalmente la comunicación del usuario, suplantándola en su nombre.

171. Gran parte de los cortafuegos de aplicación, además de la posibilidad de validar las peticiones con listas de control de acceso, entienden el protocolo y por tanto tienen la capacidad de **validar la información de la comunicación**: formato y secuencia de los comandos, validación de contenido, etc.

172. Los cortafuegos a nivel de aplicación pueden ser desde una aplicación ***proxy*** que implementa la funcionalidad cliente/servidor de un protocolo o aplicación concreta, a un decodificador de múltiples protocolos que realiza la función de **pasarela**. Obviamente, para cada nuevo protocolo necesita un nuevo módulo capaz de interpretarlo.

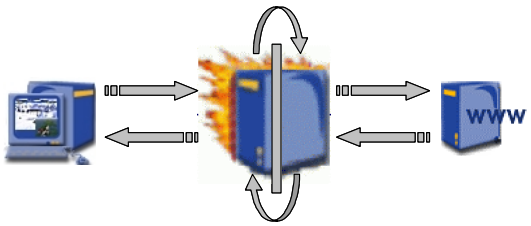

Figura 11. Cortafuegos a nivel de aplicación (proxy)

173. Las principales ventaja de este tipo de cortafuegos residen en su "inteligencia" respecto a los protocolos y se basan en que:
   - inspeccionan el contenido
   - realizan control del estado de la comunicación (*stateful inspection*)
   - garantizan que se cumplen los RFC o estándares correspondientes
   - aíslan totalmente la comunicación por su actuación en las siete capas OSI

174. Estas ventajas implican habitualmente una mayor necesidad de recursos, capacidad de proceso y memoria, limitando el rendimiento: número máximo de conexiones y volumen de tráfico (*throughput*).

175. Las desventajas derivadas de su situación en medio de la comunicación son:
   - Al tener una dirección IP visible para responder a las peticiones, son más vulnerables a ataques y corren el riesgo de ser comprometidos o sufrir denegación de servicio
   - La configuración de su uso en los clientes de la red supone una carga administrativa.

176. Estos efectos se ven paliados con los "***proxies* transparentes**". Estos dispositivos son enrutadores que interceptan todo el tráfico a nivel de red y lo redireccionan a una aplicación de proxy que se ejecuta en el mismo sistema o en otro (para evitar sobrecarga).

Dicha aplicación realiza la petición correspondiente y recibe la respuesta, que es enviada a través del *proxy* transparente a nivel de red en la misma sesión que tenía establecida el cliente final. El cliente no percibe que su petición ha sido interceptada y no es necesario hacer ningún tipo de cambio de configuración.

177. Existe otra funcionalidad muy habitual llamada "***proxy* inverso**", que atiende las peticiones de clientes externos para proteger el acceso a un servicio interno.

178. Gran parte de las soluciones de cortafuegos incorporan funcionalidades a nivel de aplicación para los protocolos más habituales (SMTP, HTTP, FTP, LDAP, SQL, etc.).

6.5. CORTAFUEGOS TRANSPARENTES

179. Se considera cortafuegos transparentes a todos aquellos que funcionen transparentemente como se ha explicado en el apartado de funcionalidades.

6.6. CORTAFUEGOS A NIVEL SISTEMA

180. Un cortafuegos de sistema es aquel que está instalado en el servidor o en el cliente en vez de tratarse de un elemento aparte de red.

6.6.1. SISTEMAS UNIX

181. En los sistemas UNIX (Linux, BSD, Solaris, etc.), los cortafuegos a nivel sistema realizan la misma terea que un cortafuegos estándar de red. La única diferencia existente es que los juegos de reglas no son aplicados al tráfico que atraviesa el dispositivo sino al tráfico que tiene por destino el dispositivo en sí mismo. De esta forma, configurar un cortafuegos a nivel sistema no es muy distinto a configurar un cortafuegos de red del mismo tipo (es habitual que los sistemas UNIX integren cortafuegos de forma estándar en el sistema operativo).

182. Es recomendable que, independientemente de los cortafuegos de la plataforma, todos los servidores cuenten con su propia herramienta cortafuegos que, además de filtrar el tráfico no permitido, lo monitorice.

6.6.2. SISTEMAS WINDOWS: CORTAFUEGOS PERSONALES

183. En los sistemas Windows, los cortafuegos a nivel sistema, más conocidos en este caso como **cortafuegos personales**, realizan a menudo más tareas que el simple filtrado de los paquetes destinados al mismo. Las abundantes amenazas en un sistema Windows (virus, gusanos, troyanos, etc.), tras introducirse en el Sistema por métodos ajenos al tráfico de red (habitualmente gracias a técnicas de ingeniería social) inician conexiones salientes muy difíciles de filtrar, desde el punto de vista de un cortafuegos convencional, dado que aparecen ante el mismo como conexiones lícitas.

184. La solución a este tipo de comportamiento ha sido la de incluir en el cortafuegos capacidades adicionales, como la posibilidad de verificar qué proceso establece cada conexión saliente. Se puede configurar el cortafuegos para que permita acceder al exterior sólo a determinados programas y deniegue el acceso al resto o pida confirmación del usuario.

185. Algunas soluciones de cortafuegos de red incluyen cortafuegos personales integrados con los clientes VPN. Estos cortafuegos pueden ser gestionados remotamente el cortafuegos de red, creando políticas controladas para los usuarios móviles de la Organización.

6.6.3. BUENAS PRÁCTICAS

186. La **configuración** de cortafuegos a nivel de sistema es una práctica altamente recomendada, especialmente en aquellos sistemas que estén especialmente expuestos o que sean críticos para la Organización y en general para servidores donde las necesidades de comunicación no suelen cambiar drásticamente.

187. Se recomienda **revisar los *logs*** (registros de eventos) de los cortafuegos a nivel sistema periódicamente, al menos de forma diaria, y configurar adecuadamente los **sistemas de alertas** frente a tráfico no esperado/deseado.

188. A pesar de que lo anterior pueda parecer una labor ardua cuando crece el número de servidores y estaciones de trabajo, en realidad con una buena política de reglas y un sistema eficiente de recolección y procesamiento de eventos llevar a cabo esta tarea debería consumir un tiempo mínimo.

189. Una de las razones para poner en práctica lo mencionado es que una vez definido claramente el juego de reglas que han de proteger a un servidor, eliminando el ruido con las reglas correspondientes, cualquier otro tráfico que llegue al mismo se puede considerar como malicioso, lo que convierte a los cortafuegos a nivel sistema en excelentes elementos de detección de intrusiones.

6.7. CORTAFUEGOS VIRTUALES

190. La implantación de las tecnologías VLAN (*virtual LAN*) en todo tipo de dispositivos de red y sistemas permite compartir el mismo medio físico al tráfico correspondiente a distintas redes virtuales. Esto resulta extremadamente útil para optimizar los cada vez más amplios anchos de banda con los que cuentan las infraestructuras de red modernas, especialmente las de grandes Organizaciones o proveedores de servicio.

191. Los cortafuegos se han adaptado a esta tecnología, permitiendo gestionar el flujo de tráfico entre distintas VLAN. Permiten definir cortafuegos virtuales sobre un sólo sistema físico, contando con la posibilidad de que cada cortafuegos atienda a una VLAN distinta y trabaje con un juego de reglas distinto, siendo posible delegar la gestión de cada uno de los cortafuegos a un administrador potencialmente distinto.

192. Un ejemplo de este tipo de cortafuegos lo encontramos en la **Figura 12**, en la que se observa como tres redes distintas (tres departamentos diferentes dentro de una Organización que ofrezcan distintos tipos de servicios con distintos requisitos de seguridad) comparten el mismo cortafuegos físico para acceder a Internet, pero cuentan con distintos cortafuegos virtuales.

193. En el ejemplo, el tráfico de Internet llega a un sólo sistema físico que sustenta los tres cortafuegos virtuales distintos, y es encaminado al cortafuegos virtual que corresponda al destinatario en cuestión. A partir de ahí, dicho tráfico se filtra de acuerdo con la política de seguridad correspondiente al sitio final y sale del dispositivo utilizando una VLAN concreta dedicada a dicho sitio (en el caso del “sitio 3” aparecen dos VLAN dedicadas).

194. En este ejemplo concreto se percibe como el *switch* que se encuentra asociado a cada una de las redes es el que se encarga de desencapsular la información de VLAN y entregar el tráfico a los sistemas finales.

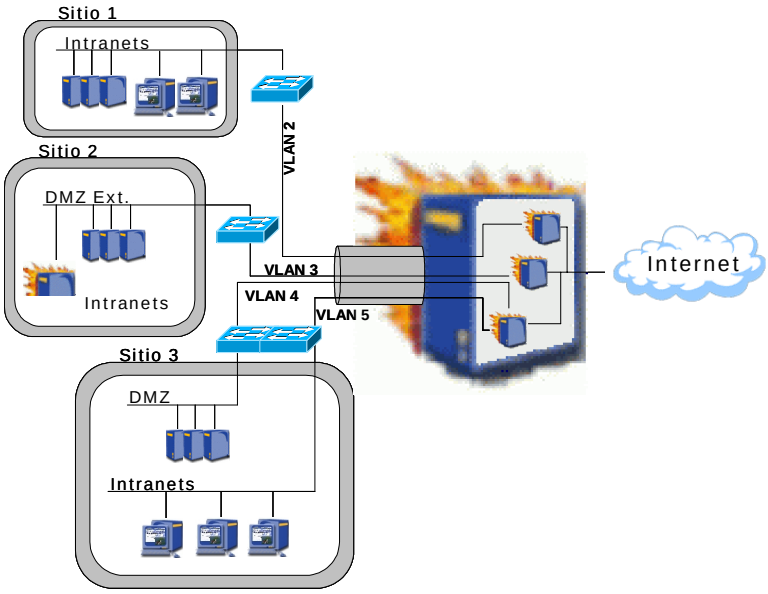

Figura 12. Ejemplo de cortafuegos virtual

195. La seguridad de todo el conjunto va a depender de que los switches sean capaces de asegurar la estanqueidad de las VLAN. La utilización de una VLAN no está exenta de posibles problemas de seguridad; en caso de optar por una solución de estas características, se recomienda que se compruebe previamente la seguridad de la infraestructura de red involucrada.

196. Esta tecnología tiene una gran utilidad para algunos sectores como los proveedores de acceso, que pueden combinarla con redes privadas MPLS proporcionar servicios de cortafuegos a distintas Organizaciones finales.

197. Es importante destacar que los cortafuegos virtuales disponen de las mismas características que los cortafuegos tradicionales en términos de funcionalidad (NAT, VPN, etc.) según se ha descrito en apartados anteriores.

6.8. SISTEMAS DEDICADOS (APPLIANCE) Y DE PROPÓSITO GENERAL

198. Una de las discusiones tradicionales a la hora de poner en marcha una infraestructura de cortafuegos es decidir si se va a optar por un **sistema de propósito general** e instalar sobre el mismo el software de cortafuegos o directamente optar por un **dispositivo dedicado** o ***appliance***. La tendencia general parece ser utilizar *appliances*, pero la decisión final debe ser tomada por la Organización sin tener en cuenta tendencias.

199. Los *appliances* presentan las siguientes ventajas:

- son dispositivos más fáciles de instalar y gestionar por haber sido pensados ex profeso para realizar esa función
- suelen estar optimizados para su función

200. Los sistemas de propósito general presentan las siguientes ventajas:

- permiten mayor flexibilidad en su uso

– la inversión suele resultar inferior

201. Las condiciones de seguridad no dependen del tipo de sistema sino de la elección de la solución, dependerá del sistema elegido y del sistema operativo sobre el cual opera el *software* de cortafuegos. Los *appliances* suelen utilizar un sistema operativo de propósito general optimizado para su función, por no serán necesariamente más eficientes o seguros que los de propósito general.

7. DISPOSITIVOS ADICIONALES

7.1. SISTEMAS DE DETECCIÓN DE INTRUSIONES

202. Los sistemas de detección de intrusiones (*Intrusion Detection Systems* - IDS) son otro elemento esencial de la arquitectura de seguridad perimetral de una Organización. Tienen como función detectar indicios de ataque o compromiso hacia elementos de la infraestructura de los sistemas o redes de la misma.

203. En este apartado únicamente se realiza una introducción somera a este tipo de dispositivos. Para más información, acuda a la guía CCN-STIC 432 ([Ref.- 56]).

204. Existen dos tipos generales de sistemas de detección de intrusiones: a nivel de sistema o a nivel de red. Los primeros realizan su labor a través del análisis de distintos parámetros del sistema como los ficheros de registro (logs) o la integridad de los archivos. Los segundos realizan su labor a través del análisis del tráfico de red.

205. En ambos casos existen dos aproximaciones distintas para detectar la presencia de actividad maliciosa:

– Buscar indicios de ataques concretos.

– Analizar el perfil del comportamiento habitual del sistema o la red para detectar actividades que se alejen de su perfil habitual.

206. Los ataques y los compromisos de sistemas o redes a menudo no dejan ninguna traza rastreable, por lo que es importante poder detectar cuándo se está produciendo un ataque y poder identificar si el ataque ha tenido éxito o no.

207. En este sentido los IDS son una potente herramienta. Los IDS a nivel sistema y los de red tienen ventajas e inconvenientes que los hacen complementarios.

7.1.1. IDS A NIVEL DE RED

208. Los IDS a nivel de red tienen las siguientes ventajas:

– **Eficiencia**: con un número reducido de sensores se puede cubrir toda la Organización.

209. Los IDS a nivel de red tienen las siguientes desventajas:

– **Falsos positivos**: producidos por la falta de perspectiva acerca de la situación y características concretas del sistema destinatario del tráfico.

– Imposibilidad de monitorizar **tráfico cifrado**.

– Dificultad para operar en entornos con un **alto volumen de tráfico**.

– Inadecuada implementación.

- **Dificultad de operación**: Falta de conocimientos por parte de los analistas y operadores para configurar y realizar el mantenimiento y operación de forma adecuada.

210. Debido a estas desventajas, algunas Organizaciones perciben los IDS a nivel de red como elementos con poco retorno de inversión.

211. Las nuevas generaciones de IDS van dando respuesta a estos problemas mediante el uso de inteligencia adicional en el dispositivo.

212. A pesar de los problemas mencionados, si se realiza una adecuada configuración y mantenimiento, estos dispositivos se convierten en un elemento fundamental de la seguridad perimetral que permite verificar el cumplimiento de la política de seguridad y ayudar a determinar cuándo se producen incidentes de seguridad.

7.1.2. IDS A NIVEL DE SISTEMA

213. Los IDS a nivel de sistema tienen las siguientes ventajas:

- Facilidad de monitorización de los destinatarios finales, con sus propias características y estado concreto, frente a la del tráfico.
- Determinan con una **menor probabilidad de error** si un ataque ha tenido éxito o no.

214. Los IDS a nivel de sistema tienen las siguientes desventajas:

- **Escalabilidad** complicada: han de ser instalados en todos los sistemas que se desea supervisar
- **Dificultad de gestión**: requieren de algún medio centralizado para realizar su mantenimiento, gestión de alertas, etc.
- Elevado **coste** de las versiones comerciales de los mismos
- Su configuración, mantenimiento y gestión suelen ser más complejos y requerir mayor dedicación y conocimiento que otros dispositivos de seguridad perimetral.

215. Debido a estas desventajas, en la mayor parte de los casos su implantación se ve reducida a sistemas críticos o muy expuestos.

7.2. SISTEMAS DE PREVENCIÓN DE INTRUSIONES

216. Los sistemas de prevención de intrusiones (*Intrusion Prevention Systems - IPS*) utilizan una aproximación parecida a la de los IDS para detectar ataques, pero además detectarlos y generar algún tipo de alerta, los IPS intentan detenerlos. Al igual que sucede en el caso de los IDS, existen **IPS a nivel de red** y **a nivel de sistema**.

217. En lo que respecta a los IPS a nivel de red, en cierto modo, se pueden considerar como cortafuegos que en lugar de juegos de reglas utilizan firmas y análisis de anomalías para denegar o permitir el tráfico.

218. Los IPS de red no pueden permitirse falsos positivos o estarían rechazando tráfico válido. Para ello, se utilizan las estrategias más estables de las tecnologías de IDS, reglas mucho más exactas, análisis de anomalías y otros mecanismos que permiten minimizar esta probabilidad.

219. La utilización de IPS es recomendable tanto a nivel sistema como a nivel red, aunque suele suponer una inversión considerable. Es adecuado seguir las mismas pautas definidas para los IDS en cuanto a priorizar sistemas expuestos o críticos.

7.3. CONCENTRADORES DE VPN

220. Las VPN son utilizadas fundamentalmente para proporcionar a usuarios móviles, colaboradores, socios o sucursales un medio que les permita acceder de forma segura a los recursos de la Organización cuando la conexión ha de realizarse en un entorno inseguro como puede ser Internet.

221. La mayor parte de los productos de cortafuegos actuales proporcionan esa funcionalidad, aprovechando su posición privilegiada a la entrada del perímetro y combinando VPN con control de acceso, filtrado de contenidos, control de admisión a la red, registro, etc.

222. Sin embargo, el cifrado de las VPN suele imponer una alta carga de proceso al cortafuegos. Cuando crece el número de conexiones este efecto puede ocasionar que el cortafuegos se sobrecargue, pudiendo afectar a su habilidad de filtrar paquetes.

223. La solución a este problema puede ser utilizar un "concentrador de VPN".

224. Existen dos tipos de concentradores de VPN:

- soluciones cerradas, con hardware criptográfico que se encargue del cifrado
- servidores generalistas, con el software necesario para gestionar y establecer las VPN.

8. CICLO DE VIDA DEL CORTAFUEGOS

225. Una vez concluida la elaboración de la política de seguridad, llega el momento de su aplicación. Se deben definir los elementos que han de formar parte de la infraestructura de seguridad perimetral para que cumplan los requisitos establecidos por la política.

226. El despliegue de la infraestructura de seguridad sigue a lo largo de su vida 4 hitos importantes: diseño, implementación, gestión y retirada.

8.1. DISEÑO

227. Un buen diseño de una infraestructura de seguridad perimetral debe combinar los distintos elementos para alcanzar un equilibrio adecuado entre funcionalidad y seguridad, garantizando que la Organización puede desarrollar su actividad con las suficientes garantías de seguridad en lo que a integridad, confidencialidad y disponibilidad del conjunto de la infraestructura, servicios, información y transacciones se refiere. Todo ello dentro de los límites y parámetros que hayan sido definidos en la política de seguridad.

8.1.1. PARÁMETROS DE DISEÑO

228. A continuación se destacan algunos de los parámetros que se han de tener en cuenta a la hora de diseñar cualquier arquitectura de seguridad perimetral. Muchos de estos parámetros son comunes a cualquier implementación de seguridad, mientras que otros lo serán en concreto para el caso de la seguridad perimetral.

8.1.1.1 SEGURIDAD EN PROFUNDIDAD.

229. La “seguridad en profundidad” o “seguridad multicapa” debe estar siempre presente en cualquier implementación de seguridad.

230. Cualquier implementación de una política de seguridad se enfrenta a los siguientes riesgos:

- ninguna tecnología es infalible
- pueden existir errores de configuración
- en ocasiones es preciso optar por configuraciones subóptimas desde el punto de vista de la seguridad para poder proporcionar una funcionalidad
- no se puede evitar que en algún momento alguna parte de nuestra infraestructura pueda llegar a ser comprometida

231. La solución adoptada consiste en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las tecnologías falle o que permita, al menos, minimizar el impacto si el compromiso llega a materializarse.

232. Las implicaciones de este concepto en el mundo de la seguridad perimetral son claras. No se debe de confiar en el cortafuegos como único dispositivo para garantizar la seguridad de las redes y sistemas sino que ha de garantizarse un reforzamiento a todos los niveles (red, sistema operativo y servicio). Estas son algunas de las estrategias que se pueden poner en marcha:

- Securización de los sistemas operativos, especialmente en los servidores expuestos.
- Securización de los servicios.
- Separación de servicios en distintos sistemas de acuerdo con su criticidad, muy en especial aquellos sensibles o especialmente vulnerables como DNS, SMTP, web, bases de datos, etc.
- Aplicación del principio de mínimo privilegio (para usuarios, red y servicios).
- Securización de los dispositivos de red que interconecten dispositivos expuestos.
- Cifrado de las comunicaciones.
- Introducción de sistemas de detección y prevención de intrusiones (IDS e IPS), tanto a nivel de sistema como de red.
- Biodiversidad.
- Duplicación de las capas de dispositivos de seguridad críticos.

233. Otro factor a tener en cuenta es el equilibrio entre el esfuerzo y los costes de implementación y mantenimiento y el índice real de riesgo e impacto de una posible intrusión.

234. Tomar las medidas destacadas anteriormente en todos y en cada uno de los sistemas y dispositivos de la Organización sería deseable, pero normalmente es un objetivo inalcanzable. Al menos, debe garantizarse su aplicación en aquellos sistemas especialmente expuestos o críticos para la Organización.

8.1.1.2 COMPLEMENTARIEDAD DE TECNOLOGÍAS

235. Suele haber siempre una gran controversia acerca de que tecnología es mejor que otra a la hora de incrementar la seguridad de sistemas y redes. Aunque en términos generales unas tecnologías sean más eficaces que otras, se deberá seleccionar la más adecuada para proteger mejor cada entorno concreto.

236. Hay que intentar evitar caer en tópicos o modas, que tienen en muchas ocasiones su origen en la necesidad de los fabricantes de dar salida a un producto concreto, y hacer uso

de aquel conjunto de tecnologías y aproximaciones que hayan demostrado ser eficaces en el entorno de actuación concreto.

8.1.1.3 PRINCIPIO DE MÍNIMO PRIVILEGIO

237. Uno de los principios de seguridad más eficaces es el conocido como principio de mínimo privilegio y se engloba dentro de la utilización de estrategias conservadoras a la hora de plantear la estrategia de seguridad. Dicho principio estipula que a la hora de conceder privilegios para la realización de una función concreta, no se deben de conceder más de los que sean estrictamente necesarios.

238. Como extensión, se debe tender a aplicar el principio de mínimo privilegio incluso si se corre el riesgo de producir un mal funcionamiento, no crítico, del servicio. Es decir, ante la duda de conceder más privilegios por miedo a que algo deje de funcionar correctamente, han de considerarse las medidas más restrictivas y a partir de ahí corregir los problemas que puedan derivarse, nunca al revés.

8.1.1.4 SIMPLICIDAD

239. Una de las estrategias más importantes a la hora de poner en marcha cualquier funcionalidad, es estudiar todas las posibilidades y elegir la más sencilla de entre las que cumplan los requisitos necesarios.

240. Esta regla es especialmente recomendable al poner en marcha arquitecturas de seguridad o juegos de reglas en los cortafuegos. El contar con estructuras complejas suele hacer difícil el análisis y la verificación de los mismos, permitiendo que aparezcan agujeros en los controles establecidos y que ocurran errores humanos que no son detectados.

241. Este principio se conoce también como KISS (*Keep It Simple, Stupid*).

8.1.1.5 BIODIVERSIDAD

242. Por biodiversidad se entiende la introducción de elementos que proporcionen la misma funcionalidad pero que sean distintos en su tecnología, como pueden ser dos cortafuegos de distintos fabricantes. El requisito previo, por supuesto, es que ambos dispositivos cuenten con las características de funcionalidad necesarias para poder desempeñar adecuadamente su papel en la red, y que su coexistencia no suponga ningún inconveniente.

243. Se pretende reducir el impacto de los problemas de seguridad intrínsecos a cada tecnología (por ejemplo un fallo en el sistema operativo o en el propio *software* de cortafuegos), de modo que no sea posible utilizar la misma vulnerabilidad para atacar a otros dispositivos análogos. La arquitectura se vuelve resistente a fallos simples en uno de sus elementos.

244. La biodiversidad puede ser aplicada a distintos niveles como sistemas operativos, servicios, hardware, etc.

245. Hay que tener ciertas precauciones a la hora de poner en práctica una estrategia de biodiversidad dentro de la Organización. Mantener servicios y plataformas con distintas tecnologías implica un mayor esfuerzo de gestión y mantenimiento y la necesidad de contar en la Organización con personal especializado en todas las tecnologías usadas, por lo que en general será conveniente ceñir la elección a plataformas y productos que ya existan y estén siendo mantenidos dentro de la Organización, y para los que ya se cuente

con el personal adecuado, e ir ampliando el catálogo de manera paulatina para poder absorber los costes.

8.1.1.6 CONTROL DE ACCESO

246. Ha de asegurarse que la arquitectura elegida obliga al tráfico de red a pasar por los puntos de control de acceso señalados y que no existe ningún camino que pueda escapar a dicho control.

8.1.1.7 ADECUACIÓN A LAS NECESIDADES PRODUCTIVAS Y DE RIESGO

247. Es importante que el diseño de seguridad perimetral, además de proporcionar seguridad, obedezca a las necesidades productivas de la Organización, proporcionando una herramienta más al servicio de la misma y no un impedimento para realizar sus funciones.

248. Este equilibrio ha de estar claramente definido para que una necesidad productiva no se pueda usar como excusa para degradar los requisitos de seguridad. Asimismo, deberá ser adecuada a los niveles de riesgo y tipos de amenaza a los que la Organización esté expuesta.

8.1.1.8 ESCALABILIDAD

249. Las necesidades de una Organización no son estáticas sino dinámicas. Es previsible que la Organización crezca, por lo que cualquier diseño ha de tener esto en cuenta.

250. Será necesario dimensionar adecuadamente los cortafuegos para que puedan soportar el previsible incremento de tráfico, número de conexiones y, posiblemente también, de subredes conectadas al mismo sin tener que llevar a cabo cambios drásticos de hardware o software. Esto es especialmente importante si se van a utilizar redes privadas virtuales, dado que suelen ser computacionalmente muy intensivas.

251. También es adecuado conocer el límite operativo de la arquitectura diseñada, y prever las alertas necesarias que permitan detectar cuándo el crecimiento se acerca a dicho límite para afrontar los cambios necesarios con suficiente antelación.

8.1.1.9 REDUNDANCIA

252. Una buena arquitectura de sistemas, redes y procedimientos debe evitar o limitar el daño producido por la falta de disponibilidad de los distintos componentes de la infraestructura, ya sea por eventualidades de tipo malicioso o no. Pero siempre hay que mantener el equilibrio entre el coste que supone la redundancia y el riesgo que supone duplicar la infraestructura, que es costoso e introduce nuevos niveles de complejidad y nuevos posibles puntos de vulnerabilidad.

8.1.2. ELEMENTOS DE LA ARQUITECTURA

253. A la hora de diseñar la solución de seguridad perimetral, han de tenerse en cuenta las distintas zonas de las que se compone la red, reflejando el nivel de seguridad de cada subred concreta. Las zonas más habituales son:

- **Intranets**: redes internas a la Organización.
- **DMZ**: zonas desmilitarizadas (*De-Militarized Zone*). Redes con un nivel de protección intermedio entre las internas y las externas.

– **Extranets**: redes privadas establecidas con otras Organizaciones con el fin de compartir algún tipo de recurso o servicio.

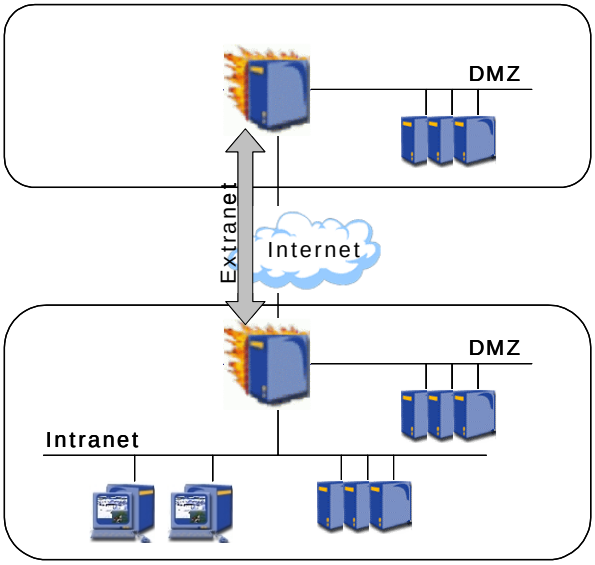

Figura 13. Intranet, DMZ, Internet, Extranet

254. Algunos autores más puristas definen DMZ de acuerdo con su concepción militar, es decir la zona que está entre los elementos propios y el enemigo. Según esta definición, la DMZ residiría en el espacio situado entre el cortafuegos e Internet. Sin embargo, en este documento se va a seguir la concepción más habitual de DMZ, que la que se puede ver en la **Figura 13**.

255. En esta definición, DMZ no se refiere a una única red sino a varias, dado que existen redes expuestas, aisladas y protegidas en distintos puntos de la arquitectura. Incluso en un mismo cortafuegos, se pueden establecer diferentes DMZ si existe la necesidad de establecer distintas zonas de seguridad debido a distintos requisitos.

8.1.3. PROCEDIMIENTO DE DISEÑO

256. Al emprender el diseño de la arquitectura de seguridad deben considerarse los siguientes aspectos:

8.1.3.1 POLÍTICA DE SEGURIDAD

257. La política de seguridad es el resultado de un análisis de las necesidades productivas, de riesgo y de requisitos de seguridad de la Organización, por lo que ha de constituirse en la guía de referencia para la elección e implantación de tecnologías y diseños concretos.

8.1.3.2 CLASIFICACIÓN EN NIVELES DE SEGURIDAD

258. Partiendo como base de la política de seguridad establecida, lo primero que habrá de hacerse será identificar claramente las distintas zonas de seguridad presentes en la Organización. Han de separarse eficazmente aquellas redes, sistemas o servicios que requieran condiciones de seguridad distintas o estén sometidos a riesgos distintos. Un ejemplo típico de zona de seguridad es la DMZ externa en la que suelen residir los sistemas que ofrecen servicios al exterior, como servidores de correo, web, DNS, etc.

259. Para cada servicio ofertado e información gestionada, y para cada departamento, socio o colaborador de la Organización que vaya a tener acceso a esa información o servicio, debe determinarse cuál es su nivel de seguridad y confianza, y si éste se corresponde con el del resto de los elementos que comparten el mismo entorno (ya sea físico, de red, de sistema, etc.).

260. De no ser así, se deben separar los servicios e información en áreas de seguridad mediante elementos de control que sean capaces de verificar adecuadamente el flujo de información entre distintos niveles de seguridad. En términos de red, esta función la llevarán a cabo prioritariamente los cortafuegos, que proporcionan.

- Segregación del tráfico entre áreas
- Control y registro del tráfico de red entre áreas
- autenticación y autorización requeridas
- cifrado necesario para garantizar la confidencialidad.

261. No deben existir sólo elementos de seguridad perimetral entre el interior y el exterior de la Organización, sino incluso dentro de la misma Organización en tantos puntos como sean necesarios para garantizar la separación apropiada de las diferentes zonas de seguridad.

8.1.3.3 DISPOSITIVOS DE RED

262. Los dispositivos de red (*switches*, enrutadores, etc.) representan el sustento del resto de la infraestructura. Por eso es importante definir qué dispositivos se van a utilizar, cómo se van a configurar, si se va a hacer uso de VLAN o no, etc.

8.1.3.4 CORTAFUEGOS

263. Una vez establecido cuántos niveles de seguridad son necesarios, cuál va a ser su grado de protección, qué flujo de información se va a permitir entre ellos y cómo se va a controlar ese flujo, se deben utilizar los medios adecuados que habitualmente, aunque no necesaria ni exclusivamente, se basarán en cortafuegos.

264. Algunos de los detalles a tener en cuenta serán:

- **Número** de cortafuegos necesarios y localización de los mismos en la red.
- Necesidades de **autenticación** y mecanismos más adecuados para implementarla.
- Necesidades de **registro y alertas**, así como necesidades de recolección y almacenamiento.
- Necesidades de **cifrado**.
- Necesidades de **filtrado de contenidos**.
- Necesidades de **prevención de intrusiones**.
- **Funcionalidades adicionales** como NAT, alta disponibilidad, balanceo de carga, etc.

265. Muchas de estas funcionalidades están disponibles en otros tipos de dispositivos aparte del cortafuegos, que en ocasiones no es el elemento más adecuado. Si se considera necesario, se pueden migrar determinadas funciones a otros dispositivos que puedan efectuarlas de forma apropiada dentro de los márgenes establecidos en la política de seguridad.

266. Es necesario definir los procedimientos a seguir para cambiar la política de seguridad del cortafuegos:

- Proceso de solicitud de cambios.
- Autorización necesaria.
- Procedimiento de introducción de cambios.
- Requisitos de documentación.

8.1.3.5 DISPOSITIVOS ADICIONALES

267. Se deben elegir los elementos que permitan construir la arquitectura de seguridad manteniendo los requisitos de funcionalidad y operatividad de la Organización. Los cortafuegos ocupan un papel preponderante en dicha arquitectura, pero pueden ser complementados por otros elementos.

268. Una vez que los cortafuegos están colocados en su sitio, es el momento de poblar la red con otras medidas de seguridad como las mencionadas en su momento: IDS, IPS, *Honeypots*, sistemas de gestión de eventos, etc.

269. La decisión de introducir un elemento u otro ha de estar dirigida por un conocimiento de lo que se quiere proteger, de los riesgos existente y las tecnologías de seguridad existentes. Se han de seguir las pautas adecuadas para que la introducción de dichos elementos resulte eficaz y no suponga riesgos adicionales e innecesarios.

270. Finalmente, una buena arquitectura de seguridad no puede centrarse únicamente en la implantación y configuración de cortafuegos y otros elementos de seguridad, por muy bien que se lleve a cabo. Todos los despliegues de seguridad son tan fuertes como el elemento más débil. Por ello se deben tener en cuenta el resto de elementos de la infraestructura, como sistemas operativos, servicios, enrutadores, etc., y se deben cuidar también aspectos como la seguridad física de éstos.

8.1.3.6 ANÁLISIS DE ESCALABILIDAD

271. Es importante tener en cuenta las capacidades de los productos elegidos a la hora de afrontar la evolución y probable crecimiento de la Organización. Si es posible, es recomendable realimentar esta información en el diseño.

8.1.4. DISEÑOS BÁSICOS

8.1.4.1 SMALL OFFICE - HOME OFFICE (SOHO)

272. La arquitectura más simple a la hora de diseñar la solución de seguridad es aquella en la que la Organización no ofrece ningún servicio en Internet. Esta arquitectura constituye un escenario típico para redes domésticas, pequeñas Organizaciones o sucursales también conocidas como *Small Office - Home Office* o SOHO.

273. En estos casos puede bastar con un simple enrutador que hace las funciones de cortafuegos, como se muestra en la **Figura 14**.

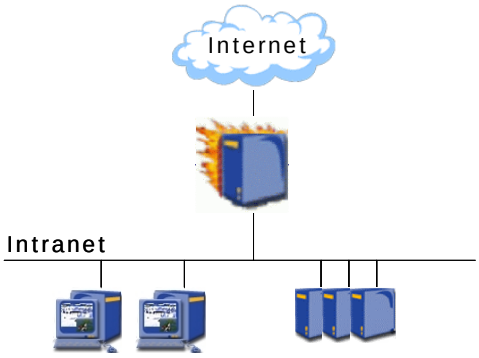

Figura 14. Diseño de red doméstica o de pequeña oficina típica

8.1.4.2 UNA DMZ

274. El segundo caso, más habitual en Organizaciones de mayor tamaño, contempla el que se puedan ofrecer servicios al exterior. Los servicios ofrecidos están expuestos a un mayor riesgo que el resto de los sistemas de las redes internas y por tanto en un nivel de seguridad distinto.

275. Con objeto de evitar que el compromiso de uno de los servidores acabe comprometiendo a toda la infraestructura se separan los servicios públicos del resto de los sistemas internos con una DMZ, tal y como se muestra en la **Figura 15**.

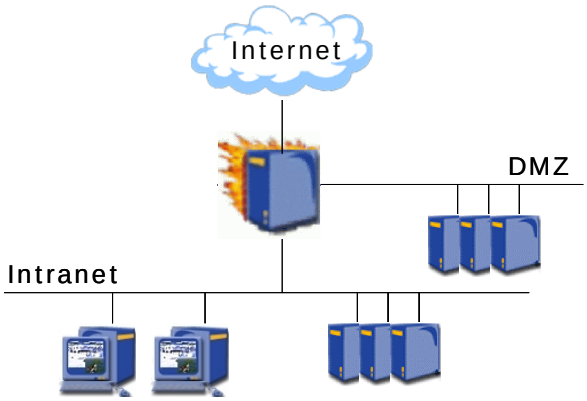

Figura 15. Diseño en tres zonas, con una DMZ

276. Este diseño es un tanto simplista y quizás no refleje la realidad de la Organización. En una Organización de tamaño medio será deseable mantener separados dentro de la red interna los servidores críticos de las estaciones de usuario.

8.1.4.3 DISEÑO MULTIZONA CON VARIOS CORTAFUEGOS

277. Conviene recordar que los ataques pueden tener origen interno, ya sea porque de alguna forma se ha conseguido romper el perímetro (dispositivos inalámbricos, ruptura del perímetro desde dentro hacia fuera, etc.), por la infección de *malware* (virus, gusanos, etc.) o porque el ataque proviene de un usuario interno malicioso. En cualquier caso, se debe intentar que el atacante interno no pueda aprovechar esa situación de privilegio, creando una nueva jerarquía que proteja los recursos propios más críticos, tal y como se muestra en la **Figura 16**.

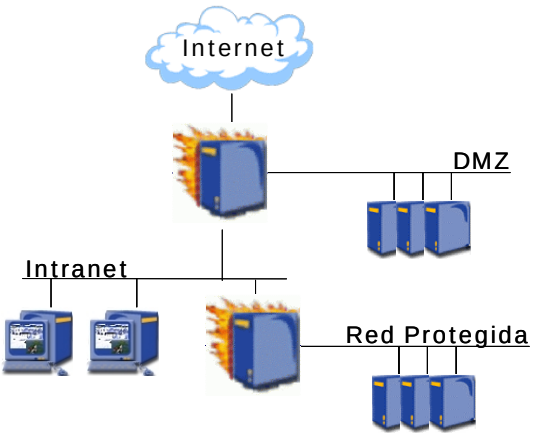

Figura 16. Diseño multizona con varios cortafuegos

8.1.4.4 DISEÑO MULTI-DMZ CON UN CORTAFUEGOS

278. Es habitual que los servidores de la DMZ externa (típicamente servidores de correo, web, etc.) tengan que comunicarse con servidores de las redes internas. Si un servidor de la DMZ es comprometido, cuenta con una posición ventajosa para atacar a los servidores de las redes internas con los que se comunica. Por eso es una buena idea separarlos de otros servidores críticos para la Organización, configurando una red dedicada como se muestra en la **Figura 17**.

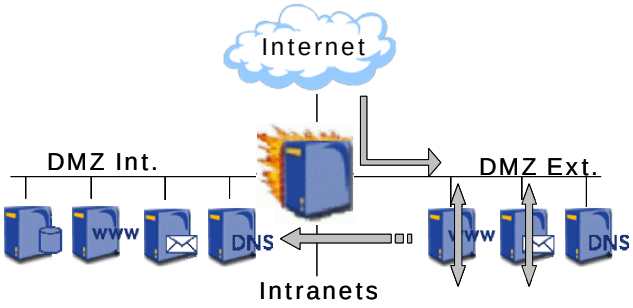

Figura 17. Diseño con dos DMZ y un sólo cortafuegos

279. El gran problema que presenta la configuración anterior es la existencia de un punto único de fallo de seguridad en el cortafuegos de entrada. Si el cortafuegos es comprometido, toda la red quedaría comprometida.

8.1.4.5 DISEÑO MULTI-DMZ CON VARIOS CORTAFUEGOS

280. En el caso de una estructura con mulítples DMZ, igual que en las redes multizona, es aconsejable utilizar varios cortafuegos como se muestra en la **Figura 18**.

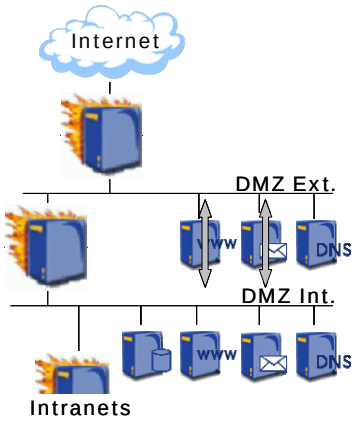

Figura 18. Diseño con dos DMZ multicapa

281. Una infraestructura multicapa con varios cortafuegos tiene las siguientes ventajas:

- Se introducen capas adicionales de seguridad gracias a la presencia de dos nuevos cortafuegos en la arquitectura.
- Se puede llegar a gestionar redes más complejas cumpliendo todos los requisitos de seguridad de una Organización. Además, a medida que el número de interfaces de red crece, la configuración se hace más compleja, dando pie a frecuentes errores..
- Un sólo cortafuegos supone un punto de fallo único de seguridad en la red, aunque se encuentre en una configuración de alta disponibilidad (todos los dispositivos que forman parte de un grupo suelen tener las mismas características). Si el cortafuegos es comprometido toda la infraestructura queda automáticamente comprometida.

282. Se recomiendan las siguientes buenas prácticas al diseñar una infraestructura multicapa:

- Los cortafuegos elegidos deben ser de distintos fabricantes (biodiversidad) para garantizar un grado más de seguridad.
- El enrutador de perímetro no debe ejercer las funciones del primer cortafuegos de la arquitectura. Esto puede ser una ventaja en términos de facilidad de mantenimiento y gestión pero redunda en una solución menos segura, dado que los cortafuegos suelen contar con medidas adicionales de seguridad (inspección de protocolos) no incluidas en los enrutadores.
- Distintos cortafuegos deben ser gestionados por distintos equipos de administradores.
- Alcanzar un equilibrio entre el número de dispositivos y de redes por dispositivo que satisfaga los requisitos de separación en zonas de seguridad y prevenga daños críticos en caso de compromiso. Tan malo es un solo cortafuegos como un número excesivo con sólo dos interfaces por dispositivo, que aumenta la inversión necesaria y la complejidad de la gestión..

283. Es habitual llegar a un término medio como el que aparece en la **Figura 19** (conocido a veces como *service leg*), en el que el enrutador de perímetro actúa como primera línea de defensa apoyando al primer cortafuegos.

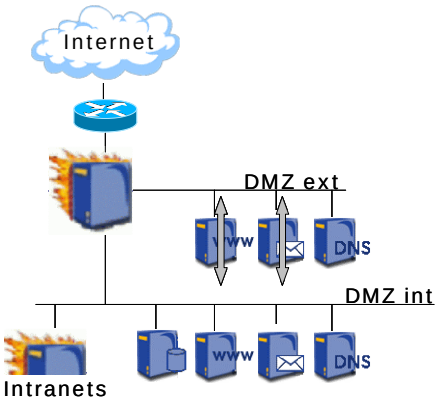

Figura 19. Arquitectura con dos DMZ en modo "service leg"

8.1.4.6 DISEÑO MULTI-DMZ POR VLAN

284. Utilizando VLAN, si el cortafuegos lo soporta, es posible aislar servidores dentro de un mismo nivel de seguridad. En la **Figura 20**, se puede ver como los servidores de correo, de nombres y web de la DMZ han sido aislados en sendas VLAN y conectadas a un cortafuegos que soporta este tipo de filtrado virtual.

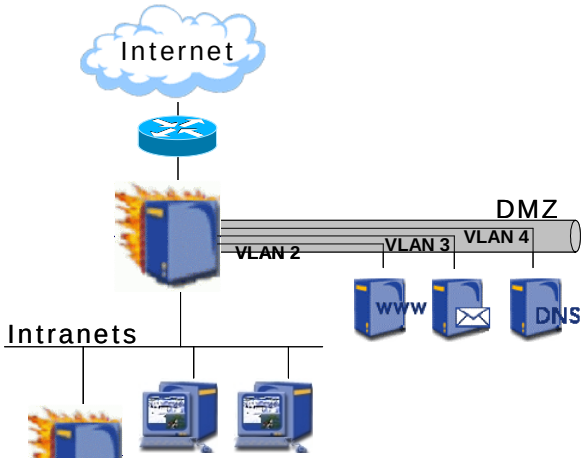

Figura 20. Cortafuegos sobre VLAN

8.1.5. ARQUITECTURAS DE VPN

285. Como se ha explicado en el apartado “7.3 Concentradores de VPN”, existen dos soluciones para la gestión de las VPN. La primera consiste en utilizar el propio cortafuegos su posición privilegiada a la entrada del perímetro, tal y como se muestra en la **Figura 21.**

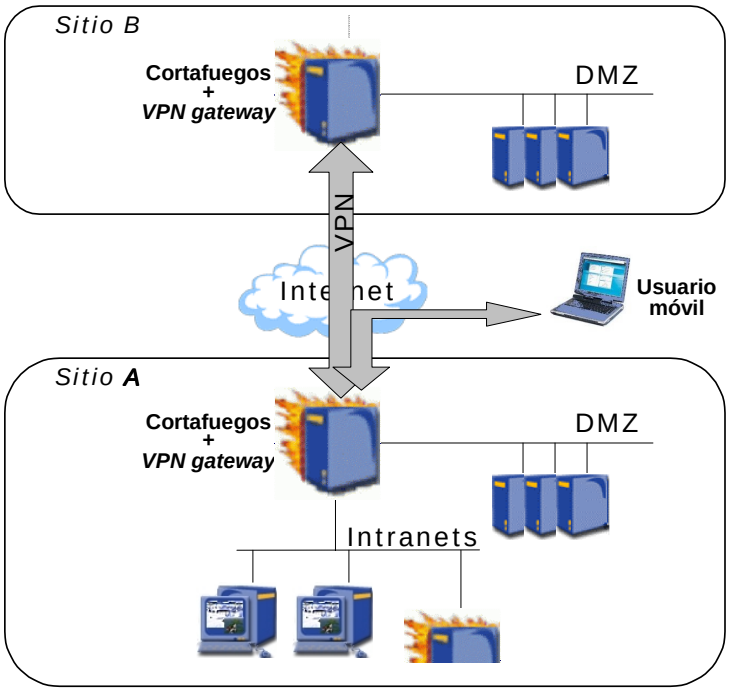

Figura 21. Configuración típica de acceso VPN

286. La segunda solución pasa por la utilización de concentradores de VPN. La situación que debe ocupar un concentrador de VPN en la red depende de dónde se requiera dicha funcionalidad, pero es habitual encontrarlo en la entrada de la Organización. Las opciones más habituales de posicionamiento son:

- Entre el cortafuegos y el exterior. No se recomienda esta configuración. El concentrador de VPN no está protegido por el cortafuegos y queda expuesto a posibles ataques desde el exterior.
- En la red interna, detrás del cortafuegos. No se recomienda esta configuración. El tráfico dirigido hacia al concentrador está cifrado cuando atraviesa el cortafuegos, por lo que no se puede analizar, aplicarle las políticas de seguridad necesarias, filtrarlo por contenido, someterlo a detección o prevención de intrusiones, etc. Sólo es recomendable si se puede garantizar que las redes conectadas poseen el mismo nivel de seguridad y no es posible situarlo en otra posición por necesidades de confidencialidad o similares.
- En una DMZ dedicada. Es la configuración recomendada. El concentrador puede quedar debidamente protegido por el cortafuegos y se puede controlar el tráfico que va desde el concentrador hacia el interior. Esta situación se muestra en la **Figura 22**.

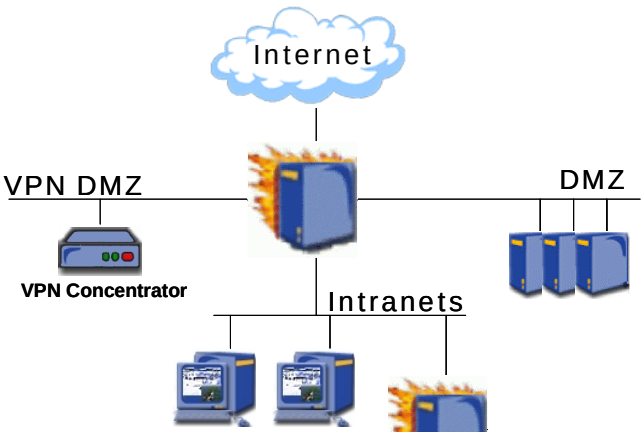

Figura 22. Concentrador VPN externo

287. Cualquiera que sea la opción elegida, se debe recordar que algunas configuraciones de VPN pueden tener problemas con la traducción de direcciones, lo que debe tenerse en cuenta a la hora de elegir un posicionamiento adecuado en la red.

8.1.6. EJEMPLO DE ARQUITECTURA DE SEGURIDAD PERIMETRAL MULTICAPA

288. A continuación se desarrolla un ejemplo de arquitectura que combina los elementos introducidos en este documento. Este ejemplo no constituye la mejor arquitectura posible para cualquier Organización, que ha de ser diseñada en cada caso a partir de un proceso de análisis detallado.

289. Este diseño incluye, siguiendo un orden desde fuera hasta adentro:

- Un enrutador que actúa como primera capa de protección de la Organización.
    - Capacidades: filtro de paquetes para eliminar "ruido" y algunos tipos de tráfico malicioso.
    - Conectado a: Internet y el primer cortafuegos
- Un primer cortafuegos de la Organización, configurado en alta disponibilidad con dos elementos hardware. Protege adecuadamente a los servidores de la DMZ externa.
    - Capacidades: memoria del estado de las conexiones, inspección de protocolos y de contenidos. Opcionalmente, punto concluyente de VPN.
    - Conectado a: enrutador externo, DMZ externa, DMZ interna y un inspector de contenidos.
- Una DMZ externa, que incluye, aislados en VLAN distintas para añadir un nivel más de protección, dada la exposición de estos servidores, los frontales de acceso a los servicios exteriores:
    - un proxy de correo.
    - un proxy inverso de web, destinado a proteger a los servidores web situados en la DMZ interna y opcionalmente a aplicar filtrado y otras medidas de seguridad, que se comunicarán con sus homólogos en la DMZ interna.
    - un servidor de nombres configurado como primario de la Organización de cara al exterior DNS-R-ext (en una configuración *Split DNS*), pero que en

realidad es una réplica del maestro que está en la DMZ protegida (DNS-M-ext).

- Un servidor de inspección de contenidos, conectado en otro interfaz del cortafuegos externo.
- Una DMZ interna, más protegida que la DMZ externa, pero aún segregada de las redes internas. Tendrá contacto con los servidores más expuestos de la DMZ externa. En ella se pueden encontrar:
    - El servidor de correo,
    - El servidor de base de datos que hace de backend al servidor web.
    - El servidor maestro DNS (DNS-M) de cara al exterior.
- Un segundo cortafuegos que separa la DMZ interna de las redes internas.
    - Capacidades: NAT para las redes internas
    - Conectado a: DMZ interna, red wireless, el cortafuegos de las redes internas de usuarios de las estaciones de trabajo (Intranets), el cortafuegos interno.
- Una red wireless que, debido al riesgo que entraña, ha de estar siempre segregada del resto de redes.
- Un cortafuegos de redes departamentales
    - Conectado a: segundo cortafuegos, todas las Intranets
- Varias Intranets (Redes internas departamentales), que a menudo no tienen los mismos requisitos de seguridad y deben ser separadas. Si se utilizan los propios enrutadores, puede suponer una menor garantía de seguridad. En el esquema posterior se representan dos, pero pueden existir más.
- Un cortafuegos interno, usado para proteger el nivel inferior, donde se encuentran las redes más sensibles de la Organización, las que guardan los recursos más críticos.
    - Conectado a: segundo cortafuegos, cortafuegos de las redes internas, DMZ protegida, Red protegida
- Una DMZ protegida en la que los proxies o servidores de réplica servirán de puente para ofrecer los servicios necesarios al resto de redes de la Organización: servidor primario de DNS para los servicios internos (DNS-R-int), réplica del servidor maestro (DNS-M-int), servidor réplica de autenticación, servidor réplica de base de datos, etc.
- Una red protegida, en la que se hallan los servidores maestros DNS para los servicios internos (DNS-M-int), de autenticación, bases de datos, etc., que no tendrá contacto con el resto de las redes excepto con la DMZ protegida.

290. La práctica de emplear **réplicas en producción**, manteniendo los servidores maestros aislados en una zona más protegida (tanto para los servicios internos, separando la Red Protegida de la DMZ Protegida, como para los servicios externos, con las DMZ externa e interna) y restringiendo la comunicación de los mismos exclusivamente a la réplica, permite añadir una nueva capa de protección frente a ataques directos a dichos servidores (recursos críticos) una vez que un atacante ha ganado acceso a las redes internas. La réplica debe c**onfigurar**se **de modo más restrictiv**o posible (por ejemplo, sólo lectura) y debe ser reforzada adecuadamente.

291. Para acceder a los servidores críticos situados en la red restringida, un atacante tendría que salvar múltiples barreras. Si a este esquema se le añaden sistemas de detección y prevención de intrusiones en cada una de las subredes como los que aparecen en la figura,

la seguridad del conjunto se vería tremendamente fortalecida y, muy probablemente, se estaría en condiciones de responder en tiempo adecuado a un intento de acceso no autorizado.

292. Es aconsejable que los servidores de las DMZ (interna, externa, protegida) cuenten con un **cortafuegos a nivel sistema** de forma que sólo se permita el tráfico exclusivamente necesario para realizar su función. De esta manera, se dificultaría el acceso al mismo en el caso de que otro servidor fuera comprometido.

293. En la **Figura 23** se muestra el esquema de la arquitectura diseñada.

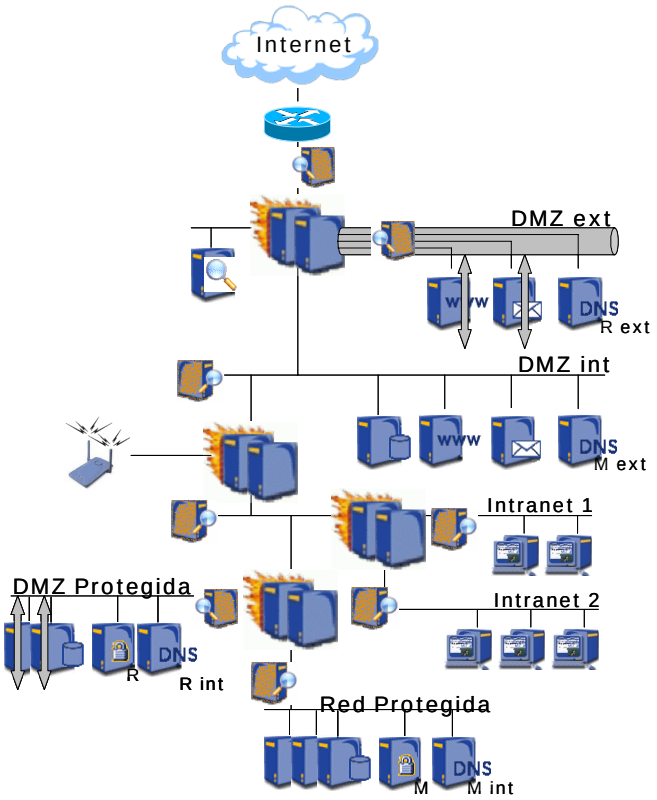

Figura 23. Arquitectura de seguridad perimetral multicapa

294. Como parte de este ejemplo, se incluye un posible juego de reglas para el cortafuegos más externo de la Organización, que se encuentra inmediatamente después del enrutador.

295. La política de seguridad con respecto al acceso hacia/desde el exterior para este ejemplo es:

- El tráfico proveniente desde el exterior quedará exclusivamente restringido a los servidores situados en la *DMZ* externa.
- El tráfico de las redes internas hacia el exterior quedará restringido a web y ftp.

296. A esta política de seguridad y arquitectura concretas le correspondería el siguiente juego de reglas en el cortafuegos más externo:

Protocolo	*Dir. Origen*	*Puerto Origen*	*Dir. Destino*	*Puerto destino*	*Acción*	*Registro*
[1]	consola cortafuegos	[1]	cortafuegos	[1]	aceptar	si
cualquiera	cualquiera	cualquiera	cortafuegos	cualquiera	denegar	alerta
[1]	cortafuegos	[1]	serv.filt.contenidos	[1]	aceptar	no*
tcp	cualquiera	cualquiera	$correo_{DMZext}$	25	aceptar	no *
tcp	cualquiera	cualquiera	$correo_{DMZext}$	123	rechazar	no
tcp	$correo_{DMZext}$	cualquiera	$correo_{DMZint}$	25	aceptar	no *
tcp	$correo_{DMZext}$	cualquiera	$correo_{DMZint}$	123	rechazar	No
tcp/udp	cualquiera	cualquiera	dns_{DMZext}	53	aceptar	no *
tcp/udp	dns_{DMZext}	cualquiera	dns_{DMZint}	53	aceptar	no *
tcp	cualquiera	cualquiera	www_{DMZext}	80	aceptar	no *
tcp	cualquiera	cualquiera	www_{DMZext}	443	aceptar	no *
tcp	www_{DMZext}	cualquiera	www_{DMZint}	80	aceptar	no *
tcp	www_{DMZext}	cualquiera	www_{DMZint}	443	aceptar	no *
tcp	redes internas	cualquiera	Exterior	21	aceptar	no *
tcp	redes internas	cualquiera	Exterior	80	aceptar	no *
tcp	redes internas	cualquiera	Exterior	443	aceptar	no *
tcp	DMZ ext	cualquiera	Cualquiera	cualquiera	denegar	alerta
tcp	serv.filt.contenidos	cualquiera	Cualquiera	cualquiera	denegar	alerta
tcp	cualquiera	cualquiera	Cualquiera	cualquiera	denegar	Si

*** Realizar el registro de todas las conexiones es deseable, pero en una red de con un tráfico elevado puede ser inviable debido a los requisitos de almacenamiento y la penalización en el rendimiento del cortafuegos. La decisión final dependerá del entorno concreto de producción.**

[1] Los protocolos y puertos fijados dependerán del producto concreto utilizado.

297. El juego de reglas anterior está agrupado por protocolos para facilitar su comprensión y no ha sido optimizado, pero se plante aquí para dar una idea clara del papel que juegan los cortafuegos en la seguridad perimetral de una Organización.

298. No se incluyen reglas anti-*spoofing* (que evitarían que direcciones IP de redes internas fueran aceptadas provenientes del exterior), ni se han bloqueado las direcciones privadas RFC 1918 (al ser el último eslabón de la cadena, ya no deberían existir direcciones privadas a partir de este punto). En una aplicación real sería recomendable incluir las reglas correspondientes excepto cuando el cortafuegos lo implemente de forma implícita, sin una inclusión específica en el propio juego de reglas. Este tipo de reglas suelen ir al comienzo del juego para evitar que alguna regla anterior pueda permitir el paso a este tráfico ilegal.

299. Para poder crear un juego de reglas adecuado hay que tener un conocimiento en profundidad de los protocolos que intervienen. Por ejemplo, en el caso del protocolo DNS es importante saber:

   – Utiliza tanto TCP como UDP, pero no indistintamente. Para peticiones estándar se utiliza UDP, pero si el paquete de respuesta es mayor de 512 bytes, entonces se recurrirá al protocolo TCP. Por tanto, se deberá permitir de manera general tanto el tráfico TCP como UDP.

   – La transferencia de información entre el servidor DNS primario y los servidores DNS secundarios utiliza TCP ("transferencia de zona"), por lo que el tráfico TCP ha de ser habilitado desde el secundario ($DNS_{DMZint\text{-}R}$) al primario ($DNS_{DMZint\text{-}M}$).

   – Si el servidor interno maestro ($DNS_{DMZint\text{-}M}$) utiliza al servidor interno de ráplica ($DNS_{DMZint\text{-}R}$) como pasarela (*forwarder*) al exterior (lo que puede ser recomendable para evitar su contacto directo con el mundo exterior), se habrá de permitir tráfico TCP y UDP entre ambos.

300. Se debe repetir el proceso de conocimiento para definir las reglas correspondientes al tráfico entre el cortafuegos y la consola, el cortafuegos y el servidor de filtrado de contenidos y para el resto de protocolos involucrados.

301. Otro detalle a tener en cuenta es cómo el cortafuegos interpreta el juego de reglas. Lo más habitual es que siga una política *first match*, es decir, en cuanto las características del paquete cumplan una regla se aplica la acción indicada, evitándose el procesado del resto del juego de reglas.

302. Suponiendo que el primer cortafuegos no fuera el responsable de los túneles VPN sino que esto estuviera delegado a otro elemento (segundo cortafuegos, servidor dedicado, etc.), habría que introducir reglas que permitieran pasar el tráfico IPSec. Este tráfico utiliza dos protocolos IP (ESP y AH) y el puerto 500 (servicio IKE) del protocolo UDP. Los protocolos ESP y AH no poseen información de puerto.

Protocolo	*Dir. Origen*	*Puerto Origen*	*Dir. Destino*	*Puerto Destino*	*Acción*	*Registro*
Udp	cualquiera	cualquiera	cortafuegos-2	500	aceptar	si
Esp	cualquiera	N/A	cortafuegos-2	N/A	aceptar	si
Ah	cualquiera	N/A	cortafuegos-2	N/A	aceptar	si

8.2. DESPLIEGUE

8.2.1. INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS Y DISPOSITIVOS DE RED

303. Se deben seguir los procedimientos estándar en lo que se refiere a buenas prácticas de instalación y configuración de sistemas y dispositivos, entre otros:

- Instalación en entornos aislados seguros.
- Instalaciones mínimas.
- Actualización de software.
- Desactivación de servicios no necesarios.
- Reforzamiento.
- Elección de la opción de configuración más segura frente a la más cómoda en caso de conflicto.
- Aplicación de principios de seguridad: seguridad en profundidad, principio de mínimo privilegio, etc.
- Inspección.
- Diseño de procedimientos de inspección, mantenimiento, documentación, recuperación frente a desastres, auditoría, actualización, etc.

304. Se debe garantizar que la configuración inicial sea robusta, pero no basta con eso. Además se deben poner los pilares para que, inmediatamente después de que la infraestructura entre en funcionamiento, puedan ser aplicados los procedimientos que garanticen que se va a mantener su robustez.

8.2.2. SEGURIDAD FÍSICA

305. No debe olvidarse ni menospreciarse la seguridad física de todos los sistemas involucrados en la seguridad perimetral, entendiendo como tal la protección de los sistemas frente acceso no autorizado y eventualidades que puedan comprometer el adecuado cumplimiento de su función dentro de los entornos de seguridad globales (EGS) y locales (ELS).

306. El acceso físico a un sistema proporciona la posibilidad de modificar arbitrariamente las características del mismo, evitando los mecanismos de control que puedan existir. Es muy importante mantener todos los dispositivos involucrados en la seguridad perimetral en un entorno de acceso controlado y debidamente registrado según los requisitos definidos por la política de seguridad.

307. También es importante asegurar que no se puede modificar el funcionamiento de estos dispositivos de forma colateral a través del acceso físico a dispositivos circundantes o modificando características del entorno físico.

308. En el caso de los cortafuegos, además de controlar y registrar todo acceso físico a cualquiera de los componentes del mismo, también se debe garantizar que no se puede modificar su funcionamiento acediendo a otros elementos de red como concentradores (*switches*) o enrutadores, y que no es posible alterar o interrumpir su funcionamiento cambiando condiciones del entorno físico tales como temperatura, alimentación o similares.

309. Es necesario que todos los elementos que conforman el entorno físico del cortafuegos (*switches*, enrutadores, SAI, prevención de incendios, etc.) estén sometidos a los mismos requisitos de seguridad física que define la política de seguridad para el cortafuegos.

8.2.3. CONFIGURACIÓN DE LOS CORTAFUEGOS

310. Se ha de garantizar que se aplica la configuración de los cortafuegos de acuerdo a la la política de seguridad de la Organización y el diseño de la red de seguridad que se haya realizado, incluyendo:

- La separación de las zonas de seguridad identificadas.
- La autenticación para el acceso a sistemas o servicios, así como otros métodos de control de acceso como puede ser el control de admisión a la red.
- Los sistemas de registro y alertas, para que recojan toda la información potencialmente interesante y se generen alarmas si se producen violaciones o intentos de violación serios de la política de seguridad implementada.
- Las redes privadas virtuales necesarias, si se han identificado requisitos de empleo de cifrado en las comunicaciones.
- El filtrado de contenidos para evitar el riesgo en la interacción de los usuarios con las redes externas.
- Las capacidades de prevención de intrusiones disponibles.
- Otras medidas funcionales que puedan ser necesarias como NAT, alta disponibilidad, balanceo de carga, etc.

311. Además de estos parámetros de configuración específicos del cortafuegos, se deben aplicar aquellos generales a todos los dispositivos, tal y como se han detallado anteriormente,

8.2.4. EVALUACIÓN DE LA CONFIGURACIÓN DEL CORTAFUEGOS

312. Una vez que se haya completado la configuración inicial del cortafuegos, es extremadamente importante evaluar la seguridad de dicha configuración. Se deben comprobar los puertos abiertos en el cortafuegos, así como el tráfico que está permitido a través del mismo.

313. El método más habitual consiste en utilizar un escáner de puertos junto con una herramienta de análisis de tráfico, realizar un barrido de puertos y verificar la correspondencia con la política de seguridad estipulada. Este proceso debe repetirse desde todos y cada uno de los interfaces del cortafuegos hacia todas y cada una de las redes que se encuentran detrás del mismo, poniendo especial énfasis en aquellos puertos que se han dejado abiertos según la política de seguridad y verificando que son sólo accesibles según lo especificado por ésta.

314. El objetivo final de las futuras inspecciones de seguridad es comparar el estado del sistema en cada momento con su estado en un momento en el que dicho sistema tenía una configuración, comportamiento, etc. conocido y determinado. Por tanto, es fundamental **almacenar los resultados** de la inspección de seguridad inicial así como los resultados de las inspecciones posteriores.

8.3. GESTIÓN

8.3.1. ADMINISTRACIÓN REMOTA

315. No se recomienda realizar la administración remota a través de un interfaz web, incluso si el cortafuegos la soporta y especialmente en el caso en que esta gestión no esté protegida por cifrado y autenticación mediante el protocolo HTTPS. Los servidores web son sistemas bastante complejos que periódicamente se ven afectados por vulnerabilidades diversas y, por tanto, son susceptibles de ataques exitosos.

316. Se aconseja utilizar SSH para tunelizar la conexión HTTP siempre que exista la posibilidad. No obstante, es conveniente asegurarse de que se utiliza SSH versión 2, al estar la versión 1 sujeta a diversas vulnerabilidades bien conocidas como ataques *man-in-the-middle*.

317. Es aconsejable, siempre que sea posible, utilizar una conexión "fuera de banda" para gestionar el cortafuegos, , a través de un interfaz dedicado. Esto permite acceder a él incluso bajo algunas condiciones de denegación de servicio y reduce las posibilidades de que el tráfico administrativo sea interceptado o se acceda al cortafuegos ilegítimamente aprovechando relaciones de confianza entre el cortafuegos y los sistemas de gestión.

8.3.2. ACTUALIZACIONES DE SOFTWARE

318. Una gran parte de los problemas de seguridad que sufren los sistemas y redes suelen deberse a fallos en sus componentes *software*, ya sean el sistema operativo subyacente o

en aplicaciones, incluyendo el *software* de los componentes de seguridad perimetral como los cortafuegos, IDS, etc.

319. El impacto de estos problemas de seguridad puede ser muy variado, desde permitir realizar una denegación de servicio hasta subvertir los controles de acceso, pudiendo llegar a permitir un control absoluto sobre el dispositivo comprometido.

320. Los fabricantes suelen publicar actualizaciones para sus aplicaciones corrigiendo estos fallos, también conocidas como "parches". Estas actualizaciones deben aplicarse lo antes posible en todos los sistemas afectados. Determinados parches pueden requerir un reinicio del sistema en cuestión, por lo que es conveniente reservar una ventana de mantenimiento para poder aplicarlos de forma fiable.

321. Contar con sistemas redundantes facilita el proceso de actualización: permite reiniciar un sistema manteniendo el otro u otros operativos, evitando la interrupción del servicio. Además, permite verificar las consecuencias del parche sobre un sistema primero, verificar su correcto funcionamiento durante un intervalo razonable de tiempo y aplicar posteriormente la misma actualización al resto de los sistemas redundantes, dado que en ocasiones se producen problemas derivados de la aplicación de los parches.

322. Las actualizaciones sólo corrigen aquellos problemas conocidos por los fabricantes. Existen problemas de seguridad descubiertos por terceros que no son notificados a los fabricantes y que son utilizados de forma implacable contra los sistemas vulnerables. Son los conocidos como *exploits* de día cero. Las protecciones frente a este tipo de ataques son los sistemas de prevención de intrusiones, y especialmente aquellos que cuentan con la capacidad de detectar anomalías en el tráfico de red o el comportamiento de los sistemas, junto con estrategias de seguridad generales como seguridad en profundidad, biodiversidad, principio de mínimo privilegi*o, etc.*

8.3.3. PROCEDIMIENTOS Y DOCUMENTACIÓN

323. Con el paso del tiempo, crecen las necesidades de comunicación de las Organizaciones, el número y la peligrosidad de las amenazas. Como respuesta, se vuelven cada vez más sofisticadas y complejas la arquitectura de seguridad, la seguridad perimetral y la necesidad de personal para su gestión.

324. Si no se homogeneizan los procesos a seguir y no se coordinan adecuadamente los cambios, estos cambios pueden ser catastróficos. Hay dos estrategias fundamentales para minimizar este riesgo:

- El desarrollo de procedimientos debidamente probados y estandarizados para la realización de las tareas de mantenimiento.
- La documentación adecuada de todos y cada uno de los cambios que se llevan a cabo (gestión de configuración).

325. Estas medidas son cada vez más necesarias conforme crece el número de integrantes de los equipos de gestión.

326. La información de configuración de los sistemas de seguridad perimetral es altamente sensible, por lo que nunca debe estar almacenada en sitios que carezcan de los adecuados mecanismos de protección y control de acceso.

327. Toda la información intercambiada entre los integrantes de los equipos de gestión de los dispositivos de seguridad perimetral deberá ser adecuadamente protegida, tanto en

tránsito como en su almacenamiento. La utilización de tecnologías de cifrado tales como certificados digitales, PGP, etc. pueden ayudar a solucionar el problema.

8.3.4. SUBCONTRATAS

328. Es posible que en determinadas Organizaciones se considere la subcontratación de parte o de la totalidad de la gestión de la seguridad perimetral.

329. Como en toda subcontrata de sistemas relacionados con el funcionamiento de la empresa, y especialmente en aquellas que tengan en sus manos algún componente que influya en la seguridad de la información, ha de garantizarse que en el contrato se contemplan las siguientes cláusulas:

- Confidencialidad de la información compartida, incluyendo la documentación provista, los procedimientos seguidos, la configuración de los sistemas, y aquellos datos internos a los que se pueda tener acceso como parte del servicio prestado (en el caso de la seguridad perimetral, todo el tráfico registrado).
- Obligación de información a la Organización de las operativas realizada y de generación de documentación.

330. Ha de recordarse que la subcontrata no supone un mecanismo para beneficiarse de capacidad extra de trabajo y conocimientos avanzados de expertos externos, pero no una descarga de responsabilidades sino un aumento de éstas, por lo que deben realizarse auditorías de seguridad y funcionamiento, no pudiendo ser éstas realizadas por el mismo prestador del servicio.

8.3.5. RECUPERACIÓN ANTE INCIDENTES

331. A lo largo de la vida operacional de cualquier instalación es inevitable (aunque el riesgo es reducible) la aparición de eventos no deseados e inesperados, de mayor o menor envergadura, tanto debido a errores humanos como a fallos de hardware o incluso a desastres naturales.

332. Toda Organización debe contar con un plan de recuperación frente a desastres acorde con las características de sus instalaciones, que cubra todos los componentes indispensables de la arquitectura de sistemas y comunicaciones.

333. Como parte de la seguridad perimetral, dentro de dicho plan debe incluirse la posibilidad de:

- fallos del *hardware* del cortafuegos
- introducción de reglas inadecuadas
- fallos en el funcionamiento del sistema operativo o *software*
- fallos eléctricos o de suministro
- incendios, inundaciones o catástrofes naturales
- etc.

334. Los tres objetivos fundamentales de este plan deben ser:

- minimizar la probabilidad de que los incidentes ocurran
- minimizar el impacto de los incidentes

- proporcionar una capacidad de recuperación ante incidentes lo más rápida posible.

335. Aunque la elaboración de un plan integral de recuperación frente a incidentes puede ser altamente complejo y costoso, sí podemos definir una serie de procedimientos y medidas que pueden abordar eficazmente los tres factores citados anteriormente en el caso concreto de la seguridad perimetral.

336. También es imprescindible contar con un servicio de soporte adecuado y/o hardware adicional disponible para poder cubrir esa eventualidad.

8.3.5.1 COPIAS DE SEGURIDAD

337. Una de las medidas más sencillas y útiles es la realización de copias de seguridad periódicas, y por tanto son el mínimo exigido con respecto a recuperación frente a desastres. Su existencia es fundamental para la recuperación frente a cualquier tipo de incidente, ya sea mayor o menor. La complejidad y el esfuerzo de mantenimiento son típicamente bajos ya que la mayor parte de los productos permiten el volcado de los datos de una forma fácil y automática, garantizando un máximo de eficiencia y seguridad.

338. Algunos detalles importantes respecto a las copias de seguridad que deben cumplirse son:

- Documentar detalladamente cómo realizar las copias y cómo restaurar los distintos sistemas a partir de las mismas.
- Realizar copias de seguridad del sistema:
  - antes de entrar en producción.
  - periódicamente (a diario es lo más habitual).
  - antes y después de cada cambio
- Etiquetar las copias de seguridad identificando claramente el sistema al que pertenecen, el momento en que fueron realizadas, el nivel (en caso de que se trate de copias incrementales) y cualquier otra característica relevante que pueda ser necesaria para una correcta restauración.
- Guardar un registro detallado del contenido de las copias de seguridad, habitualmente en formato electrónico, para poder localizar rápidamente la información buscada. Este registro es actualizado automáticamente por gran parte del *software* automático de *backup*.
- Comprobar la integridad de las copias tras su realización.
- Realizar periódicamente una restauración completa para validar los procedimientos de volcado y recuperación.
- Establecerse un procedimiento que permita almacenar una réplica de dichas copias en al menos un lugar externo, lo más alejado posible, como medida frente a desastres geográficos.
- Someter tanto las copias como el registro de su contenido deben al mismo nivel de seguridad y control físico que los propios dispositivos a los que respaldan.

339. Garantizando todo lo anterior se obtiene una probabilidad muy alta de recuperación con éxito en un tiempo mínimo.

8.3.5.2 PROTECCIÓN FRENTE A ERRORES HUMANOS

340. Hoy en día, casi todos los componentes de la seguridad perimetral son susceptibles de ser configurados en una arquitectura a prueba de fallos. Esto reduce pero no elimina la probabilidad de que se produzcan fallos múltiples que afecten al servicio.

341. Se pueden establecer elementos altamente eficaces contra los errores humanos, como una estricta política de documentación o el desarrollo de procedimientos. Por ejemplo, un procedimiento que establezca como ha de ser modificado el juego de reglas de un cortafuegos y como han de ser documentados dichos cambios.

8.3.6. SEGURIDAD PERIMETRAL A LARGO PLAZO

342. Con un conocimiento adecuado de las tecnologías involucradas, las condiciones de financiación y personal existentes y necesarias para una implementación adecuada, no resulta demasiado difícil conseguir una arquitectura de seguridad perimetral suficientemente robusta para cubrir las necesidades de una Organización estándar.

343. El gran reto reside en poder garantizar que esa configuración inicial se mantiene robusta a lo largo del tiempo, adaptándose a las necesidades de la Organización con el paso del tiempo.

344. Las claves para lograr este objetivo son:

- Contar con una política de empresa claramente definida que indique bajo qué circunstancias se pueden hacer cambios en la política de seguridad perimetral.
- Contar con personal capacitado para rediseñar, según necesidades, las partes necesarias de la infraestructura manteniendo el mismo nivel de seguridad.
- Realizar periódicamente inspecciones de la configuración para verificar que el estado es el deseado.

345. Auditar la seguridad de todos los elementos involucrados en la seguridad perimetral puede ser un proceso complejo dada la variedad de tecnologías involucradas. Hay distintos tipos de auditorías de seguridad: desde simples revisiones pasivas hasta agresivos tests de penetración.

346. Asimismo, las auditorías, algunas de las cuales son obligatorias, pueden ser llevadas a cabo por la propia Organización o por un tercero. Una aproximación no resulta mejor que la otra sino que deben ser complementarias. Realizar auditorías internas de seguridad coordinadas con externas de forma periódica es una buena combinación para poder obtener un grado adecuado de confianza.

347. Entre los parámetros generales de los sistemas de protección perimetral que han de ser verificados periódicamente figuran:

- Cuentas de usuario.
- Contraseñas.
- Puertos abiertos.
- Versiones de los Sistemas Operativos y actualizaciones.
- Control de acceso.
- Seguridad física.

348. En el caso concreto de los cortafuegos, además, se debe verificar:

- los juegos de reglas, comparándolos con el último estado validado, y analizando la razón y la conveniencia de los cambios introducidos desde entonces.
- el comportamiento activo, para verificar que efectivamente el juego de reglas implementado está funcionando de la forma esperada.
- la información estadística proporcionada por el propio cortafuegos respecto a la utilización de cada una de las reglas

349. En base al resultado de las auditorías, debe estudiarse si los dispositivos están operando eficientemente o si necesitan algún tipo de reorganización.

8.4. RETIRADA/SUSTITUCIÓN

350. La vida de todo dispositivo concluye con su retirada, ya sea porque se elimina por cambios en la política de seguridad y los servicios que presta, o porque se sustituye por un nuevo dispositivo con las mismas o nuevas capacidades por fallo *hardware* o necesidades de la Organización.

351. Cuando se retira un dispositivo, ha de conservarse una copia de seguridad de su configuración y contenido para futuras referencias.

352. Además, dicha configuración es considerada información sensible, por lo que debe borrarse del sistema antes de que el dispositivo abandone físicamente el entorno protegido de la Organización, de modo que no pueda ser recuperada por agentes externos ni utilizada para atacar la red. Algunos cortafuegos cuentan con una funcionalidad de reinicio de configuración, que elimina todas sus reglas y capacidades configuradas y los devuelve al estado en el que salieron de fábrica.

353. Finalmente, en el caso de una sustitución, es conveniente establecer un estado de convivencia de ambos dispositivos, nuevo y viejo, que permitan volver a la situación anterior como respuesta ante algún incidente consecuencia del cambio. Durante esa coexistencia debe realizarse una evaluación del comportamiento del nuevo cortafuegos, utilizando los resultados de las evaluaciones del viejo como referencia.

9. RESUMEN DE BUENAS PRÁCTICAS

354. A continuación se realiza un resumen de las buenas prácticas en la gestión de los cortafuegos incluidas en este documento:

- Reglas:
    - Comentar las reglas.
    - Situar primero las reglas más utilizadas.
    - Rechazar (reject) el tráfico *identd*
    - Prohibir el acc*eso no autorizado al* cortafuegos
    - Prohibir los paquetes desde direcciones marcianas
    - Prohibir puertos habitualmente atacados/escaneados
    - Permitir el tráfico de gestión y monitorización necesario
    - Permitir los protocolos de enrutamiento y de red necesarios
    - Permitir el acceso a los puertos/servicios ofrecidos por la organización
    - Evitar objetos repetidos

    - Establecer una nomenclatura única
    - Evitar reglas temporales
- Registro y detección:
    - Registrar el tráfico denegado
    - Alertar en caso de tráfico desde una zona desmilitarizada
    - No registrar el tráfico ruidoso pero necesario (*broadcast*, etc.)
    - Centralización y análisis automático de registros.
- Garantizar el soporte y actualización de los *proxies* de filtrado y las reglas de prevención de intrusiones.
- Activar la normalización de paquetes garantizando que los servicios no se ven afectados.
- No activar en el cortafuegos servicios extra que puedan suponer un punto de ataque (DHCP, etc.)
- Garantizar la alta disponibilidad
- Acceso remoto::
    - Definir la necesidad de un concentrador de VPN o no. En su caso situar el concentrador de VPN en una DMZ dedicada.
    - Uso de IPSec, MPLS o SSL
    - Integrar autenticación de usuarios con directorio excepto en entornos críticos
    - Establecer normas de acceso por usuario
- Cortafuegos de sistema:
    - Usar en todos los servidores y estaciones de trabajo
    - Configurar y gestionar centralizadamente
    - Revisar los *logs* y establecer sistemas de alertas
- Utilizar IDS e IPS de red y de sistema
- Definir (físicamente o por VLAN) distintas subredes por niveles de seguridad, separando al menos (en redes complejas):
    - DMZ externa
    - DMZ interna
    - Red de dispositivos móviles
    - Una o varias subredes internas
- Utilizar distintos cortafuegos entre las redes (de marcas distintas)
- En entornos complejos, repartir la gestión entre equipos de administración distintos
- Política de seguridad:
    - Garantizar la redacción, coherencia, filosofía y soporte de la política de seguridad
    - Realizar una inspección de seguridad inicial y guardar sus resultados para la comparación con futuras inspecciones.
    - Garantizar que el flujo de aprobación de permisos incluye técnicos que comprenden los riesgos que asumidos con nuevas reglas, y que las prisas no son un criterio para la aprobación.

- Seguir todos los principios de buenas prácticas aplicables a la seguridad y la gestión de la red, incluyendo:
    - Procedimentación y documentación (gestión de cambios y configuración)
    - Planes de actualización y mantenimiento
    - Administración segura
    - Plan de recuperación ante incidentes
    - Política de backup.
    - Contratación de servicio de soporte y mantenimiento
    - Garantizar la confidencialidad de la información y documentación. Especialmente importante en el caso de subcontratas de gestión.
    - Borrado de configuración en la retirada

ANEXO A. CRITERIOS DE ELECCIÓN DE CORTAFUEGOS

A continuación se detallan en orden de importancia algunos de los criterios a considerar en la elección de un dispositivo cortafuegos. En todo caso, su ponderación y orden dependerá del despliegue concreto: objetivo, tipo, ubicación, etc.

Es importante destacar que el factor decisivo para elegir un producto u otro debe ser fundamentalmente de tipo tecnológico y no de funcionalidad añadida o de presentación. Se debe primar en todo momento la calidad del cortafuegos y las funcionalidades orientadas al control de acceso o protección de la red frente a otras funcionalidades que en ocasiones son añadidas a dichos productos pero que caen fuera de su ámbito y que habitualmente se pueden obtener con otro tipo de dispositivos añadidos.

- **Tecnología:**
  - Filtrado de paquetes con o sin información de estado.
  - Inspección “inteligente” de tráfico y protocolos soportados.
  - Niveles: red/transporte, aplicación (proxy).
  - Capacidad de trabajo en modo “transparente”.
  - Traducción de direcciones.
  - Soporte de distintas posibilidades de autenticación, local y centralizada.
  - Soporte de distintas aproximaciones de autenticación: usuario, sesión.
  - Filtrado de contenidos: código malicioso, antispam, etc.
  - Control de admisión (si los clientes soportan esta aproximación).
  - Capacidad de VLAN
  - Soporte dual de pilas de red: IPv4/IPv6.
  - Mecanismos de respuesta activa.
  - Normalización de paquetes.
- **Arquitectura y rendimiento:**
  - Número máximo de conexiones.
  - Volumen máximo de tráfico soportado.
  - Número máximo de interfaces de red y velocidad asociada.

- Capacidad de procesamiento y memoria.
- Appliance o sistema de propósito general.

- **Gestión y registro:**
  - Trazas de registro de actividad y control de acceso.
  - Protocolos de gestión seguros.
  - Gestión centralizada.
  - Facilidad de operación.
  - Sistema de optimización de reglas.
  - Rotación de trazas de registro.
  - Gestión de la configuración.
- **Redes Privadas Virtuales**
  - Tipos: entre sedes y de acceso remoto.
  - Criptografía realizada por hardware criptográfico especializado.
- **Alta disponibilidad y escalabilidad**
  - Redundancia.
  - Balanceo de carga.
  - Capacidad de crecimiento.
  - Fuentes de alimentación redundantes.
- **Soporte y mantenimiento**
  - 24x7 para elementos hardware.
  - 24x7 o 8x5 para soporte ante incidencias software.
  - Política publicación de actualizaciones software (mecanismo, frecuencia,...)
- **Informes (reporting)**
- **Funcionalidades de valor añadido:**
  - Implementación de Honeypots.
  - Servicios de red: NTP, DHCP, etc.
  - Visualización de mapas o diagramas de red.

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Amenaza	Evento que puede desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Análisis o valoración de Riesgos	Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema.
Antispam	Contramedida cuyo objetivo es la contención de correo electrónico no solicitado (spam).
Antispyware	Contramedida cuyo objetivo es evitar la infección por código malicioso de tipo spyware.
Área de seguridad	Área que incluye redes, sistemas o servicios con unos requisitos o condiciones de seguridad similares o sometidos a un mismo grupo de riesgos.
Autenticación	Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.
Autorización	Definición granular de permisos de acceso concedidos a un determinado usuario, dispositivo o sistema. habitualmente implementado mediante listas de control de acceso.
Balanceo de carga	Mecanismo que permite repartir la carga del sistema entre dos o más dispositivos que ofrecen un mismo servicio.
Biodiversidad	Estrategia de introducción de elementos que ofrezcan una misma funcionalidad pero con elementos tecnológicos diferentes.
Concentrador VPN	Dispositivo que proporciona funcionalidades de redes privadas virtuales habitualmente mediante el uso de hardware de aceleración criptográfica.
Confidencialidad	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
Cortafuegos	Sistema formado por aplicaciones, dispositivos o combinación de estos encargado de hacer cumplir una política de control de acceso en las comunicaciones entre dispositivos según una política de seguridad existente
Cortafuegos de sistema	Cortafuegos centrado en el control de acceso local de un determinado nodo.
Cortafuegos personal	Cortafuegos de sistema utilizado en estaciones de usuario.
Cortafuegos transparente	Propiedad de un equipo cortafuegos que le permite ser “invisible” a los clientes y servidores de la comunicación residiendo en capa de enlace de datos aunque sea capaz de intervenir a nivel de red.
Cortafuegos virtuales	Plataforma que permite la definición de cortafuegos lógicos o virtuales sobre un solo sistema físico pudiendo implementarse en ellos políticas de seguridad diferentes y ser gestionados individualmente.
Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
Enrutador	Dispositivo de nivel de red encargado de encaminar los paquetes entre redes gracias a una tabla de enrutamiento de red.
Extranet	Redes privadas virtuales establecidas con otras Organizaciones con el fin de compartir algún tipo de recurso o servicio.
Filtrado de Camino Inverso	Técnica de filtrado del tráfico entrante basada en la verificación de la dirección origen de los paquetes con la tabla de enrutamiento para comprobar que dicha red es alcanzable por dicho interfaz de entrada.
Filtrado de entrada/salida	Filtrado realizado en los puntos de comunicación del perímetro de la Organización con el exterior.

Filtrado de paquetes sin información de estado	Filtrado de paquetes básico que trata los paquetes de manera individual sin tener en cuenta información del estado de la comunicación.
Filtrado de paquetes con información de estado	Filtrado de paquetes que memoriza las comunicaciones a nivel de transporte previamente establecidas.
Filtrado de paquetes con información de estado e inspección	Filtrado de paquetes que además de memorizar las comunicaciones a nivel de transporte, inspecciona el contenido de los paquetes utilizando decodificadores de protocolo para así interpretar los flujos dinámicos de comunicaciones asociados.
Fuera de Banda	Mecanismo de acceso a dispositivo mediante un canal de comunicación diferente al utilizado para las comunicaciones de producción.
Gestión de Eventos de Seguridad (SEM)	Sistema para la clasificación y análisis de eventos de seguridad mediante el uso de técnicas de correlación de trazas de registro de múltiples dispositivos
Gestión de la Configuración	Conjunto de procedimientos que regulan el almacenamiento y la modificación de la configuración y juego de reglas de los dispositivos.
Juego de Reglas	Conjunto de reglas que actúan como un todo para implementar la política de seguridad de la Organización.
Integridad	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
Intranet	Red interna de la Organización habitualmente segmentada de manera apropiada para controlar el flujo de comunicaciones con el resto de redes: Internet, Extranet, DMZ, etc.
Lista de Control de Acceso (ACL)	Especificación de un conjunto de reglas representadas mediante entradas de control de acceso basadas en diferentes campos o propiedades.
Máquina Trampa (Honeypot)	Recurso cuyo valor reside en el hecho de ser comprometido. Al ser elementos no productivos, cualquier actividad dirigida u originada en ellos es considerada maliciosa y por tanto de gran utilidad en detección de intrusiones como elemento de alerta temprana.
Normalización	Mecanismo de adaptación de ciertos parámetros de paquetes en tránsito de manera que resulten más robustos a nivel de seguridad, además de descartar aquellos considerados anómalos por incumplir las especificaciones.
Perímetro	Límite exterior que delimita el contorno de una determinada área
Política de Seguridad	Documento de alto nivel que sirve como marco para reflejar las intenciones y requisitos de seguridad de la información de una Organización.
Proxy	Dispositivo pasarela que implementa la funcionalidad cliente/servidor de uno o más protocolos o aplicaciones, según los RFC o estándares correspondientes, con el objetivo de servir peticiones a servidores en nombre de los clientes que lo utilizan.
Proxy inverso	Dispositivo proxy con el objetivo de servir peticiones de clientes externos de nuestra red protegiendo el acceso a un servicio externo.
Proxy transparente	Dispositivo proxy con la capacidad de interceptar el tráfico a nivel de red sin que sea percibido por parte de los clientes.
Pruebas de penetración (pen-testing)	Pruebas de auditoria para comprobar la correcta aplicación y configuración de contramedidas de seguridad en los dispositivos de información y comunicaciones según lo especificado en la política de seguridad y así alertar de posibles desviaciones detectadas.
Redes Privadas Virtuales (VPN)	Mecanismo que permite el establecimiento de una comunicación segura y flexible entre dos nodos, entre un nodo y una red o entre dos redes cuando dicha comunicación ha de atravesar un medio inseguro.
Riesgo	Probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad causando daño (impacto) en un proceso o sistema.
Ruta de Descarte (null route)	Mecanismo de filtrado de tráfico básico basado encaminar el tráfico a un interfaz virtual de descarte.

Salvaguardas (contramedidas)	Procedimiento o mecanismo tecnológico que reduce el riesgo.
Seguridad de las Tecnologías de la Información y las Comunicaciones	La capacidad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistema) para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, integridad y/o confidencialidad de los datos almacenados o transmitidos y de los servicios que dichos Sistemas ofrecen o hacen accesibles.
Seguridad en Profundidad (Defense-in-Depth)	Estrategia de protección consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto.
Sistema de las Tecnologías de la Información y las Comunicaciones	Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única autoridad.
Sistema de Detección de Intrusiones (IDS)	Sistema con la función de detectar indicios de ataque o compromiso desde o hacia los elementos que conforman nuestro STIC.
Sistema de Prevención de Intrusiones (IPS)	Aproximación de un IDS a la tecnología cortafuegos consistente en permitir o denegar el tráfico mediante el uso de firmas o análisis de anomalías.
Reglas Implícitas	Reglas aplicadas al inicio o final del juego de reglas aunque no estén explícitamente especificadas.
Reglas ”No logging”	Reglas configuradas explícitamente de manera que denieguen el tráfico pero sin registrar dicho evento al carecer este de importancia o repetirse con excesiva frecuencia.
Reglas “Log Denied”	Reglas configuradas explícitamente de manera que denieguen el tráfico registrando dicho evento.
Reglas ”Lockdown”	Reglas cuyo objetivo es prohibir explícitamente todo el tráfico dirigido al cortafuegos o dispositivo de red salvo el proveniente de la estación administrativa con los protocolos de gestión necesarios.
Reglas “Sneaky”	Reglas con el objetivo de denegar tráfico originado por servidores ubicados en una DMZ y alertar de dicha situación al ser esto un claro indicio de intrusión.
Spyware	Código malicioso diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario.
Traducción de Direcciones	Mecanismo implementado en cortafuegos o enrutadores de red consistente en la modificación de las direcciones de origen o destino de los paquetes.
Trazas de Registro (log)	Registro de información de una aplicación o sistema con el objetivo de conservar el estado y actividad en sus diferentes intervalos de tiempo. Es vital la sincronización de tiempo para su integridad y correlación entre dispositivos.
Vulnerabilidad	Debilidad de seguridad de un sistema que le hace susceptible de poder ser dañado al ser aprovechado por una amenaza.
Zona Desmilitarizada (DMZ)	Zona con un nivel de protección intermedio entre dos áreas de seguridad diferentes.

3DES	Triple DES
AAA	Authentication, Authorization, Accounting – Autenticación, Autorización, Registro
ACL	Access Control List – Lista de Control de Acceso
AD	Active Directory – Directorio Activo
AES	Advanced Encryption Standard – Estándar Avanzado de Encriptación
AH	Authentication Header – Cabecera de Autenticación
ARP	Address Resolution Protocol – Protocolo de Resolución de Direcciones
CARP	Common Address Redundancy Protocol – Protocolo de Redundancia por Dirección Común
CCN	Centro Criptológico Nacional
CHAP	Challenge-Handshake Authentication Protocol – Protocolo de Autenticación por Intercambio de Reto
CNI	Centro Nacional de Inteligencia
DES	Data Encryption Standard – Estándar de Cifrado de Datos
DHCP	Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Sistema
DMZ	DeMilitarized Zone – Zona Desmilitarizada
DNS	Domain Name System – Sistema de Nombres de Dominio
EGS	Entornos Globales de Seguridad
ELS	Entornos Locales de Seguridad
ESP	Encapsulating Security Payload – Seguridad de Información Encapsulada
FTP	File Transfer Protocol – Protocolo de Transferencia de Ficheros
HMAC	Hash Message Authentication Code – Código de Autenticación de Mensaje Resumen
HSRP	Hot Standby Routing Protocol – Protocolo de Enrutamiento de Espera en Caliente
HTTP	HyperText Transfer Protocol – Protocolo de Transferencia de HiperTexto
HTTPS	Secure HTTP – HTTP Seguro
IANA	Internet Assigned Numbers Authority – Autoridad de Asignación de Números Internet
ICMP	Internet Control Messaging Protocol – Protocolo de Mensajes de Control Internet
IDS	Intrusion Detection System – Sistema de Detección de Intrusiones
IKE	Internet Key Exchange – Intercambio de Claves Internet
IPS	Intrusion Prevention System – Sistema de Prevención de Intrusiones
IPSec	IP Security – Seguridad IP
IRC	Internet Relay Chat – Protocolo de Charla Internet
KISS	Keep It Simple Stupid - ¡Hazlo simple estúpido!
L2TP	Layer 2 Tunneling Protocol – Protocolo de Tunelizado de nivel 2
LDAP	Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorio
MD5	Message Digest algorithm 5 – Algoritmo de Resumen de Mensaje versión 5
MITM	Man-In-The-Middle
MODP	MODular exPonential group
MPLS	MultiProtocol Label Switching – Multiprotocolo de Conmutación de Etiquetas

MTA	Mail Transfer Agent – Agente de Transferencia de Correo Electrónico
NAT	Network Address Translation – Traducción de Direcciones de Red
OOB	Out-of-Band – Fuera de Banda
OSI	Open Systems Interconnection – Interconexión de Sistemas Abiertos
P2P	Peer-to-Peer – Comunicación entre pares
PAP	Password Authentication Protocol – Protocolo de Autenticación por Contraseña
PGP	Pretty Good Privacy
PPTP	Point-to-Point Tunneling Protocol – Protocolo de Tunelizado Punto a Punto
RADIUS	Remote Authentication Dial In User Service – Servicio de Autenticación Remoto de Usuarios
RIB	Routing Information Base – Base de Datos de Información de Routing
RFC	Request for Comments
RPF	Reverse-Path Filtering – Filtrado de Camino Inverso
RPV	Red Privada Virtual
SA	Security Association – Asociación de Seguridad
SAI	Sistema de Alimentación Ininterrumpida
SAD	Security Association Database – Base de datos de Asociaciones de Seguridad
SEM	Security Event Management – Gestión de Eventos de Seguridad
SHA	Secure Hash Algoritm – Algoritmo Seguro de Resumen
SMTP	Simple Mail Transfer Protocol – Protocolo de Transferencia Simple de Correo
SPD	Security Policy Database – Base de Datos de Política de Seguridad
SQL	Structured Query Language – Lenguaje de Consulta Estructurado
SSH	Secure Shell – 'Shell' Segura
SSL	Secure Socket Layer – Capa de 'socket' seguro
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones.
STUN	Simple Transversal of UDP through NATs – Protocolo para atravesamiento de NATs mediante UDP
TACACS	Terminal Access Controller Access Control System
TCP	Transport Control Protocol – Protocolo de Control de Transporte
TIC	Tecnologías de la Información y las Comunicaciones
UDP	User Datagram Protocol – Protocolo de Datagramas de Usuario
VLAN	Virtual Local Area Network – Red de Área Local Virtual
VPN	Virtual Private Network – Red Privada Virtual
VRRP	Virtual Router Redundancy Protocol – Protocolo de Redundancia de Enrutador Virtual

ANEXO C. REFERENCIAS

[Ref.- 1] Building Internet Firewalls – 2nd Edition; D. Brent Chapman & Elizabeth D. Zwicky; O'Reilly; 2000
[Ref.- 2] Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems; Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Fredrick, Ronald W. Ritchey; Sams; 2002
[Ref.- 3] Decipher Your Firewall Logs; Robert Graham; Internet Security Advisor; Mar/Apr 2000
[Ref.- 4] Network Intrusion Detection; Stephen Northcutt, Judy Novak; Sams; 2002
[Ref.- 5] Building Firewalls with OpenBSD and PF, Jacek Artymiak; November, 2003
[Ref.- 6] Linux Firewalls; Robert Ziegler; Sams; October, 2001
[Ref.- 7] Building Linux and OpenBSD Firewalls; Wes Sonnenreich, Tom Yates; Wiley; 2000
[Ref.- 8] Essential Check Point FireWall-1 NG: An Installation, Configuration, and Troubleshooting Guide; Dameon D. Welch-Abernathy; Addison-Wesley Professional; January, 2004
[Ref.- 9] Check Point NG VPN-1/Firewall-1: Advanced Configuration and Troubleshooting; Barry J. Stiefel, et al; Syngress; May 2003
[Ref.- 10] Check Point Next Generation Security Administration; Cherie Amon et al; Syngress; March 2002
[Ref.- 11] Nokia Network Security Solutions Handbook; Doug Maxwell; Syngress; October 2002
[Ref.- 12] Cisco Security Specialist's Guide to PIX Firewall; Umer Khan, et al; Syngress; December 2002
[Ref.- 13] Cisco(R) PIX (TM) Firewalls; Richard Deal; McGraw-Hill Osborne Media; October, 2002
[Ref.- 14] Configuring NetScreen Firewalls; Rob Cameron; Syngress; November 2004
[Ref.- 15] Cisco IOS: It's Not Just for Routing Anymore; Greg Shipley; Network Computing; May 31, 1999
[Ref.- 16] Cisco IOS 12 Network Security; Cisco Press/Macmillan Technical Publishing; 1999
[Ref.- 17] Cisco Security Architectures; Gil Held & Kent Hundley; McGraw-Hill; 1999
[Ref.- 18] Firewall Configuration Done Right; Rik Farrow; Network Magazine; December 1998
[Ref.- 19] Firewall Vulnerabilities; Rik Farrow; Network Magazine; August 1999
[Ref.- 20] Firewalls 24Seven; Matthew Strebe, Charles Perkins; Sybex Network Press; 1999
[Ref.- 21] Firewalls Complete; Marcus Goncalves; McGraw-Hill; 1998 (includes CD-ROM with demo versions of major firewall products)
[Ref.- 22] Firewalls & Internet Security - Repelling the Wiley Hacker; Bill Cheswick & Steve Bellovin; Addison-Wesley; 1998
[Ref.- 23] FreeBSD Firewall Tools & Techniques; Michael Lucas; Sys Admin; June 2000
[Ref.- 24] Great Walls of Fire (Firewall Security); Linda Boyer; NetWare Connection; January 1997
[Ref.- 25] The 'Ins' and 'Outs; of Firewall Security; Mike Fratto; Network Computing; September 6, 1999
[Ref.- 26] Internet Firewalls & Network Security - Second Edition; Karanjit Siyan; New Riders Publishing; 1996
[Ref.- 27] Kicking Firewall Tires; Char Sample; Network Magazine; March 1998
[Ref.- 28] A Linux Internet Gateway; Marcel Gagne; Sys Admin; June 2000
[Ref.- 29] NAT: Network Address Translator; Ron McCarty; Sys Admin; March 2000
[Ref.- 30] Packet Filtering and Cisco's Way; Ron McCarty; Sys Admin; May 1999
[Ref.- 31] Router-Based Network Defense; Gilbert Held; Sys Admin; March 2000
[Ref.- 32] The Use of Routers in Firewall Setup; Matej Sustic; Sys Admin; May 2000
[Ref.- 33] Assembly Instructions Included (Cisco Routers); Gilbert Held; Network Magazine; January 2001
[Ref.- 34] Building A Floppy Firewall; Andreas Meyer; Sys Admin; January 2001
[Ref.- 35] Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls; NIST Special Publication 800-10
[Ref.- 36] NIST Firewall Guide and Policy Recommendations; NIST Special Publication 800-41
[Ref.- 37] RFC1700 - Assigned Numbers
http://www.faqs.org/rfcs/rfc1700.html
[Ref.- 38] RFC1918 - Address Allocation for Private Internets
http://www.faqs.org/rfcs/rfc1918.html
[Ref.- 39] RFC3330: Special-Use IPv4 Addresses
http://www.faqs.org/rfcs/rfc3330.html
[Ref.- 40] RFC3232 - Assigned Numbers: RFC 1700 is Replaced by an On-line
http://www.faqs.org/rfcs/rfc3232.html
[Ref.- 41] RFC3927 - Dynamic Configuration of IPv4 Link-Local Addresses
http://www.faqs.org/rfcs/rfc3927.html

[Ref.- 42] Página web del Team Cymru
http://www.cymru.com/
[Ref.- 43] Merit Network Routing Address Database
http://www.radb.net/
[Ref.- 44] Internet Assigned Numbers Authority (IANA)
http://www.iana.org
[Ref.- 45] RFC 2409 – "The Internet Key Exchange (IKE)" – Noviembre 1998
http://tools.ietf.org/html/rfc2409
[Ref.- 46] RFC 3526 – "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", Mayo 2003
http://www.ietf.org/rfc/rfc3526.txt
[Ref.- 47] RFC 4753 – "ECP Groups for IKE and IKEv2", Enero 2007
http://www.ietf.org/rfc/rfc4753.txt
[Ref.- 48] RFC 2412 – "The OAKLEY Key Determination Protocol" – Noviembre 2008
http://tools.ietf.org/html/rfc2412
[Ref.- 49] RFC 2408 – "Internet Security Association and Key Management Protocol (ISAKMP)" – Noviembre 2008
http://tools.ietf.org/html/rfc2408
[Ref.- 50] "How to break MD5 and Other Hash Functions", Xiaoyun Wang y Hongbo Yu, Enero 2009
http://merlot.usc.edu/csac-f06/papers/Wang05a.pdf
[Ref.- 51] Cryptographic Hash Algorithm Competition
http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
[Ref.- 52] Improved Collision Attack on MD4
http://eprint.iacr.org/2005/151
[Ref.- 53] An improved preimage attack on MD2
http://eprint.iacr.org/2008/089.pdf -
[Ref.- 54] Land Attack
http://en.wikipedia.org/wiki/LAND
[Ref.- 55] Ping of Death
http://en.wikipedia.org/wiki/Ping_of_death
[Ref.- 56] CCN-STIC-432 Seguridad Perimetral – IDS
https://www.ccn-cert.cni.es
[Ref.- 57] RFC 4301 – Security Architecture for the Internet Protocol
http://www.ietf.org/rfc/rfc4301
[Ref.- 58] RFC 4309 – Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
http://www.ietf.org/rfc/rfc4309
[Ref.- 59] RFC 3031 – Multiprotocol Label Switching Architecture (MPLS)
http://www.ietf.org/rfc/rfc3031