IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UD09

IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

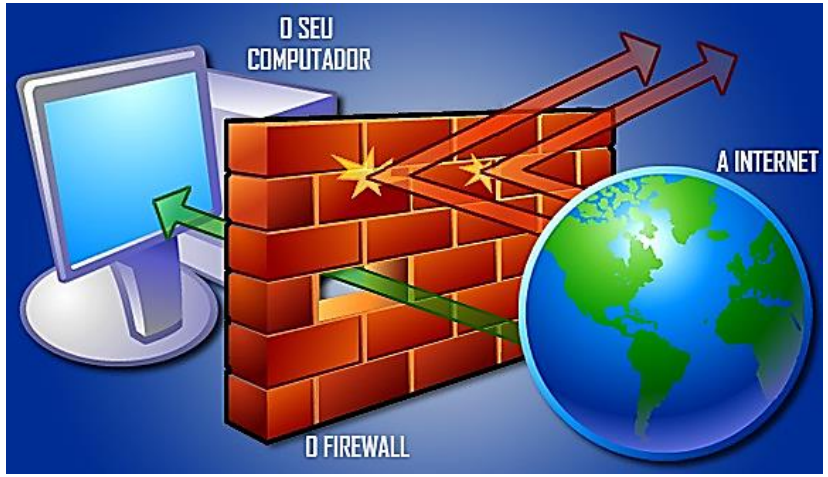
1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS / DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES / VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

1. INTRODUCCIÓN

PARA REDUCIR EL RIESGO DE LAS AMENAZAS LÓGICAS AL SISTEMA DE INFORMACIÓN**, SE DEBEN ROBUSTECER LOS PUNTOS DE ACCESO AL SISTEMA.**

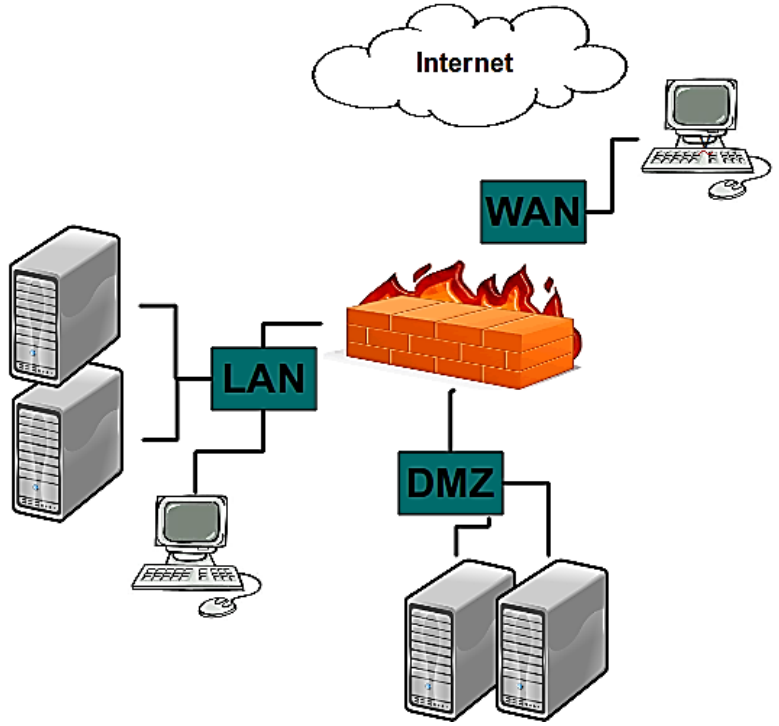
EL PUNTO DE INTERCONEXIÓN DE LA RED PRIVADA DE LA EMPRESA **CON INTERNET** ES EL PRIMER PUNTO QUE **SE DEBE PROTEGER**, YA QUE ES LA ENTRADA DESDE EL EXTERIOR AL SISTEMA DE INFORMACIÓN.

PARA ELLO SE DEBEN EMPLEAR **PASARELAS DE SEGURIDAD O CORTAFUEGOS** (**FIREWALLS**).



1. INTRODUCCIÓN

LOS CORTAFUEGOS **PERMITEN LA SEPARACIÓN FÍSICA DE LA RED EN DIFERENTES TRAMOS O ZONAS**, PARA LO CUAL DISPONDRÁN NORMALMENTE DE AL MENOS DOS TOMAS DE RED QUE LES PERMITAN INTERRUMPIR LA MISMA, **DESEMPEÑANDO LA FUNCIÓN DE PUNTO DE INTERCONEXIÓN ÚNICO**.



DE ESTA FORMA, LOS CORTAFUEGOS:

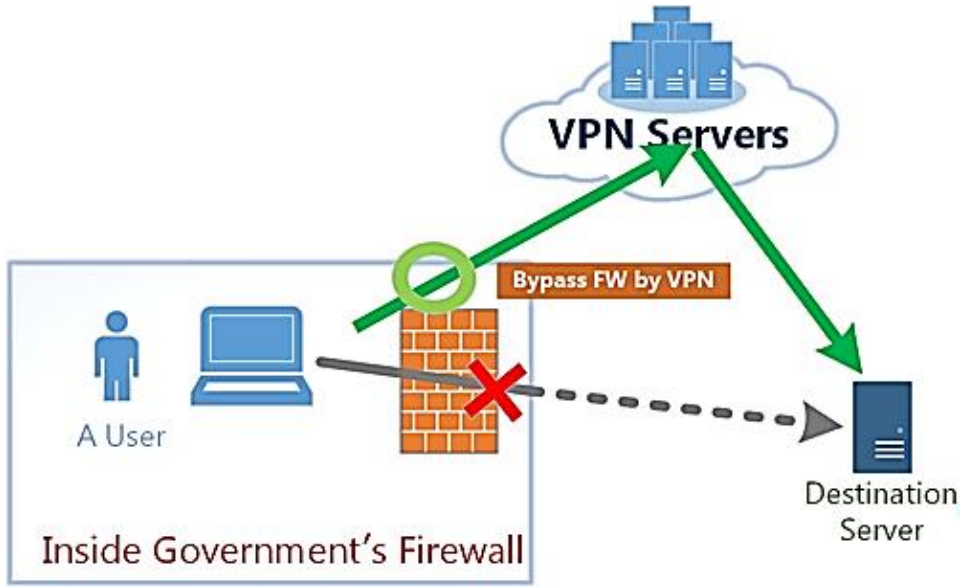
- **PROTEGEN DE UNA AMENAZA EXTERNA**
- **PERMITEN DEFINIR SUBREDES INTERNAS** PROTEGIDAS DE ELLAS MISMAS.

1. INTRODUCCIÓN

EL *ESQUEMA NACIONAL DE SEGURIDAD* ESTABLECE QUE **EL SISTEMA DEBE PROTEGER SUS PERÍMETROS**, ESPECIALMENTE CUANDO HAYA INTERCONEXIÓN A REDES PÚBLICAS COMO INTERNET, DEBIÉNDOSE ANALIZAR LOS RIESGOS DE LA INTERCONEXIÓN, Y DEBIÉNDOSE CONTROLAR EL PUNTO DE UNIÓN.

1. INTRODUCCIÓN

POR ÚLTIMO, Y REFORZANDO EL USO DE CORTAFUEGOS, CUANDO LOS REQUISITOS DE SEGURIDAD SEAN ELEVADOS, **SE DEBEN PROTEGER LAS COMUNICACIONES** CON **REDES PRIVADAS VIRTUALES**, DE MANERA QUE, AÚN VULNERADAS LAS CONTRAMEDIDAS DE LAS PASARELAS DE SEGURIDAD, LAS COMUNICACIONES NO SEAN LEGIBLES PARA UN EXTERNO.



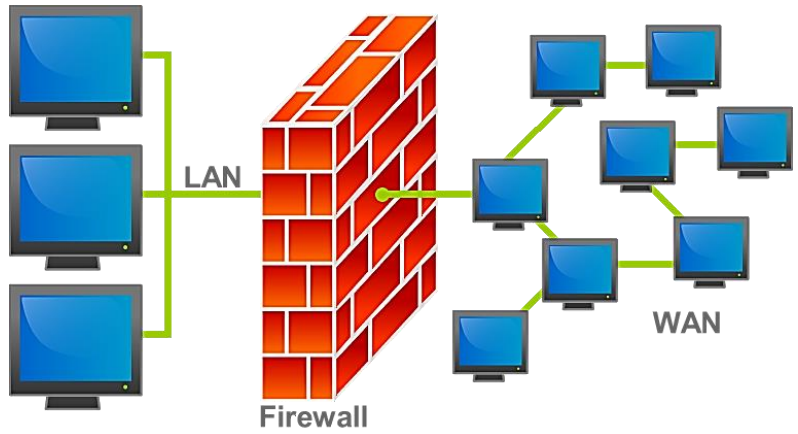
CONTENIDOS

1. INTRODUCCIÓN
2. **RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD**
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS / DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES / VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

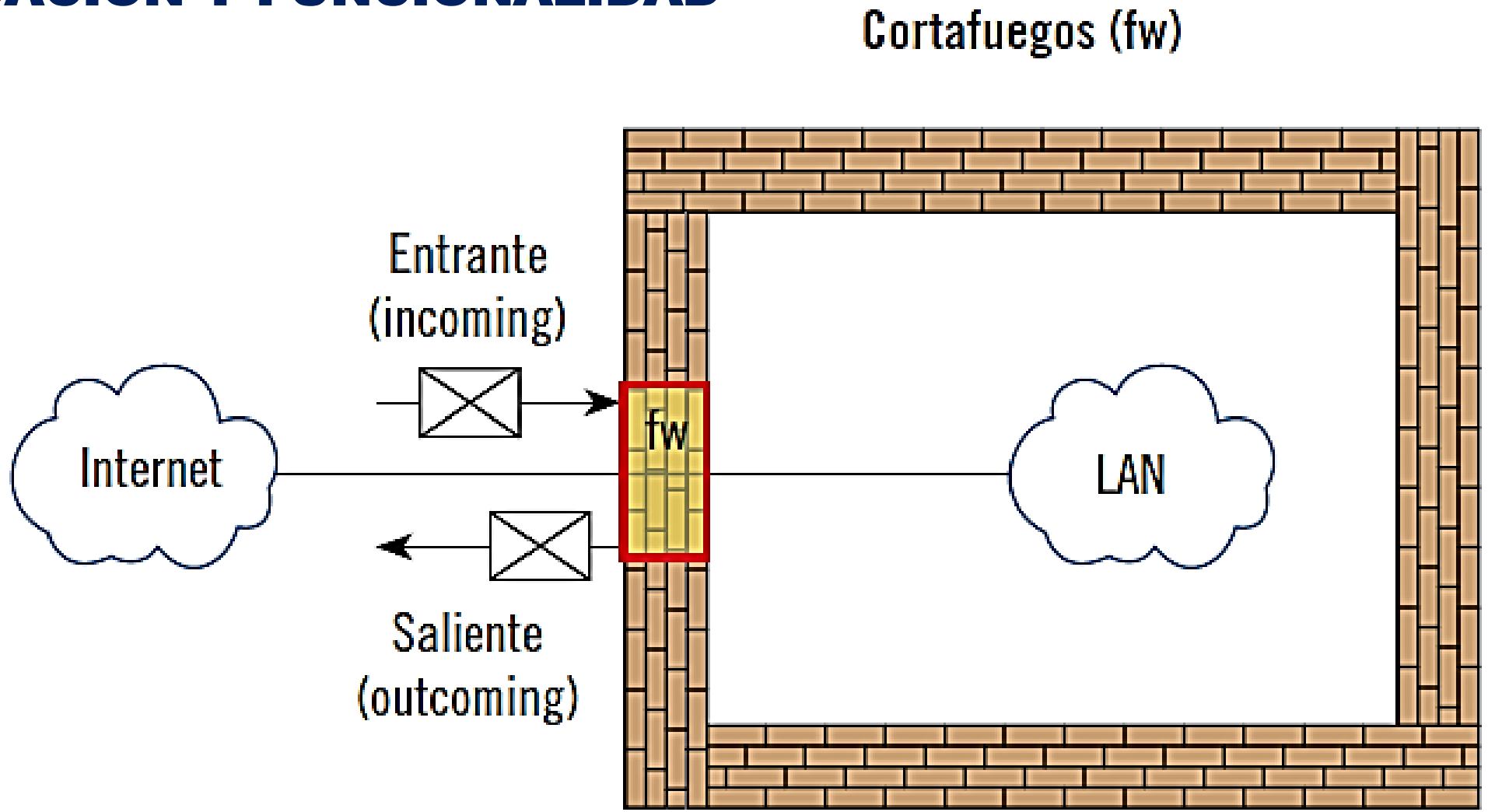
EL **ESQUEMA NACIONAL DE SEGURIDAD** INDICA QUE:

"SE DISPONDRÁ UN SISTEMA CORTAFUEGOS QUE SEPARE LA RED INTERNA DEL EXTERIOR, DE FORMA QUE TODO EL TRÁFICO PASE POR ESTE PUNTO, Y QUE SOLO SE DEJE PROGRESAR LOS FLUJOS DE TRÁFICO PREVIAMENTE AUTORIZADOS"



LOS SISTEMAS DE INTERCONEXIÓN ENTRE LA RED DE LA EMPRESA Y OTRAS REDES **DEBEN SER APROPIADOS** PARA LAS MEDIDAS DE CONTROL DE ACCESO LÓGICO QUE SE NECESITEN.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

SE PUEDE PENSAR QUE LOS ATAQUES DE SEGURIDAD SUCEDEN DE MANERA ALEATORIA Y QUE LAS INCIDENCIAS SON, POR LO TANTO, CONSECUENCIA DE LA MALA SUERTE.

SIN EMBARGO**, FRECUENTEMENTE SERÁN FRUTO DEL DESCONOCIMIENTO**, **FALTA DE CONCIENCIACIÓN** SOBRE SEGURIDAD DE LA INFORMACIÓN, O DE **LA OBSERVACIÓN QUE UN POTENCIAL ATACANTE**, HAGA DE LOS HÁBITOS DE LOS USUARIOS.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

EL ATACANTE DEBE OBTENER INFORMACIÓN DEL SISTEMA ATACADO PARA EXPLOTAR SUS VULNERABILIDADES Y QUE UN ACCESO FORZADO AL SISTEMA LE RESULTE MÁS FÁCIL, CÓMODO, Y RÁPIDO.

ENTRE LA INFORMACIÓN QUE PUEDE RESULTAR VALIOSA, CABRÍA DESTACAR:

LOS HORARIOS DE TRABAJO, NOMBRES DE USUARIO, CAMBIOS REALIZADOS EN LA EMPRESA, APLICACIONES EXISTENTES, SISTEMAS OPERATIVOS Y APLICACIONES EMPLEADAS, PROBLEMAS E INCIDENCIAS MÁS FRECUENTES, MARCA DE ORDENADORES DE USUARIO, MARCA DE IMPRESORAS, PROVEEDORES CON LOS QUE SE TRABAJA, NOMBRE DE CLIENTES, SI EXISTE WIFI O NO, SERVICIOS EXTERNOS A LOS QUE ACCEDE EL USUARIO, TIPO DE CORREO ELECTRÓNICO, E INCLUSO LAS CLAVES, SU FRECUENCIA DE CAMBIO Y COMPLEJIDAD.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

PARA LA OBTENCIÓN DE INFORMACIÓN QUE FACILITE DIRIGIR EL ATAQUE, CONVIENE MENCIONAR ESPECIALMENTE LAS SIGUIENTES **TÉCNICAS** QUE PODRÍA EMPLEAR UN ATACANTE:

- **EL EMPLEO DE MATERIAL FÍSICO,** COMO LA CORRESPONDENCIA, LOS ESTADOS DE CUENTA QUE LLEGAN A LOS DOMICILIOS, CUALQUIER TIPO DE PAPEL, INCLUSO LOS DESECHADOS A LA BASURA, O SIMPLEMENTE LA VIGILANCIA Y OBSERVACIÓN.
- **LAS TÉCNICAS DE INGENIERÍA SOCIAL,** QUE SON UN CONJUNTO DE PRÁCTICAS ACTIVAS COMO CONVERSACIONES, O LLAMADAS TELEFÓNICAS, CORREOS ELECTRÓNICOS, GENERALMENTE CON SUPLANTACIÓN DE LA IDENTIDAD, PARA ENGAÑAR AL USUARIO Y OBTENER INFORMACIÓN DE MANERA DIRECTA O INDIRECTA (POR NEGACIÓN).

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

LOS TIPOS DE AMENAZAS LÓGICAS Y, POR LO TANTO, LOS TIPOS DE ATAQUES QUE PUEDE SUFRIR UNA COMUNICACIÓN O FLUJO DE INFORMACIÓN DESDE UN EMISOR A UN RECEPTOR (*SIN QUE INTERVENGAN TERCEROS EN LA COMUNICACIÓN*), **SE DIVIDEN** TRADICIONALMENTE **EN CUATRO TIPOS**:

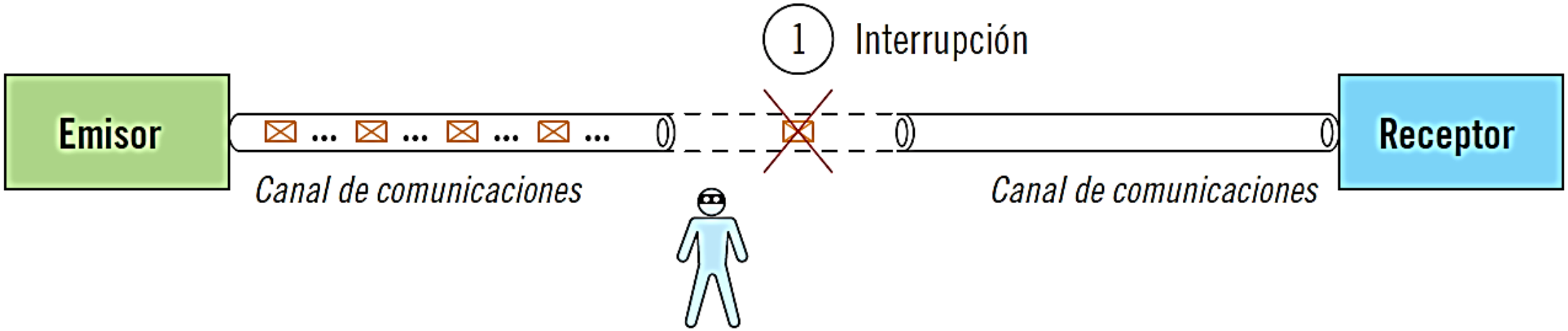
- **ATAQUE DE INTERRUPCIÓN**
- **ATAQUE DE INTERCEPTACIÓN**
- **ATAQUE DE MODIFICACIÓN**
- **ATAQUE DE FABRICACIÓN**

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

ATAQUE DE INTERRUPCIÓN

CONSISTENTE EN ***QUE UN OBJETO DEL SISTEMA NO ESTÉ DISPONIBLE***.

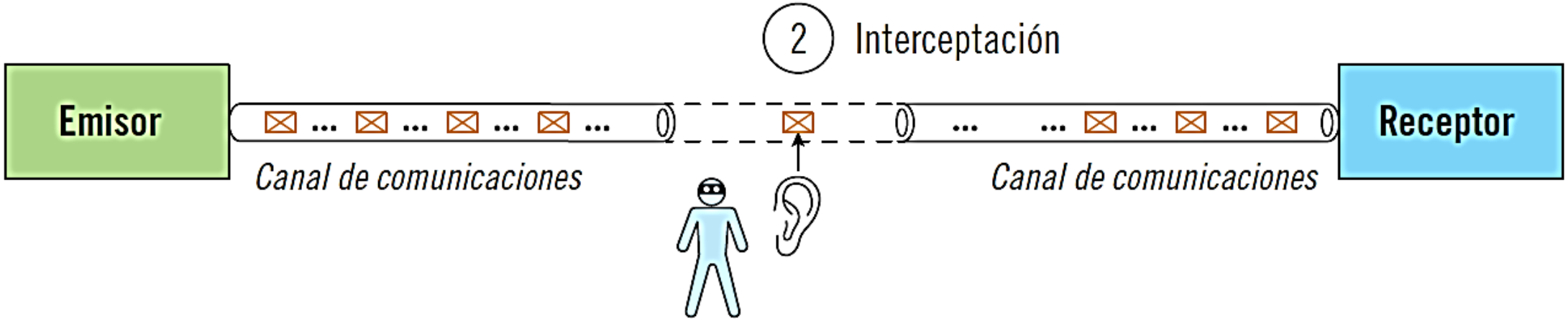


2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

ATAQUE DE INTERCEPTACIÓN

CONSISTENTE EN QUE UNA PERSONA O PROGRAMA CONSIGA ***TENER UN ACCESO NO AUTORIZADO A UN OBJETO DEL SISTEMA***.

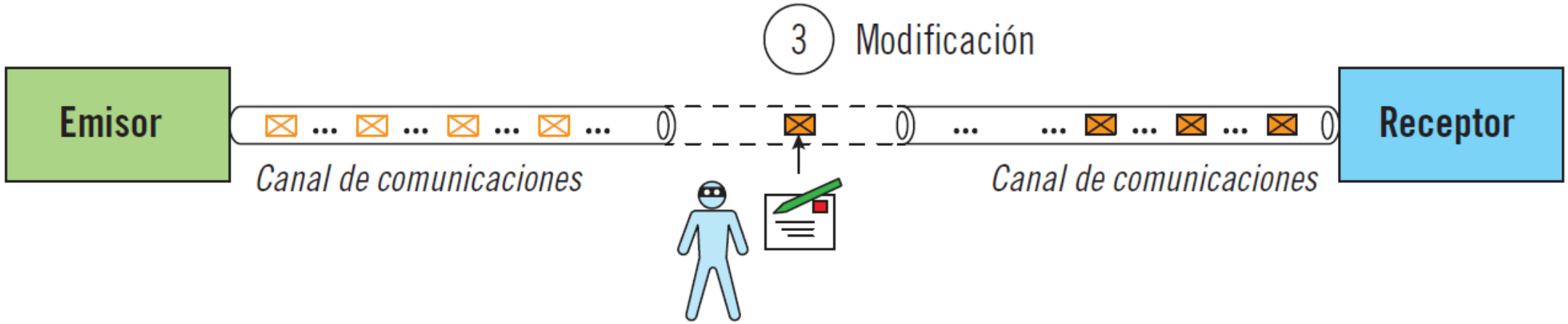


2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

ATAQUE DE MODIFICACIÓN

CONSISTENTE EN QUE, ***ADEMÁS DE LOGRAR INTERCEPTAR UN OBJETO, SE LOGRE MODIFICARLO***; LO QUE PUEDE INCLUIR LA DESTRUCCIÓN COMPLETA Y POR TANTO LA INTERRUPCIÓN.

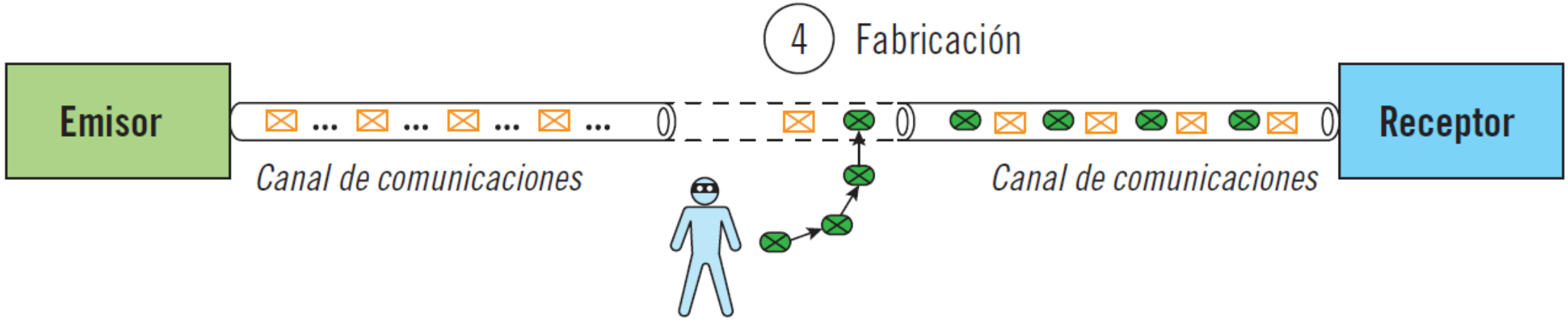


2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE ATAQUES

ATAQUE DE FABRICACIÓN

CONSISTENTE EN QUE SE REALICE ***UNA MODIFICACIÓN PARA CONSEGUIR UN OBJETO SIMILAR AL ATACADO***, DE FORMA QUE SEA DIFÍCIL DISTINGUIR ENTRE EL OBJETO ORIGINAL Y EL FABRICADO.

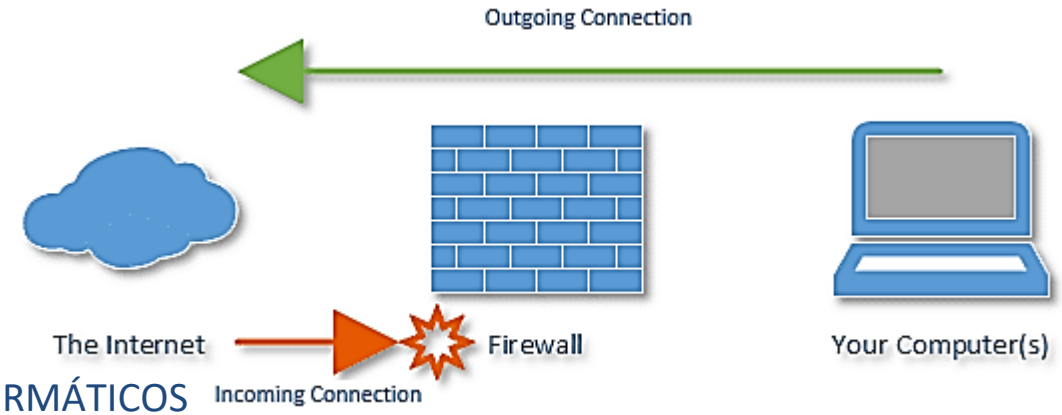


2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

SE ENTIENDE POR CORTAFUEGOS O FIREWALL, AL **CONJUNTO DE EQUIPOS EXISTENTES ENTRE DOS REDES, CON LA FINALIDAD DE RESTRINGIR Y FILTRAR EL FLUJO DE INFORMACIÓN ENTRE ELLAS**.

HABITUALMENTE, SE SEPARARÁ LA RED INTERNA DE LA EMPRESA DE INTERNET, GENERALMENTE MEDIANTE UNO O DOS EQUIPOS, QUE FORMAN UN ÚNICO FIREWALL.



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

TAMBIÉN **SE PUEDEN DEFINIR SUBREDES DENTRO DE LA EMPRESA, Y SE PUEDEN AISLAR MEDIANTE FIREWALLS**; POR EJEMPLO, PUEDE HABER UNA SUBRED PARA AQUELLOS EQUIPOS QUE CONTIENEN INFORMACIÓN CONFIDENCIAL, Y OTRA SUBRED PARA EL RESTO DE LOS EQUIPOS.

LOS CORTAFUEGOS PERMITEN IMPLEMENTAR DETERMINADOS ASPECTOS DE LA POLÍTICA DE SEGURIDAD DE LA EMPRESA, Y SON UN SISTEMA FUNDAMENTAL PARA LA SEGURIDAD LÓGICA.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

SE PUEDEN CLASIFICAR SEGÚN DIVERSOS CRITERIOS. EN FUNCIÓN DE LA **CAPA OSI DONDE ACTÚA**, EXISTEN:

- **FIREWALLS A NIVEL DE RED**
- **FIREWALL A NIVEL DE APLICACIÓN**

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

FIREWALLS A NIVEL DE RED

QUE ACTÚAN EXCLUSIVAMENTE A ESTE NIVEL, Y POR LO TANTO ESTÁN CONSTITUIDOS POR **ENCAMINADORES O ROUTER**, QUE SON ELEMENTOS DE LA CAPA DE RED.

ESTOS EQUIPOS **SE UBICAN ENTRE LA RED INTERNA Y LA RED EXTERNA** (INTERNET), **Y SOLO PUEDEN PROTEGER MEDIANTE FILTRADO DE LOS PAQUETES DE RED**.

EL FILTRADO PERMITE **ACEPTAR, RECHAZAR**, O SIMPLEMENTE **NO RESPONDER,** A LOS PAQUETES QUE PROCEDAN DE UN ORIGEN O HACIA UN DESTINO CONCRETO.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

FIREWALL A NIVEL DE APLICACIÓN

DENOMINADOS **PROXY**, QUE SE **UBICAN ENTRE CLIENTES DE LA RED INTERNA Y UN SERVIDOR UBICADO EN LA RED EXTERNA, DE MANERA QUE NO HAY COMUNICACIÓN DIRECTA DE LOS CLIENTES INTERNOS A LOS SERVIDORES DE APLICACIONES EXTERNOS**.

POR EL CONTRARIO, UN CLIENTE SE CONECTA AL PROXY, Y ESTE, SE CONECTA AL SERVIDOR DE APLICACIÓN EXTERNO.

TÉCNICAMENTE, UN PROXY NO ES UN FIREWALL, SINO QUE MÁS BIEN FORMA PARTE DEL MISMO: **EL FIREWALL BLOQUEA TRÁFICO NO PERMITIDO, Y EL PROXY PERMITE ACCESO CONTROLADO.**

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

SEGÚN EL MÉTODO DE PROTECCIÓN QUE SE APLIQUE, EXISTEN DOS TIPOS DE SISTEMAS:

- **PROTECCIÓN MEDIANTE FILTRADO DE PAQUETES**
  - *FILTRADO ESTÁTICO DE PAQUETES*
  - *FILTRADO DINÁMICO DE PAQUETES*
- **PROTECCIÓN MEDIANTE SERVIDORES PROXY**
  - *PASARELAS O PROXY DE APLICACIÓN*
  - *PROXY A NIVEL DE CIRCUITO*

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

PROTECCIÓN MEDIANTE FILTRADO DE PAQUETES

ESTE ES EL ÚNICO MÉTODO DE PROTECCIÓN QUE PUEDEN APLICAR LOS FIREWALLS DE RED, QUE PUEDE REALIZARSE DE DOS MANERAS:

FILTRADO ESTÁTICO DE PAQUETES

EN EL CUAL **TANTO LOS PAQUETES ENTRANTES, COMO LOS PAQUETES SALIENTES SE FILTRAN**, PARA AUTORIZAR O RECHAZAR SU PROGRESO EN BASE A **UNAS REGLAS FIJAS DEFINIDAS**, ES DECIR QUE NO CAMBIAN. EL CASO MÁS HABITUAL ES UN **ROUTER**.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

PROTECCIÓN MEDIANTE FILTRADO DE PAQUETES

FILTRADO DINÁMICO DE PAQUETES

O **DE INSPECCIÓN Y SEGUIMIENTO DE ESTADO**, EN LOS CUALES TAMBIÉN **SE APLICAN REGLAS PARA EL FILTRADO, PERO ESTAS SON DINÁMICAS**.

PUEDE SER QUE EL FIREWALL PUEDA RECORDAR LOS PAQUETES SALIENTES PARA PERMITIR LOS PAQUETES DE RESPUESTA ENTRANTES; ES DECIR, SE ADMITEN TODAS LAS RESPUESTAS QUE OBEDEZCAN A CONEXIONES INICIADAS DESDE LA RED INTERNA DE LA EMPRESA, SIN NECESIDAD DE DEFINIR REGLAS FIJAS PARA ELLO.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

PROTECCIÓN MEDIANTE SERVIDORES PROXY

ESTE MÉTODO ***SOLO PUEDEN APLICARLO LOS FIREWALLS A NIVEL DE APLICACIÓN***, QUE TAMBIÉN CONTEMPLA DOS TIPOS BÁSICOS:

PASARELAS O PROXY DE APLICACIÓN

PERMITEN O NO LA CONEXIÓN A UNA APLICACIÓN (HTTP, FTP, SMTP), CASI SIEMPRE CON MECANISMOS DE AUTENTICACIÓN PARA SABER SI EL USUARIO TIENE AUTORIZADO O NO PARA EL USO DEL PROTOCOLO CONCRETO, Y PARA UN ORIGEN Y DESTINO CONCRETOS.

POR EJEMPLO, UN PROXY DE APLICACIÓN FTP PODRÍA RECHAZAR LOS COMANDOS PARA BORRAR ARCHIVOS, O PODRÍA RECHAZAR LA TRANSFERENCIA DE FICHEROS DE TAMAÑO SUPERIOR A UNO DADO, O DE UN TIPO CONCRETO, CON EL PROPÓSITO DE REDUCIR EL RIESGO DE EVASIÓN DE INFORMACIÓN.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

TIPOS DE CORTAFUEGOS

PROTECCIÓN MEDIANTE SERVIDORES PROXY

PROXY A NIVEL DE CIRCUITO

QUE **CREAN UN CANAL DE COMUNICACIÓN ENTRE EL CLIENTE Y EL SERVIDOR**, INDEPENDIENTEMENTE DEL TIPO DE SOLICITUD QUE HAGA EL CLIENTE.

SUELEN REQUERIR QUE EL CLIENTE EJECUTE UN SOFTWARE ESPECÍFICO.

LA FUNCIONALIDAD ES MÁS COMPLEJA QUE LA DE UN ROUTER, Y SUELEN INCLUIR FUNCIONES DE SEGURIDAD COMO AUTENTICACIÓN MEDIANTE CONTRASEÑAS.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

NO HAY UNA FORMA ÚNICA DE CONSTRUIR UN FIREWALL. DEPENDE DE LOS REQUISITOS DE SEGURIDAD DE LA EMPRESA, DE LAS REDES INTERNAS QUE HAYA, DE LOS SERVICIOS ACCESIBLES, Y DEL PRESUPUESTO DISPONIBLE.

VEAMOS LAS **CONSTRUCCIONES MÁS HABITUALES** QUE SE SUELEN EMPLEAR EN ENTORNOS DE PEQUEÑA Y MEDIANA EMPRESA, SEÑALANDO PARA CADA EJEMPLO ALGUNAS VENTAJAS E INCONVENIENTES QUE PUEDEN SER O NO DE RELEVANCIA EN CADA CASO CONCRETO.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

ROUTER DE FILTRADO (SCREENING ROUTER)

LOS ROUTER HABITUALMENTE **PERMITEN DEFINIR REGLAS PARA BLOQUEAR EL TRÁFICO ENTRANTE O SALIENTE SEGÚN LAS DIRECCIONES**.

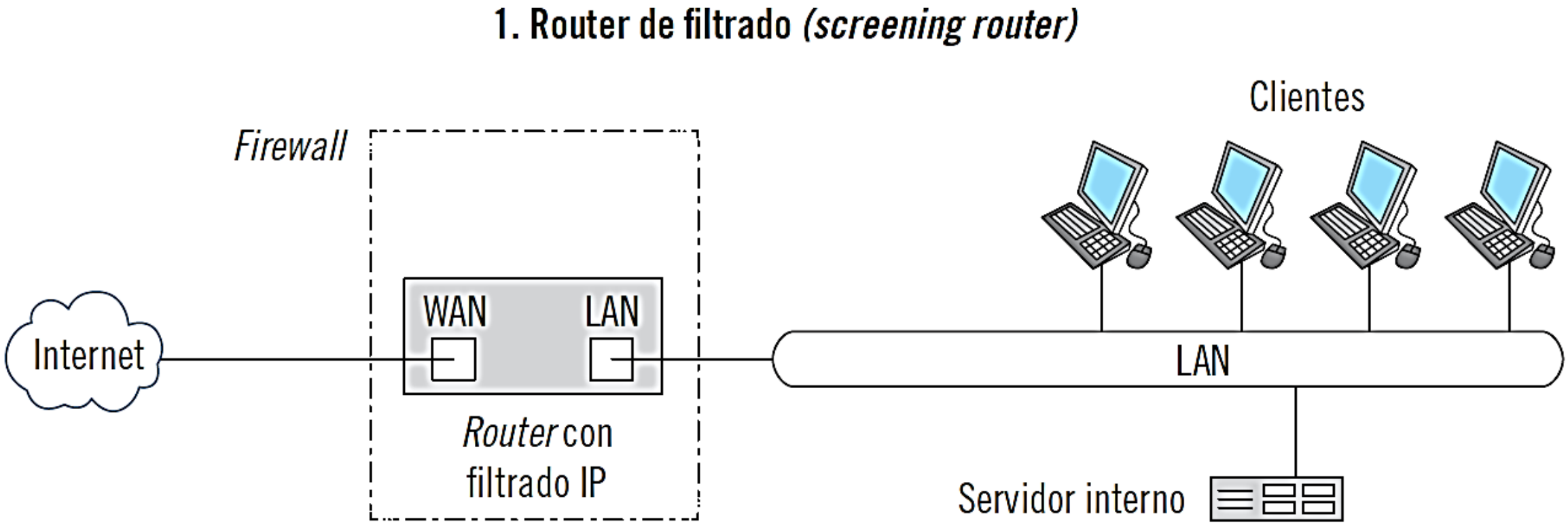
SON EL MECANISMO MÁS SENCILLO Y ECONÓMICO (LO SUELE ENTREGAR EL ISP).

SUELEN INCORPORAR LA FUNCIÓN **NAT** (**NETWORK ADDRESS TRANSLATION**), QUE PERMITE **COMPARTIR UNA DIRECCIÓN IP PÚBLICA PARA TODAS LAS DIRECCIONES IP PRIVADAS DE LA RED LAN**.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

ROUTER DE FILTRADO (SCREENING ROUTER)



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

ROUTER DE FILTRADO (SCREENING ROUTER)

VENTAJAS

- SENCILLEZ
- ROBUSTEZ LÓGICA
- ELEVADO RENDIMIENTO

DESVENTAJAS

- SOLO DISPONE DE UNA TOMA DE RED
- NECESIDAD DE CONSTRUIR MUCHAS REGLAS FIJAS PARA PERMITIR EL FUNCIONAMIENTO DESEADO
- BAJA CAPACIDAD DE REGISTRO Y MONITORIZACIÓN
- LIMITACIONES DE PROTECCIÓN QUE PROPORCIONA.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN CON UNA RED (BASTION HOST O SINGLE-HOMED HOST)

SE EMPLEA UNA **ESTACIÓN DE TRABAJO ROBUSTECIDA O BASTIONADA**, PARA PROTEGER TODA LA RED, **FILTRANDO EL TRÁFICO AL FUNCIONAR COMO UNA PASARELA O PUERTA DE ENLACE DE APLICACIÓN**.

POR EJEMPLO, EL BASTIÓN PUEDE COMPROBAR SI UN CLIENTE PUEDE NAVEGAR POR INTERNET, Y EN ESE CASO PERMITIR LA CONEXIÓN ENTRE EL CLIENTE Y EL SERVIDOR WEB EXTERNO.

DEBE DESHABILITARSE EL ENVÍO DIRECTO DEL TRÁFICO IP INTERNO AL EXTERNO (IP FORWARDING), BLOQUEÁNDOSE POR DEFECTO QUE PASE TODO EL TRÁFICO.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN CON UNA RED (BASTION HOST O SINGLE-HOMED HOST)

EL BASTIÓN FORMA PARTE DE LA RED, Y CONSTITUYE LA PARTE MÁS AVANZADA DE ESTA, O LO QUE ES LO MISMO, **ES EL INTEGRANTE DE LA RED MÁS EXTERNO Y EXPUESTO A LOS ATAQUES**, POR LO QUE **DEBE ROBUSTECERSE** PARA PODER DESEMPEÑAR LAS FUNCIONES DE PROTECCIÓN DE LA RED.

RESULTA PRIMORDIAL EMPLEAR LAS VERSIONES MÍNIMAS DEL SISTEMA OPERATIVO, ELIMINANDO LOS SERVICIOS INNECESARIOS, Y QUE LOS USUARIOS INTERNOS TENGAN POSIBILIDAD DE ACCEDER AL EQUIPO MÁS ALLÁ DE USARLO COMO ADMINISTRADOR.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

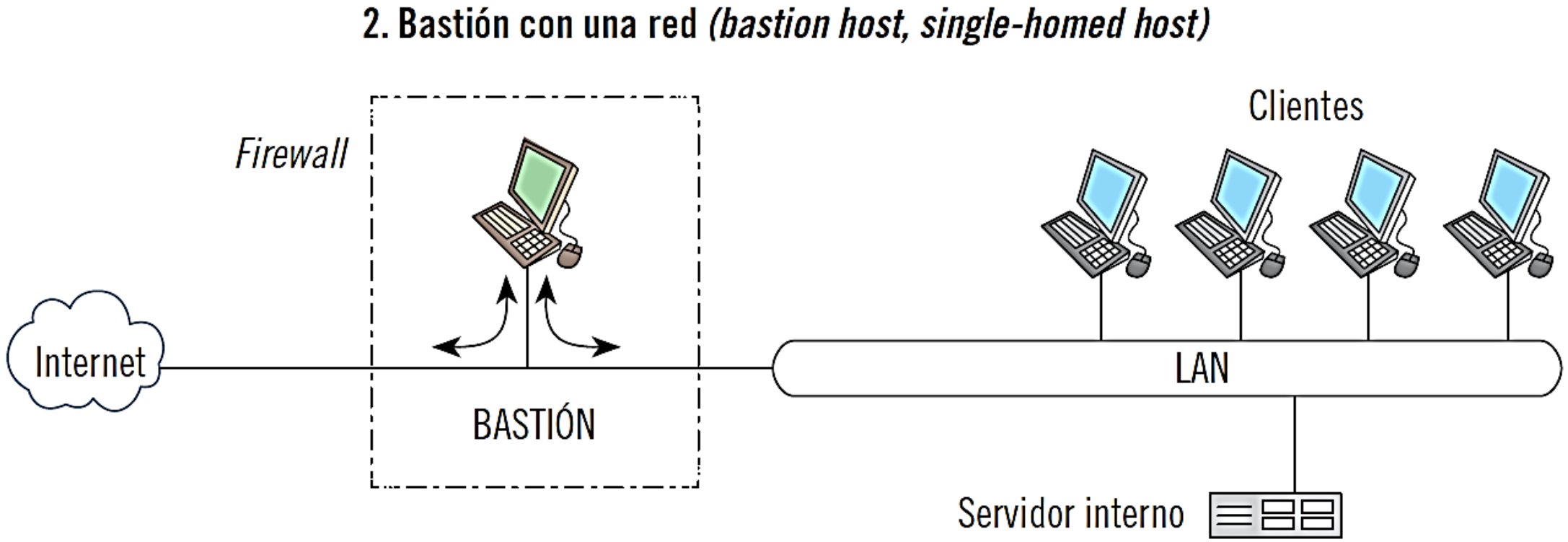
BASTIÓN CON UNA RED (BASTION HOST O SINGLE-HOMED HOST)

GENERALMENTE, **NO REALIZARÁN FUNCIONES DE FILTRADO POR PAQUETES O FILTRADO IP, Y SOLO INCLUYE UNA TARJETA DE RED** DE MANERA QUE EL TRÁFICO DE INTERNET DEBE SERLE ENCAMINADO (GENERALMENTE MEDIANTE UN ROUTER QUE NO APORTE NINGUNA PROTECCIÓN) A LA VEZ QUE LOS CLIENTES DE LA LAN TAMBIÉN SE CONFIGURAN PARA ENVIARLE SU TRÁFICO HACIA INTERNET.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN CON UNA RED (BASTION HOST O SINGLE-HOMED HOST)



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN CON UNA RED (BASTION HOST O SINGLE-HOMED HOST)

VENTAJAS

- APORTA UNA MAYOR SEGURIDAD
- DISPONE DE MAYOR FLEXIBILIDAD Y POSIBILIDADES PARA APLICAR LA POLÍTICA DE SEGURIDAD
- MAYORES CAPACIDADES DE REGISTRO Y MONITORIZACIÓN.

DESVENTAJAS

- NO HAY SEPARACIÓN FÍSICA ENTRE LA RED SIN PROTEGER Y LA RED PROTEGIDA
- NECESITARÁ DE UN MANTENIMIENTO, Y REVISIONES MÁS FRECUENTES POR LA MAYOR EXPOSICIÓN A ATAQUES QUE PRESENTA
- EN CASO DE COMPROMISO SE DEBE DISPONER DE UN EQUIPO CONFIGURADO Y PREPARADO PARA REEMPLAZAR EL BASTIÓN ORIGINAL
- SU RENDIMIENTO ES BASTANTE MENOR
- EXISTE UN SOBRECOSTE, POR EL TRABAJO NECESARIO EN PREPARAR EL BASTIONADO DEL EQUIPO.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN CON DOS REDES (DUAL-HOMED HOST)

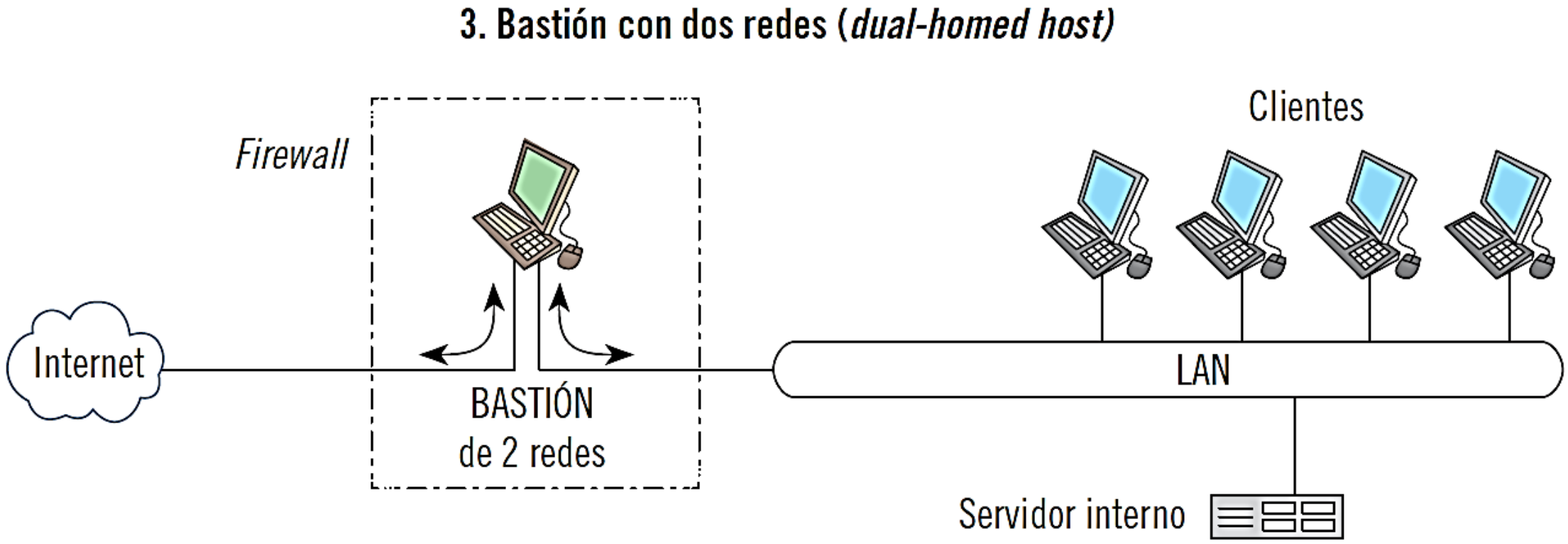
EL BASTIÓN INCORPORA 2 TARJETAS DE RED: **LA EXTERNA**, CONECTADA A INTERNET, Y **LA INTERNA**, CONECTADA A LA LAN. SE DENOMINA ESTACIÓN DE DOBLE DOMICILIO, PORQUE EL BASTIÓN ESTÁ PRESENTE EN AMBAS REDES A LA VEZ, DE MANERA QUE **SE LOGRA TENER REDES FÍSICAMENTE SEPARADAS.**

SI BIEN PODRÍA DESEMPEÑAR LA FUNCIÓN DE ROUTER, NO ES EFECTIVO QUE LO HAGA, Y DEBE DESHABILITARSE EL ACCESO DIRECTO DEL TRÁFICO IP DE UN INTERFAZ A OTRA, BLOQUEÁNDOSE POR DEFECTO QUE PASE TODO EL TRÁFICO.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN CON DOS REDES (DUAL-HOMED HOST)



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

SERVIDOR PROXY

EL TÉRMINO **PROXY** SE EMPLEAPARA REFERIRSE A UN SUSTITUTO O REEMPLAZO DE OTRO ELEMENTO. ASÍ, **LA SOLICITUD DE UN RECURSO A UN SERVIDOR SE DIVIDE EN DOS PASOS:** UNA **SOLICITUD DE UN RECURSO A UN PROXY** Y UNA SEGUNDA **SOLICITUD DEL PROXY AL SERVIDOR REAL**. **UN PROXY ES UNA APLICACIÓN QUE SE EJECUTA EN SUSTITUCIÓN DE OTRA**.

UNA PETICIÓN WEB DIRIGIDA A UN CORTAFUEGOS NO ES REENCAMINADA DIRECTAMENTE HACIA EL SERVIDOR FINAL, SINO **QUE ES ATENDIDA POR EL SERVIDOR PROXY** QUE INCORPORA EL FIREWALL, **Y** A LA VEZ **EL SERVIDOR PROXY DEL FIREWALL DIRIGE LA PETICIÓN AL SERVIDOR REAL**.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

SERVIDOR PROXY

DE ESTA FORMA, **EL CLIENTE Y EL SERVIDOR FINAL NUNCA ESTÁN EN CONTACTO DIRECTO**.

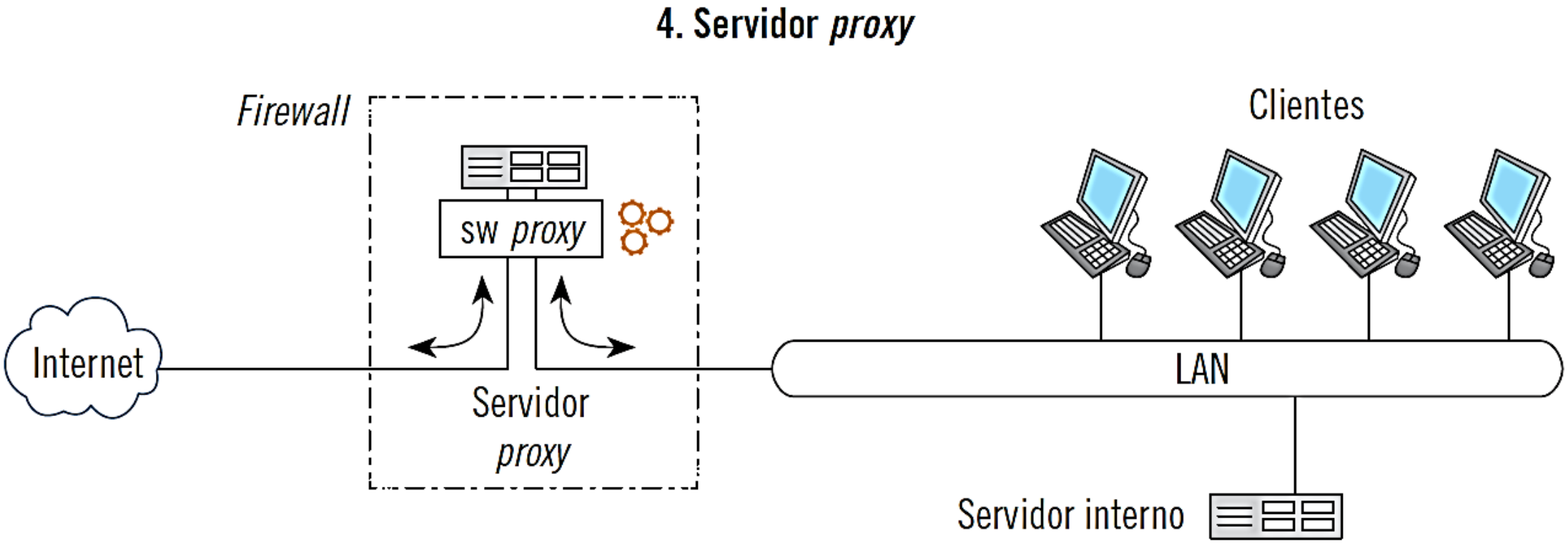
LOS PROXY MÁS HABITUALES SON LOS **PROXY PARA APLICACIÓN WEB**, QUE SE DENOMINAN SIMPLEMENTE “PROXY”; NO OBSTANTE, EXISTEN SERVIDORES PROXY PARA **SMTP, FTP**, Y OTROS.

EL SERVIDOR PROXY TENDRÁ CONFIGURADO UN CONTROL DE ACCESO, DE FORMA QUE SE LOGRA IMPLEMENTAR EL FILTRADO POR APLICACIÓN.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

SERVIDOR PROXY



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

SERVIDOR PROXY

VENTAJAS

- SE TIENE EL MÁXIMO NIVEL DE CONTROL SOBRE LAS CONEXIONES
- ELEVADA CAPACIDAD DE MONITORIZACIÓN Y REGISTRO.

DESVENTAJAS

- PÉRDIDA DE RENDIMIENTO
- SE NECESITA UN MANTENIMIENTO Y SUPERVISIÓN FRECUENTE

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN FILTRADO (SCREENED HOST)

SE EMPLEARÁ **UN BASTIÓN** AL QUE SE LE ANTEPONE UN EQUIPO QUE REALICE EL FILTRADO DE PAQUETES DE RED (**ROUTER)**.

EL **ROUTER SE CONFIGURA** PARA QUE **SOLO ADMITA** CIERTAS CONEXIONES O TIPOS DE **TRÁFICO HACIA EL BASTIÓN**, DE MANERA QUE SOLO ENVÍE EL TRÁFICO DE INTERNET, UNA VEZ FILTRADO, HACIA EL BASTIÓN. TAMBIÉN SE CONFIGURA PARA QUE **SOLO ADMITA CONEXIONES INTERNAS DESDE EL BASTIÓN**.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN FILTRADO (SCREENED HOST)

EL TRAMO DE RED COMPRENDIDO ENTRE EL ROUTER Y EL BASTIÓN SE DENOMINA **ZONA DESMILITARIZADA O DMZ (DEMILITARIZED ZONE)**.

LA **DMZ NO ES PARTE DE LA RED EXTERNA NI DE LA RED INTERNA**, ES UNA ZONA DE TRANSICIÓN (BUFFER) ENTRE AMBAS.

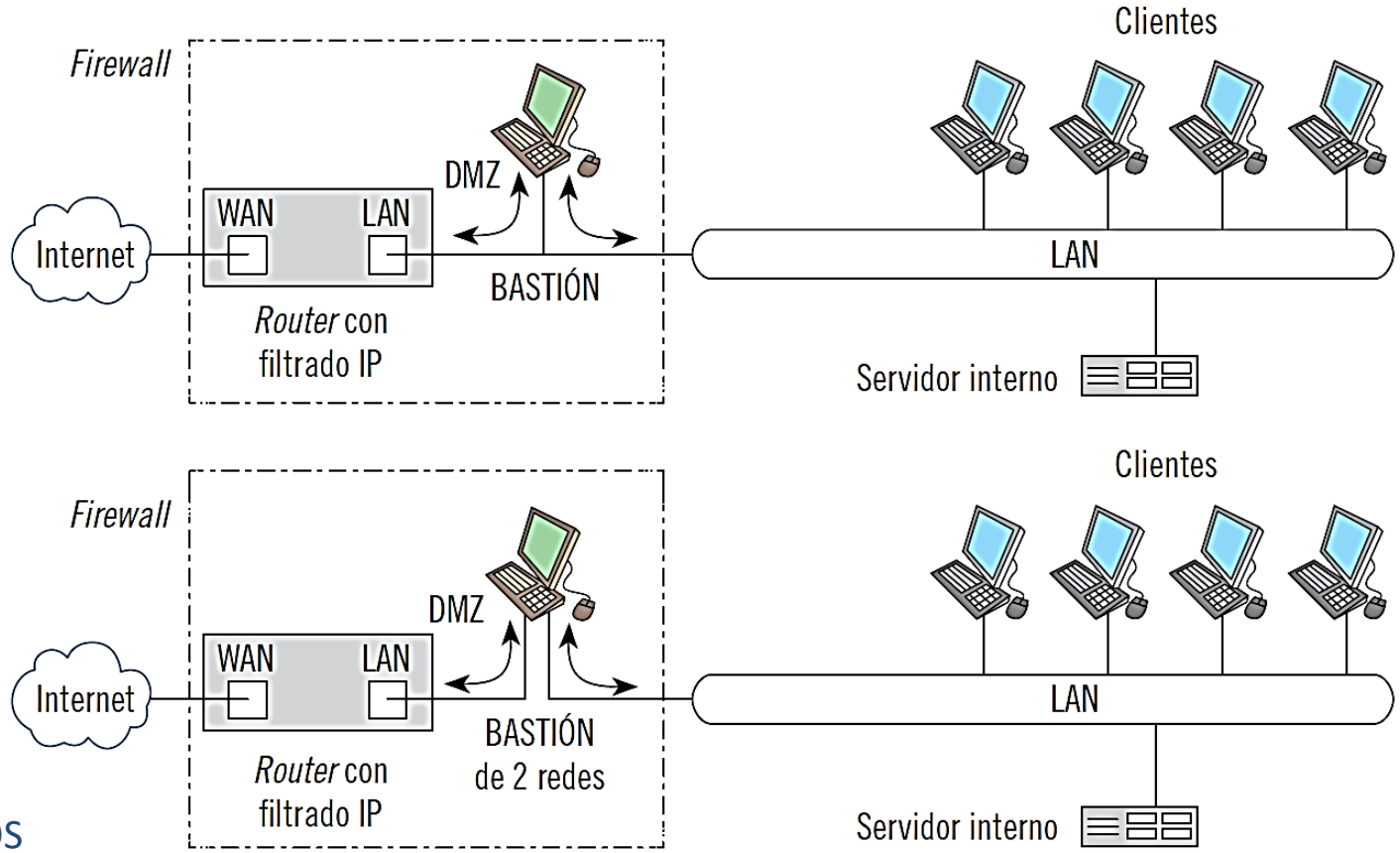
SI SE EMPLEA UN BASTIÓN DE UNA RED, LA ZONA DMZ SOLO DISPONE DE SEPARACIÓN LÓGICA, MIENTRAS QUE, SI SE EMPLEA UN BASTIÓN DE DOS REDES, LA SEPARACIÓN TAMBIÉN ES FÍSICA. SIEMPRE QUE SEA POSIBLE, SE DEBE EMPLEAR UN BASTIÓN DE DOS REDES.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

BASTIÓN FILTRADO (SCREENED HOST)

5. Bastión filtrado *(Screened host)*



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

SUBRED FILTRADA (SCREENED SUBNET)

ESTA ES **LA CONFIGURACIÓN MÁS SEGURA**, PORQUE **EL BASTIÓN SE SEPARA DE LA RED INTERNA MEDIANTE UN SEGUNDO EQUIPO DE FILTRADO DE PAQUETES** (UN ROUTER O UN FIREWALL).

EL BASTIÓN QUEDA **PROTEGIDO POR DOS ROUTER, UNO EXTERNO Y UNO INTERNO**, GENERÁNDOSE TRAMOS DE RED DESMILITARIZADOS, O DMZ QUE PUEDEN ESTAR SEPARADOS LÓGICA O FÍSICAMENTE.

DE ESTA MANERA, SI UN ATACANTE LOGRARA COMPROMETER EL BASTIÓN, AÚN NO DISPONDRÍA DE ACCESO COMPLETO A LA RED, YA QUE DEBERÍA VULNERAR UN SEGUNDO ROUTER.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

SUBRED FILTRADA (SCREENED SUBNET)

EN EL DISEÑO DE SUBRED FILTRADA, EL **ROUTER EXTERIOR** (FRECUENTEMENTE PROPORCIONADO POR EL ISP) DEBE CONFIGURARSE PARA QUE **SOLO PUEDA COMUNICARSE CON INTERNET Y CON EL BASTIÓN.**

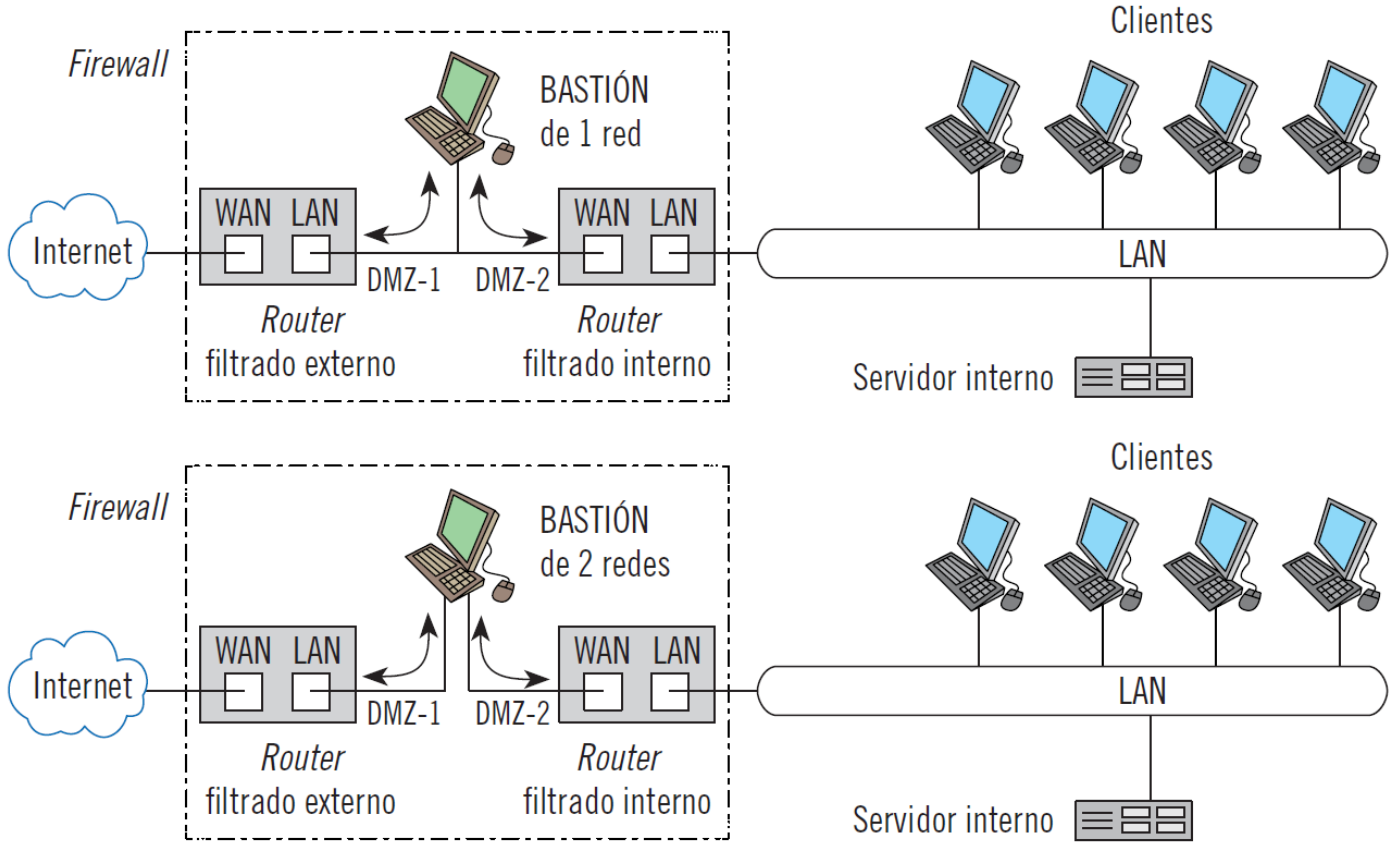
EL **ROUTER INTERIOR** DEBE CONFIGURARSE PARA QUE **SOLO PUEDA COMUNICARSE CON LA RED INTERIOR Y CON EL BASTIÓN**; AMBOS ROUTER NUNCA DEBEN COMUNICARSE ENTRE SÍ.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

SUBRED FILTRADA (SCREENED SUBNET)

6. Subred filtrada *(Screened host)*



2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS

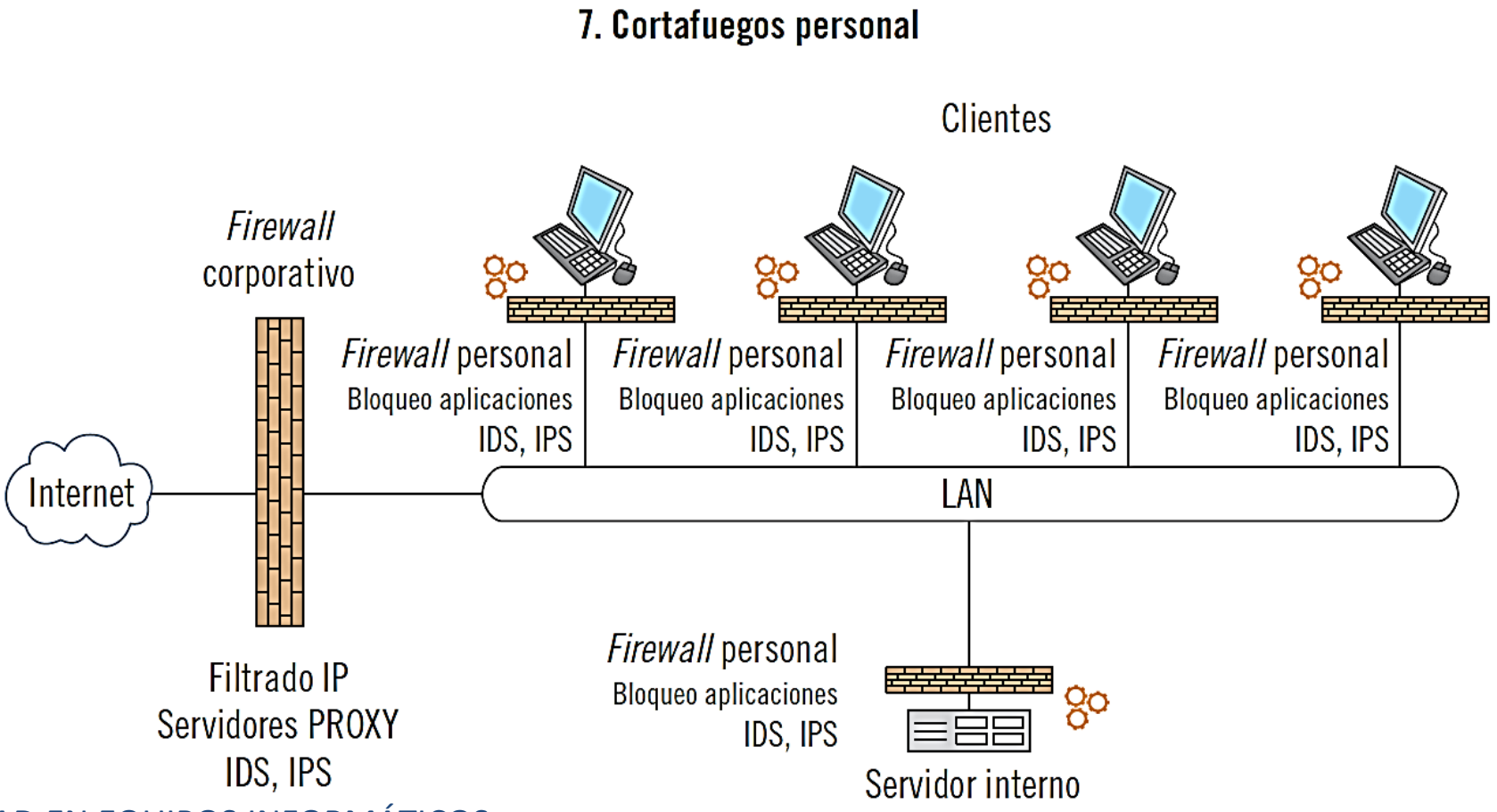
FIREWALLS PERSONALES

AUNQUE NO TIENEN UNA FUNCIÓN CORPORATIVA PROTEGIENDO A OTROS EQUIPOS, POR SU IMPORTANCIA, SE PRESENTAN LAS APLICACIONES DE CORTAFUEGOS PERSONALES QUE SE EJECUTEN EN CADA ORDENADOR (CLIENTE O SERVIDOR) QUE ESTÉ CONECTADO A LA RED.

DEBEN ACTIVARSE, PORQUE DIFICULTARÁN LA PROPAGACIÓN DE UN INCIDENTE Y CONSTITUYEN EL **PRIMER NIVEL DE DEFENSA DE CADA EQUIPO**.

2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

CONSTRUCCIÓN DE CORTAFUEGOS



CONTENIDOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. **CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ**
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

EL EMPLEO DE FIREWALLS QUE INCLUYAN DOS DISPOSITIVOS PERMITE **DEFINIR UNA SUBRED ENTRE ELLOS**, QUE NO PERTENECE NI A LA RED EXTERNA NI A LA RED INTERNA, DENOMINADA **ZONA DMZ**.

LA NUEVA SUBRED DMZ PERMITE UBICAR RECURSOS COMUNES Y SE FACILITA SEGREGAR LA LAN EN SUBREDES CON RANGOS DE RED DISTINTOS.

LOS **CRITERIOS DE SEGURIDAD** QUE SE DEBEN APLICAR PARA SEGMENTAR LA RED SE DEBEN BASAR EN UNA **EVALUACIÓN DEL RIESGO** Y **DE LOS REQUISITOS DE SEGURIDAD ESPECIALES** QUE PUEDAN EXISTIR DENTRO DE CADA UNO DE LOS DOMINIOS.

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

ESTOS PERÍMETROS DE SEGURIDAD SE IMPLEMENTAN CON FIREWALLS, QUE CONTROLAN EL ACCESO Y FLUJO DE INFORMACIÓN ENTRE ELLOS, TENIENDO EN CUENTA QUE, SI SE DISPONEN DOS FIREWALLS SEGUIDOS, SE CREA UNA DMZ, QUE APORTA GRANDES VENTAJAS. **LOS CRITERIOS DE SEGREGACIÓN DE REDES** DEBERÍAN CONTEMPLAR:

- LA POLÍTICA DE CONTROL DE ACCESOS.
- EL COSTE DE ESTAS MEDIDAS, EN TÉRMINOS MATERIALES Y DE HORAS DE TRABAJO NECESARIOS PARA LA NECESARIA MONITORIZACIÓN DE ESTOS DISPOSITIVOS.
- EL VALOR Y CLASIFICACIÓN DE LA INFORMACIÓN ALMACENADA O PROCESADA.
- SEPARAR DIFERENTES ÁREAS DE NEGOCIO, O DIFERENTES LÍNEAS COMERCIALES, REDUCIENDO EL IMPACTO QUE UN INCIDENTE EN UNA SUBRED TENDRÍA EN OTRA SUBRED. POR EJEMPLO, SEPARAR SISTEMAS DE PRODUCCIÓN, SEPARAR COMPRAS Y VENTAS, SEPARAR REDES DE OFICINA, SEPARAR REDES DE CONTROL INDUSTRIAL, SEPARAR LAS REDES DE DATOS CONFIDENCIALES, ETC.
- DEBE TENERSE EN CUENTA LA SEPARACIÓN DE REDES INALÁMBRICAS.

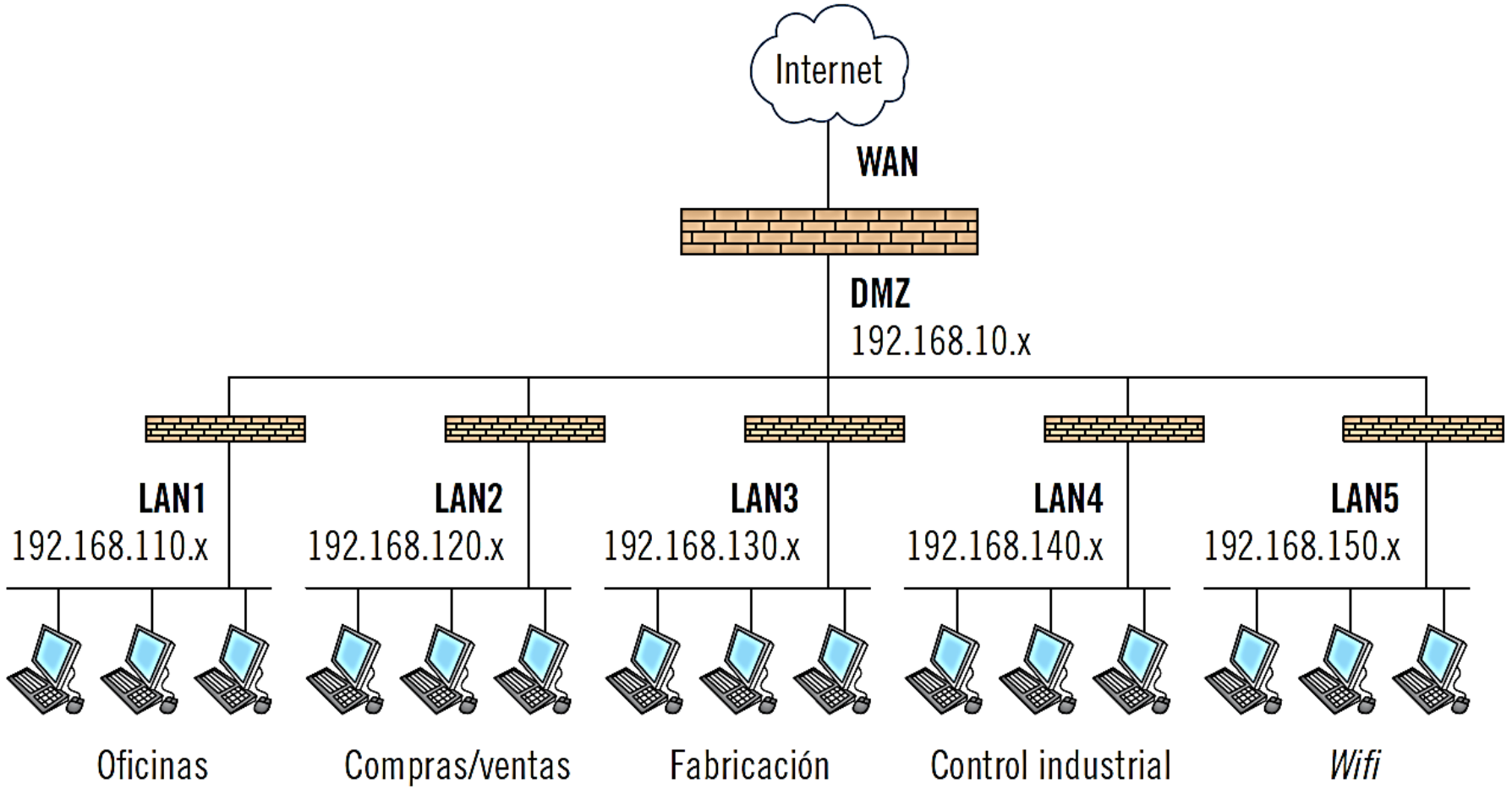
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

EL **ESQUEMA NACIONAL DE SEGURIDAD** INDICA ADEMÁS QUE DEBE SEGREGARSE EMPLEANDO **MEDIDAS QUE GARANTICEN**:

- EL CONTROL DE ENTRADA DE LOS USUARIOS QUE LLEGAN A CADA SEGMENTO
- EL CONTROL DE SALIDA DE LA INFORMACIÓN DISPONIBLE EN CADA SEGMENTO
- LOS MEDIOS FÍSICOS Y LÓGICOS QUE SE EMPLEEN PARA SEGMENTAR LA RED DEBEN ESTAR PARTICULARMENTE ASEGURADOS, MANTENIDOS Y MONITORIZADOS, COMO EN EL CASO DE LOS FIREWALLS DE ACCESO A INTERNET.

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

Diferentes subredes separadas entre sí por cortafuegos, con diferentes rangos de direcciones IP



3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

USO DE ZONAS DESMILITARIZADAS

LAS ZONAS DMZ AÑADEN SEGURIDAD, PORQUE AUMENTAN LA SEPARACIÓN ENTRE REDES.

POR EJEMPLO, EL RANGO DE DIRECCIONES IP, EMPLEADO EN LA ZONA DMZ SERÁ DIFERENTE AL RANGO DE DIRECCIONES DE LA RED PRIVADA, LO QUE AUMENTA LA DIFICULTAD PARA ACCEDER A LA RED PRIVADA.

HABITUALMENTE, **SE PUEDEN OBTENER MÁS BENEFICIOS** DE LAS ZONAS DMZ, **EMPLEÁNDOLAS PARA DIFERENTES SERVICIOS**.

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

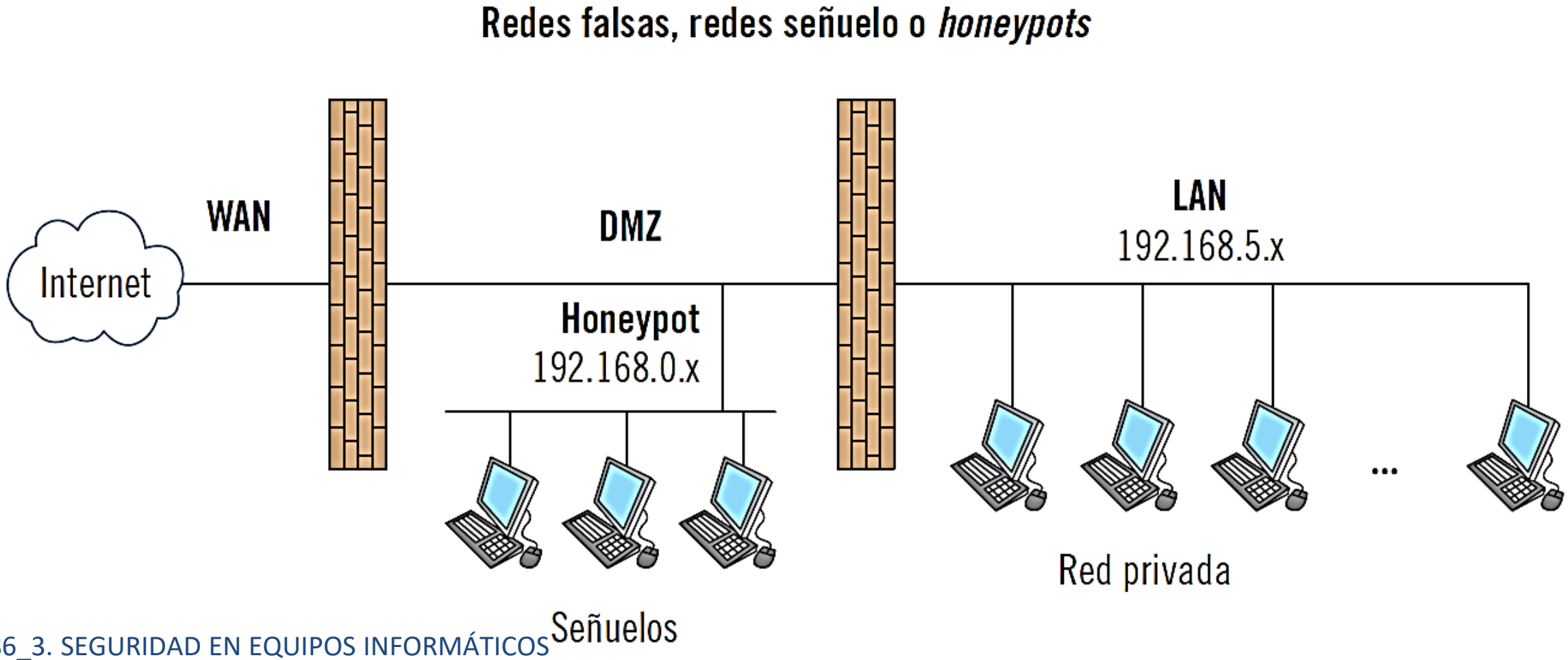
USO DE ZONAS DESMILITARIZADAS. REDES FALSAS O HONEYPOTS

TAMBIÉN CONOCIDAS COMO **REDES SEÑUELO**, CONSISTEN EN UN CONJUNTO DE **MÁQUINAS INTENCIONADAMENTE VULNERABLES QUE SIMULAN UNA RED PRIVADA NORMAL,** DE MANERA QUE UN ATACANTE QUE GANARA ACCESO A LA DMZ PENSARÍA QUE YA ESTÁ EN LA RED PRIVADA.

DEBE PRESTARSE ATENCIÓN A CONSTRUIR ESTA RED DE MANERA CUIDADOSA, POR EJEMPLO, ASEGURÁNDOSE QUE LAS MÁQUINAS DE SEÑUELO NO TENGAN INSTALADAS APLICACIONES O UTILIDADES QUE EL ATACANTE PODRÍA EMPLEAR PARA LANZAR ATAQUES A LOS FIREWALLS CIRCUNDANTES.

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

USO DE ZONAS DESMILITARIZADAS. REDES FALSAS O HONEYPOTS



3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

USO DE ZONAS DESMILITARIZADAS. UBICACIÓN DE SERVIDORES ACCESIBLES DESDE EL EXTERIOR

CUANDO SE DEBE DAR ACCESO EXTERNO A ALGUNA APLICACIÓN, ALOJADA EN LA RED DE LA EMPRESA, EL PRIMER PASO OBLIGATORIO ES **ROBUSTECER O BASTIONAR EL SERVIDOR DONDE ESTÉ INSTALADA**.

LOS **SERVIDORES ACCESIBLES DESDE INTERNET SE DEBEN UBICAR EN ZONA DMZ.** DE ESTA FORMA, EL FIREWALL EXTERNO SE CONFIGURARÁ PARA QUE LOS ACCESOS A LA APLICACIÓN SE DIRIJAN EXCLUSIVAMENTE AL SERVIDOR DE LA APLICACIÓN.

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

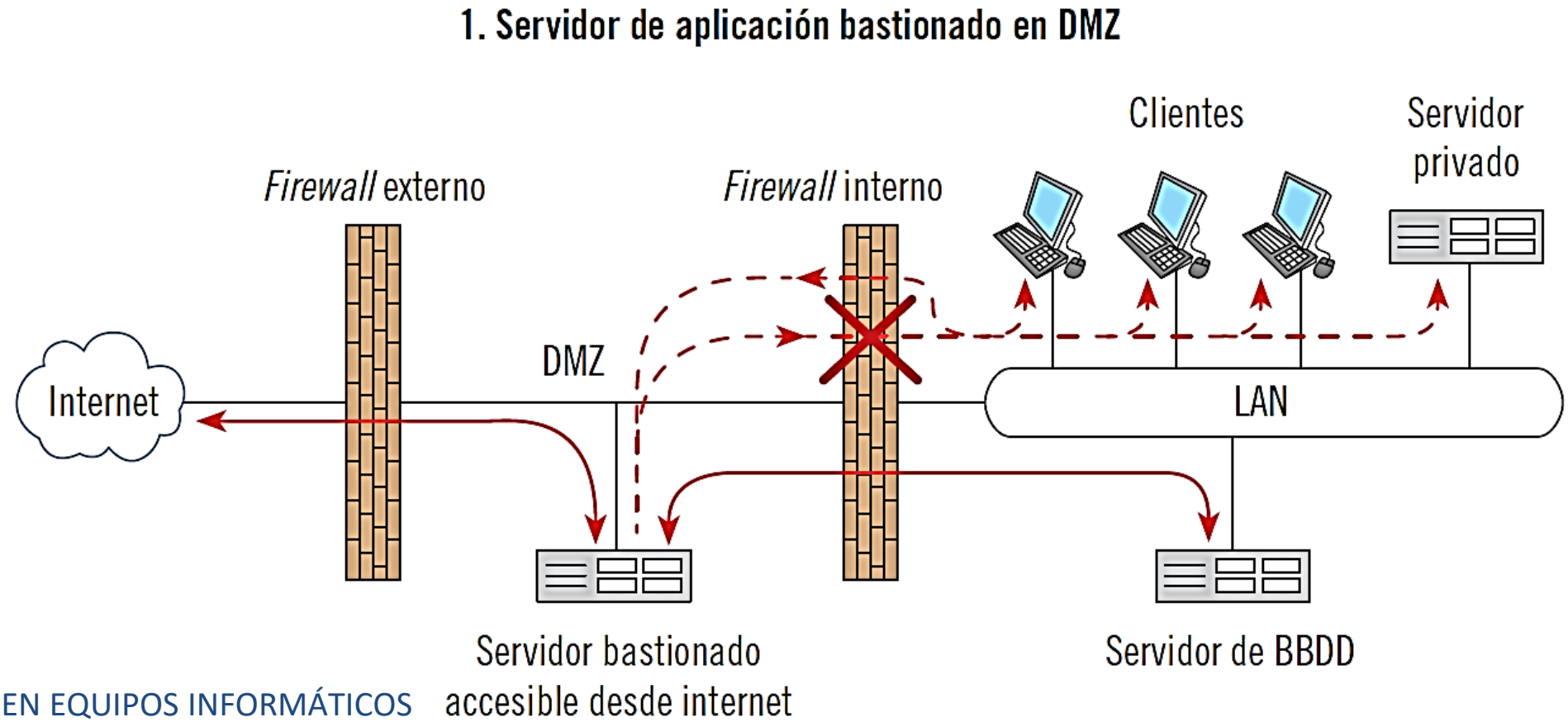
USO DE ZONAS DESMILITARIZADAS. UBICACIÓN DE SERVIDORES ACCESIBLES DESDE EL EXTERIOR

POR OTRO LADO, SI LOS USUARIOS DE LA RED PRIVADA NECESITAN ACCEDER A LA APLICACIÓN, EL FIREWALL INTERNO SE PUEDE CONFIGURAR SIN RIESGO PARA PERMITIR ESTE ACCESO.

POR ÚLTIMO, **SI EL SERVIDOR DE LA APLICACIÓN INSTALADA EN LA ZONA DMZ NECESITA ACCEDER A ALGÚN SERVIDOR DE LA RED PRIVADA, EL FIREWALL INTERNO SE DEBE CONFIGURAR PARA PERMITIR ESTE ACCESO CONCRETO**, DE FORMA QUE **SOLO EL SERVIDOR DE LA APLICACIÓN PUEDA ACCEDER** A LOS RECURSOS NECESARIOS DE LA RED PRIVADA.

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

USO DE ZONAS DESMILITARIZADAS. UBICACIÓN DE SERVIDORES ACCESIBLES DESDE EL EXTERIOR



3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

USO DE ZONAS DESMILITARIZADAS. UBICACIÓN DE SERVIDORES ACCESIBLES DESDE EL EXTERIOR

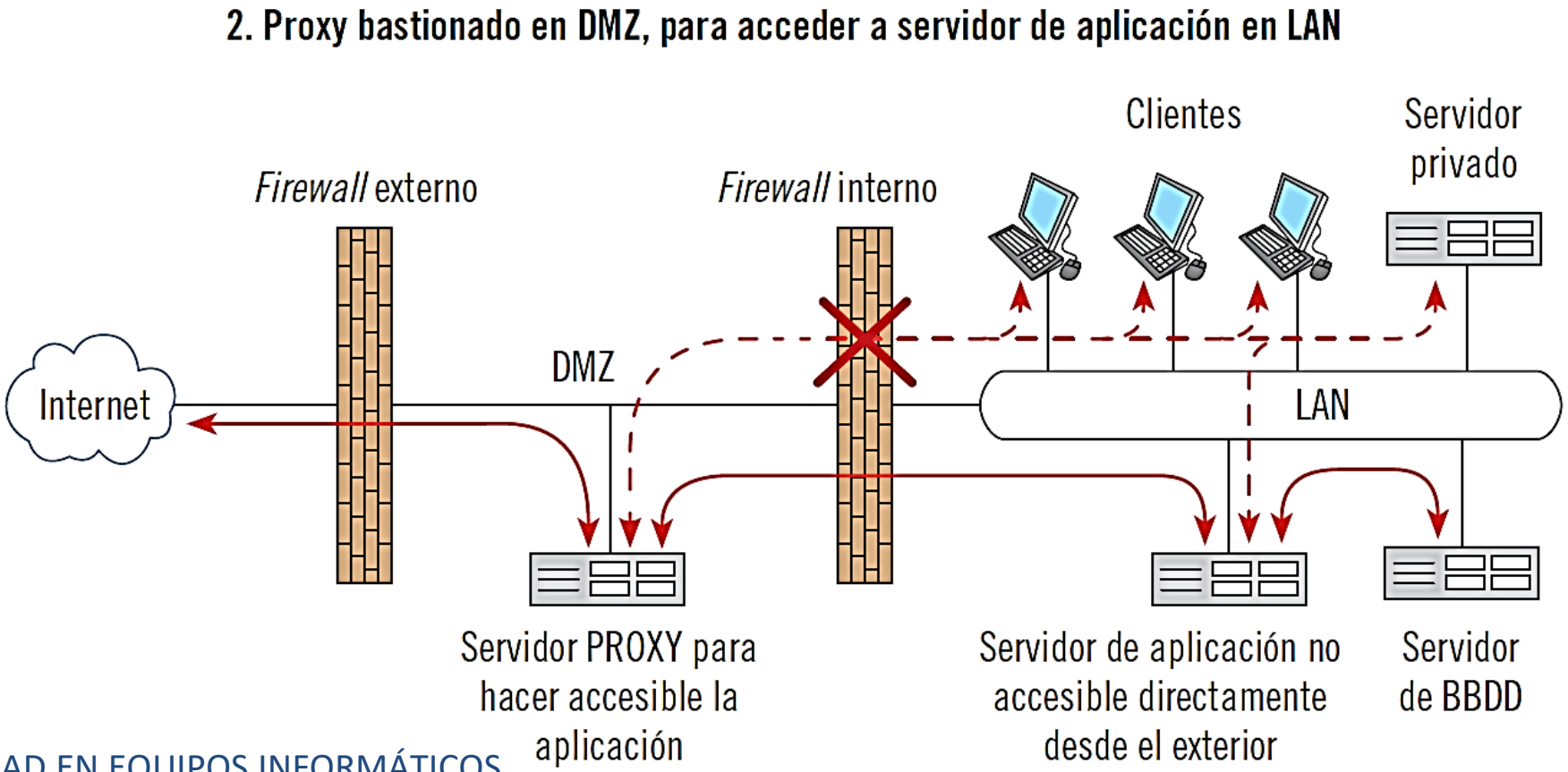
PERSISTE EL RIESGO DE QUE EL SERVIDOR DE LA APLICACIÓN SE VEA COMPROMETIDO; EN ESTE CASO PODRÁ ACCEDERSE DE MANERA INMEDIATA AL SERVIDOR DE LA RED PRIVADA AUTORIZADO.

SI SE REVISA EL DISEÑO EN EL QUE SE EMPLEAN SERVIDORES PROXY DE ACCESO, Y SE COMPARA CON LOS EJEMPLOS DE DISEÑO DE FIREWALL EN VARIAS ETAPAS, ES INMEDIATO OBSERVAR LA ANALOGÍA.

LOS BASTIONES HOST, DE UNA O DOS REDES, **SON LAS MÁQUINAS IDÓNEAS PARA EJECUTAR LAS APLICACIONES PROXY**, QUE DEN ACCESO DESDE INTERNET A LA APLICACIÓN

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ

USO DE ZONAS DESMILITARIZADAS. UBICACIÓN DE SERVIDORES ACCESIBLES DESDE EL EXTERIOR



CONTENIDOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ
4. **UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES**
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

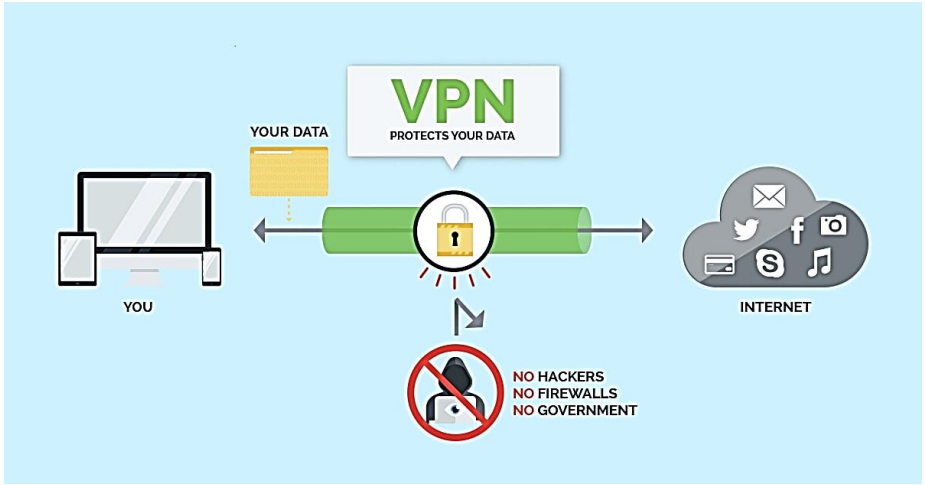
SI SE QUIERE QUE LAS **COMUNICACIONES ENTRE DOS SUCURSALES DISTINTAS** DE LA EMPRESA **SEAN SEGURAS**, SE PUEDEN EMPLEAR **DIVERSAS SOLUCIONES**:

- EMPLEAR **LÍNEAS DE COMUNICACIONES QUE SEAN PROPIEDAD DE LA EMPRESA**, ESPERANDO QUE NINGÚN AGENTE AJENO ACCEDA A ELLAS EN NINGÚN PUNTO DEL RECORRIDO. ESTO TIENE UN **COSTE MUY ELEVADO**, Y NORMALMENTE SOLO SERÁ VIABLE PARA **EMPRESAS MUY GRANDES**, O PARA **DISTANCIAS MUY PEQUEÑAS**.
- **ALQUILAR LAS LÍNEAS DE COMUNICACIONES** A SUS PROPIETARIOS (OPERADORES DE TELECOMUNICACIONES), DE MANERA QUE LAS COMUNICACIONES SE SIGAN CURSANDO POR UNA **LÍNEA DEDICADA**, CONFIANDO EN QUE NINGUNA OTRA EMPRESA NI PERSONA TENGA ACCESO.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CON LA POPULARIZACIÓN DE LOS ACCESOS DE BANDA ANCHA A INTERNET, **SE PLANTEA COMUNICAR DE MANERA SEGURA Y RÁPIDA DOS EXTREMOS, PERO A UN COSTE MUCHO MENOR.**

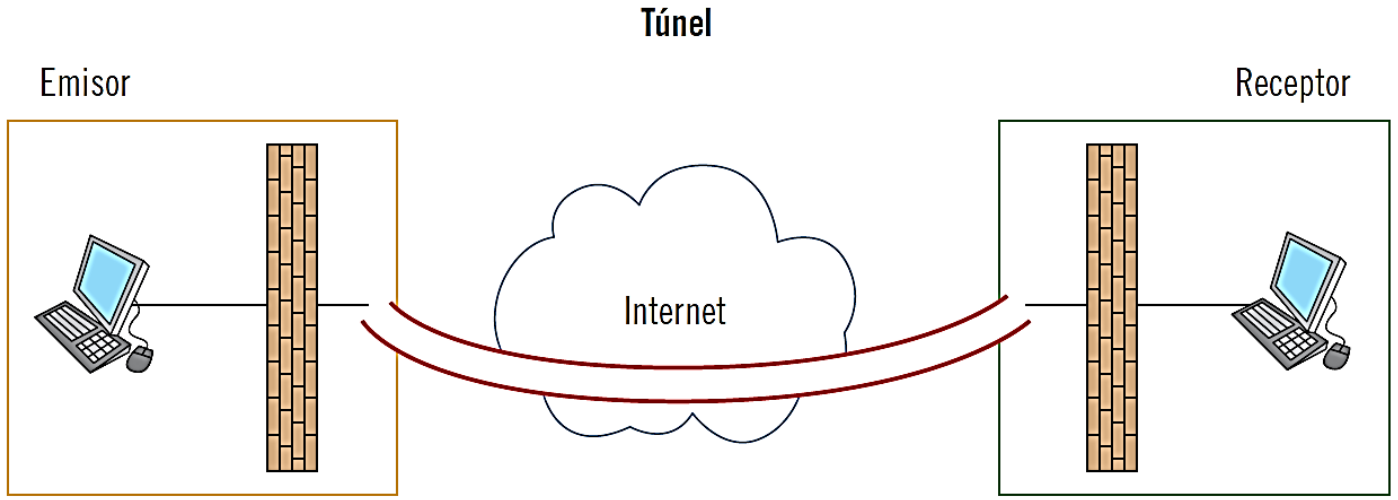
PARA ELLO, SE EMPLEAN TÉCNICAS QUE CONSTRUYEN **UNA RED PRIVADA VIRTUAL**. *ES UNA CONSTRUCCIÓN FICTICIA*, EN LA QUE EMISOR Y RECEPTOR DISPONEN DE UNA CONEXIÓN EXTREMO A EXTREMO, DEDICADA Y SEGURA.



4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

ES **UN TÚNEL QUE ATRAVIESA INTERNET**, POR EL QUE LAS COMUNICACIONES VIAJAN PROTEGIDAS DEL RESTO DE USUARIOS.

HABITUALMENTE, **ESTAS REDES PRIVADAS VIRTUALES SE CONSTRUYEN PARA OPERAR DE FORMA TRANSPARENTE**, DESDE EL CORTAFUEGOS **DE UN EXTREMO AL** CORTAFUEGOS DEL **OTRO EXTREMO**.



4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

ATAQUES DE INTERCEPTACIÓN Y ATAQUE DE MODIFICACIÓN

SE BUSCA **ASEGURAR LA CONFIDENCIALIDAD E INTEGRIDAD DE LAS COMUNICACIONES**.

LA CONTRAMEDIDA MÁS ADECUADA ES EL **EMPLEO DE TÉCNICAS DE CIFRADO O CRIPTOGRAFÍA**, QUE **JUNTO AL EMPLEO DE FIRMAS DIGITALES** PERMITEN CUMPLIR LOS REQUISITOS DE SEGURIDAD MENCIONADOS.

LAS **REDES PRIVADAS VIRTUALES** PERMITEN DISPONER DE CONEXIONES O CANALES DE COMUNICACIÓN SEGUROS, EMPLEANDO PARA ELLO MÉTODOS CRIPTOGRÁFICOS, QUE PERMITEN DEFENDER LAS COMUNICACIONES DE ATAQUES DE INTERCEPTACIÓN Y DE ATAQUES DE MODIFICACIÓN.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP

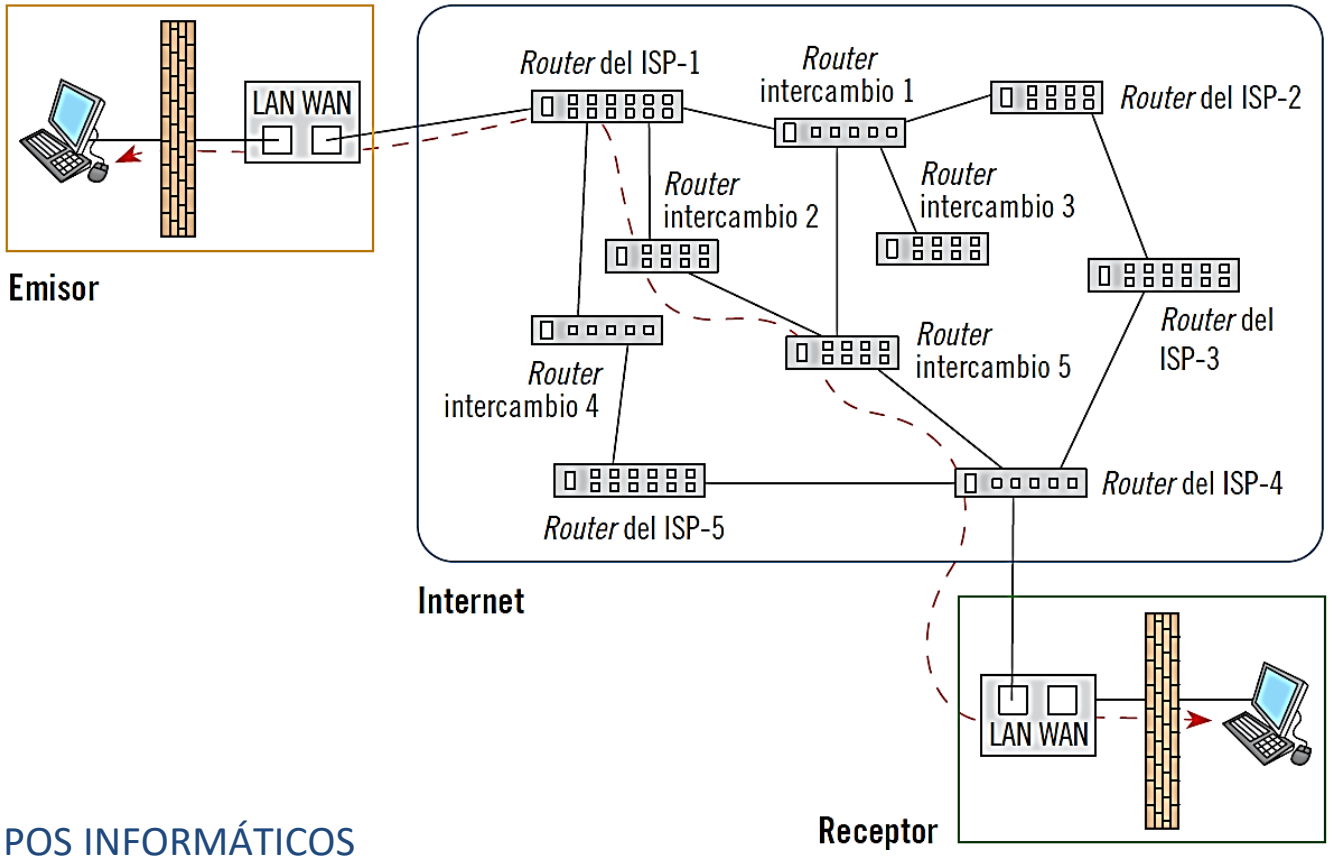
LAS COMUNICACIONES TCP/IP A TRAVÉS DE INTERNET PRECISAN DE UNA SERIE DE SALTOS ENTRE NODOS DE COMUNICACIONES, PARA ENCAMINAR LOS PAQUETES DESDE EL EMISOR HASTA EL RECEPTOR.

ESTOS NODOS INTERMEDIOS SON ENCAMINADORES O ROUTER, ES DECIR, ELEMENTOS DE LA CAPA DE RED QUE **NECESITAN SABER LA DIRECCIÓN IP DESTINO DE CADA PAQUETE**, PARA ENCAMINARLO Y QUE LOGRE ALCANZAR SU DESTINO.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP

Ruta seguida por una comunicación emisor–receptor en la que intervienen 6 router



4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP

CUANDO SE EMPLEAN **MÉTODOS CRIPTOGRÁFICOS PARA CIFRAR PAQUETES IP**, SOLO PUEDE HABER **DOS POSIBLES SITUACIONES**:

QUE LAS DIRECCIONES IP ESTÉN ENCRIPTADAS, O QUE NO LO ESTÉN

EN EL ÚLTIMO CASO, EL ROUTER NO TIENE DIFICULTAD PARA LEER LA DIRECCIÓN IP DESTINO, Y DECIDIR CÓMO ENCAMINARLO.

SIN EMBARGO, SI LA DIRECCIÓN IP ESTÁ ENCRIPTADA, EL ROUTER DEBE SER CAPAZ DE DESENCRIPTARLA, PARA SABER CÓMO ENCAMINAR EL PAQUETE, Y DEBE SER CAPAZ DE VOLVER A ENCRIPTARLO PARA ENVIARLO.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP

LO ANTERIOR ES DETERMINANTE PARA DIFERENCIAR:

SI **EL MECANISMO DE CIFRADO** QUE SE EMPLEA **ES DE EXTREMO A EXTREMO** (CUANDO LAS DIRECCIONES IP NO VIAJAN CIFRADAS Y POR LO TANTO LOS ROUTER INTERMEDIOS NO NECESITAN DESENCRIPTAR LOS PAQUETES)

SI EL MECANISMO DE CIFRADO ES NODO A NODO (CUANDO LAS DIRECCIONES IP VIAJAN ENCRIPTADAS, DE MANERA QUE CADA ROUTER DEBE DESENCRIPTAR LAS DIRECCIONES PARA RECUPERARLAS, Y LUEGO VOLVER A ENCRIPTARLAS).

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP

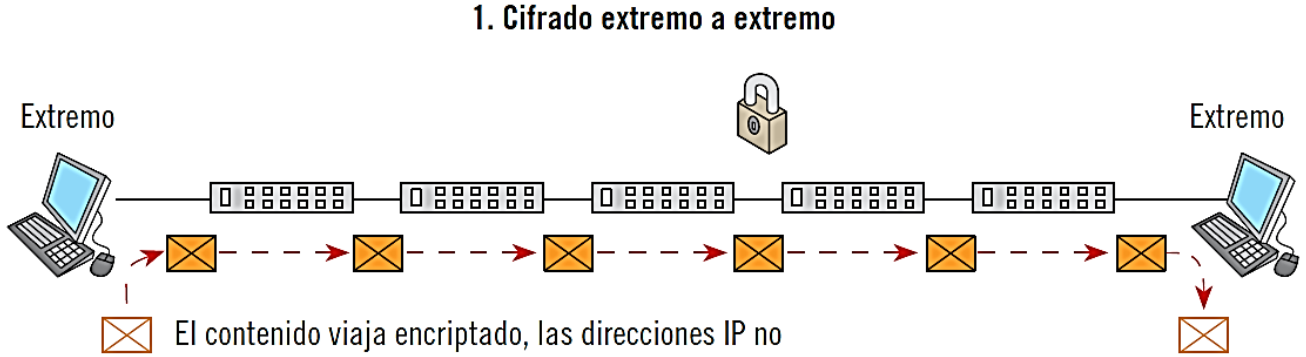
CUANDO EL MECANISMO DE **CIFRADO ES EXTREMO A EXTREMO**, LO ÚNICO QUE SE PROTEGE ES LA PARTE DE DATOS.

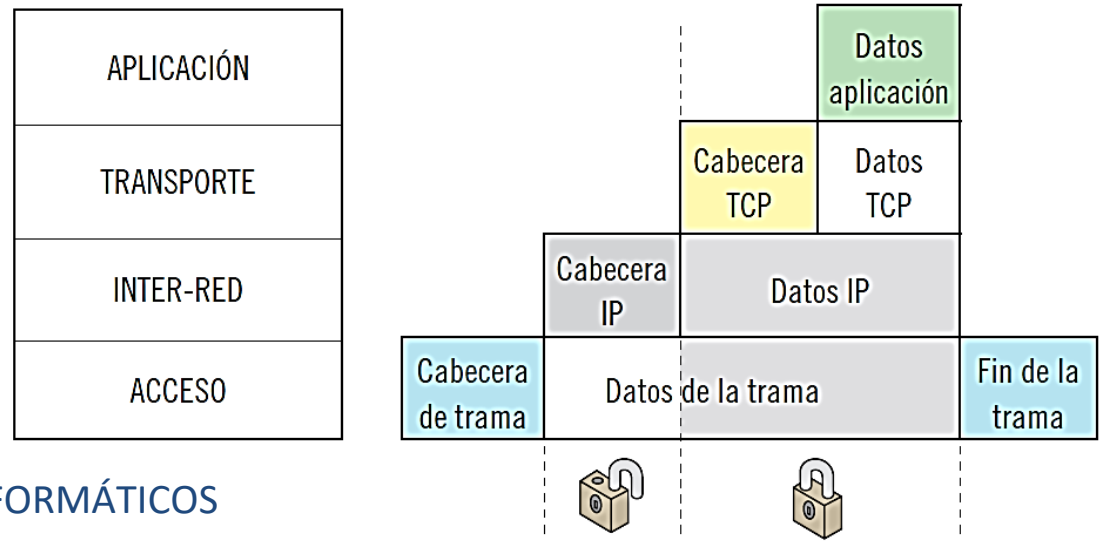
TODA LA INFORMACIÓN QUE, PROCEDENTE DE LOS NIVELES SUPERIORES (NIVEL DE TRANSPORTE Y NIVEL DE APLICACIÓN), SE HA IDO ENCAPSULANDO QUEDA PROTEGIDA.

POR EL CONTRARIO, NO SE PROTEGEN LAS DIRECCIONES DEL EMISOR Y DEL RECEPTOR, QUE SERÍAN ACCESIBLES PARA UN ATACANTE QUE TUVIERA ACCESO A LA RED.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP





4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP

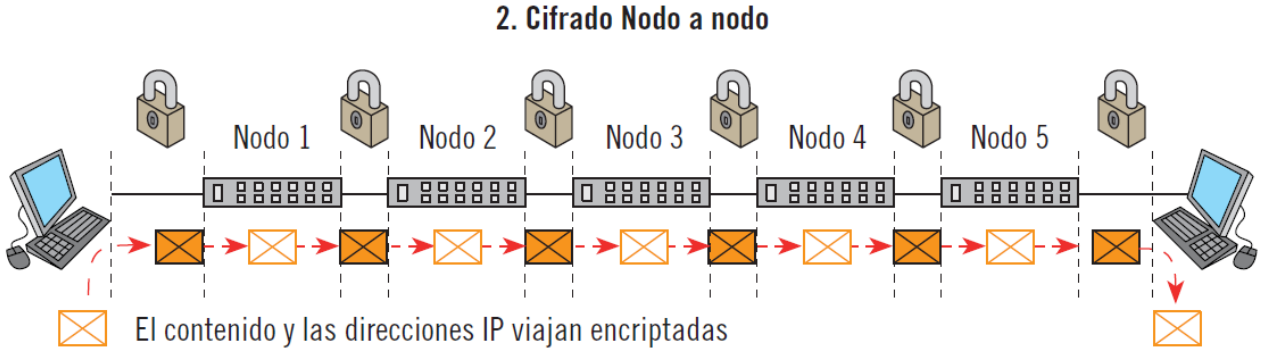
EN EL CASO DE **CIFRADO NODO A NODO SOLO ES POSIBLE SI TODOS LOS NODOS INTERMEDIOS DE LA RED SON CAPACES DE DESENCRIPTAR Y VOLVER A ENCRIPTAR LOS PAQUETES**.

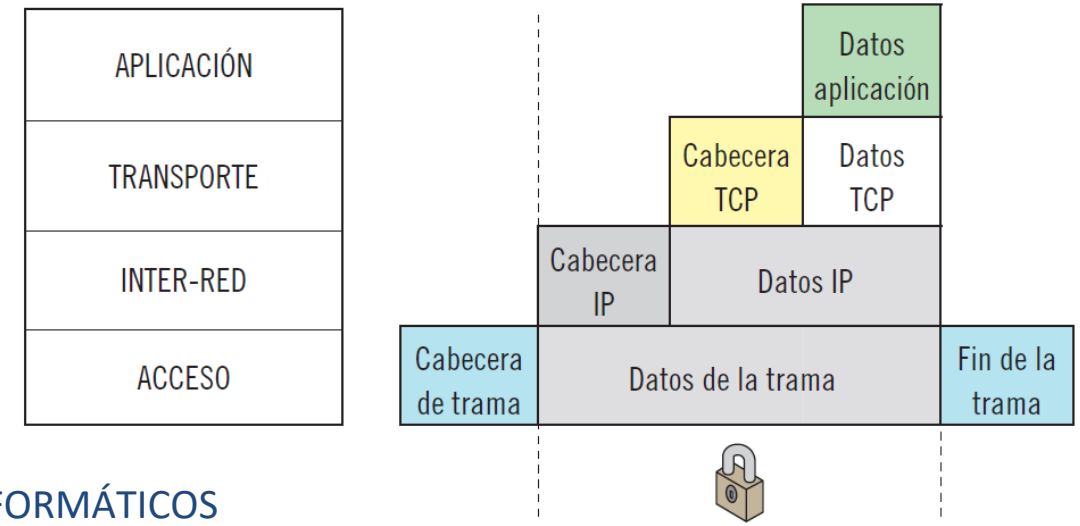
ESTO SIGNIFICA QUE TODOS LOS NODOS INTERMEDIOS DEBEN SOPORTAR UNA DETERMINADA TECNOLOGÍA DE RED VPN, LO QUE NO SIEMPRE PODRÁ ASEGURARSE, PORQUE LOS MÉTODOS DE VPN NO SON UNIVERSALES.

POR CONTRAPARTIDA, UN ATACANTE QUE OBSERVE EL TRÁFICO, NECESITARÁ DESENCRIPTARLO, INCLUSO PARA AVERIGUAR LAS DIRECCIONES DE LOS EXTREMOS.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP





4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

PROTOCOLOS VPN

LAS REDES PRIVADAS VIRTUALES (**VPN**) SURGEN PARA **PROPORCIONAR UNA CONEXIÓN SEGURA A TRAVÉS DE REDES PÚBLICAS NO SEGURAS**, AUNANDO EL USO DE CRIPTOGRAFÍA, MECANISMOS DE AUTENTICACIÓN, Y LA ENCAPSULACIÓN DE PROTOCOLOS.

EL RESULTADO FINAL ES QUE **SE LOGRA EXTENDER LA RED PRIVADA SOBRE UNA RED PÚBLICA** SIN PROBLEMAS DE SEGURIDAD, DE MANERA QUE UN USUARIO QUE EMPLEE VPN PARA CONECTARSE A LA RED PRIVADA DE SU EMPRESA LOGRA OPERAR A TODOS LOS EFECTOS, COMO SI SU ESTACIÓN DE TRABAJO ESTUVIERA EN LA RED PRIVADA DE LA EMPRESA.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

PROTOCOLOS VPN

LOS ELEMENTOS QUE INTERVIENEN SON: **UN CLIENTE VPN Y UN SERVIDOR VPN**, Y AMBOS DEBEN EMPLEAR EL MISMO PROTOCOLO VPN. EXISTEN MUCHOS CRITERIOS PARA **CLASIFICAR LAS VPN**; UNO DE LOS MÁS SENCILLOS ES CLASIFICARLAS EN DOS TIPOS, **SEGÚN EL USO QUE SE REALIZARÁ DE LA CONEXIÓN SEGURA**:

- **VPN SITIO A SITIO**
- **VPN DE ACCESO REMOTO**

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

PROTOCOLOS VPN

VPN SITIO A SITIO

PARA **CONECTAR DIFERENTES OFICINAS DE UNA MISMA EMPRESA**, QUE PRECISEN INTERCAMBIAR DATOS CONFIDENCIALES, EVITANDO EL ALQUILER DE CIRCUITOS DEDICADOS, CONSIDERABLEMENTE MÁS COSTOSOS (PERO CON OTRAS VENTAJAS)

VPN DE ACCESO REMOTO

PARA **PERMITIR EL TELETRABAJO SIN COMPROMETER LA SEGURIDAD**. ES POSIBLE TENER ACCESO DE UN ORDENADOR A UNA RED, O BIEN ACCESO DE ORDENADOR A ORDENADOR. EN AMBOS CASOS, EXISTE UN CLIENTE Y UN SERVIDOR, Y LA VPN PUEDE SER INICIADA POR EL CLIENTE (ESTACIÓN REMOTA EXTERNA A LA LAN), O POR EL SERVIDOR DE LA RED PRIVADA.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

PROTOCOLOS VPN

LA PRINCIPAL **DESVENTAJA** DEL EMPLEO DE VPN ES LA **PÉRDIDA DE RENDIMIENTO**, DERIVADA DEL COSTE DEL CIFRADO CRIPTOGRÁFICO, Y DERIVADA DEL COSTE DE LA ENCAPSULACIÓN QUE SE EMPLEA (UN PROTOCOLO SE ENVÍA COMO SI FUERAN DATOS DE OTRO PROTOCOLO).

ADEMÁS, COMO TODAS LAS CONTRAMEDIDAS, **SE INTRODUCEN NUEVAS VULNERABILIDADES**. POR EJEMPLO, EN UNA VPN DE ACCESO REMOTO, PARA UN TELETRABAJADOR QUE ACCEDE DESDE SU DOMICILIO, SE TRASLADA A UNA UBICACIÓN SIN MEDIDAS DE CONTROL NI SEGURIDAD FÍSICA UN EQUIPO QUE TENDRÁ ACCESO LÓGICO A LA RED PRIVADA DE LA EMPRESA.

4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES

PROTOCOLOS VPN

PARA CONSTITUIR UNA RED PRIVADA VIRTUAL, AMBOS EXTREMOS **DEBEN EMPLEAR EL MISMO PROTOCOLO VPN**.

EXISTEN VARIOS PROTOCOLOS VPN ACEPTADOS Y ESTANDARIZADOS, ADEMÁS DE SOLUCIONES COMERCIALES QUE FACILITAN LA CONFIGURACIÓN Y PUESTA EN MARCHA DE ESTA TECNOLOGÍA.

LOS PROTOCOLOS QUE SE INTRODUCEN SON LOS MÁS BÁSICOS, Y FUNCIONAN EN LAS CAPAS 2 Y 3 DEL MODELO DE RED OSI.

- **PPTP (POINT TO POINT TUNNELING PROTOCOL)**
- **L2TP (LAYER 2 TUNNELING PROTOCOL)**
- **IPSEC (IP SECURITY)**

CONTENIDOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. **DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS**
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

LAS REGLAS DE CORTE SE DEBEN DEFINIR **PARTIENDO DE LA SITUACIÓN DE TODO PROHIBIDO**, PARA A CONTINUACIÓN HABILITAR EXCLUSIVAMENTE LOS FLUJOS DE TRÁFICO PERMITIDOS. ESTE DISEÑO ES EL HABITUAL, DONDE SE PRECISA UN CONTROL DE ACCESO LÓGICO ADECUADO.

LAS REGLAS DE FILTRADO DE UN FIREWALL PRESENTAN LA PECULIARIDAD DE PODER ESTABLECERSE DE MANERA INDEPENDIENTE, SEGÚN EL SENTIDO DEL TRÁFICO, Y EXISTEN:

- **REGLAS DE TRÁFICO ENTRANTE (INCOMING)** PARA FILTRAR EL TRÁFICO QUE PROCEDE DE INTERNET Y VA DESTINADO A LA RED PRIVADA.
- **REGLAS DE TRÁFICO SALIENTE (OUTCOMING)** PARA FILTRAR EL TRÁFICO QUE PROCEDE DE LA RED PRIVADA Y VA DESTINADO A INTERNET.

5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

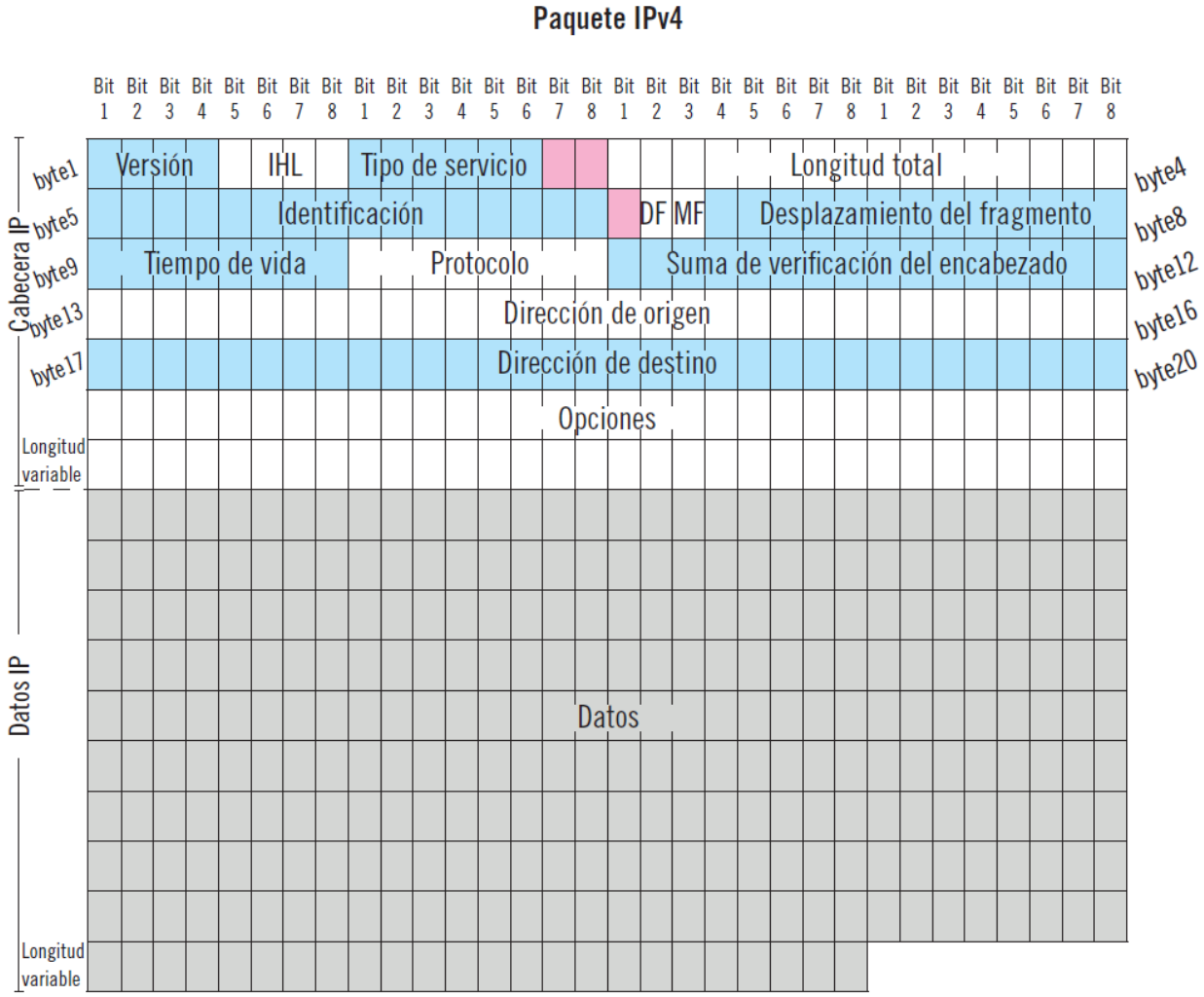
EL FIREWALL DISPONDRÁ AL MENOS DE DOS INTERFACES DE RED, UNO PARA LA CONEXIÓN A INTERNET O RED WAN, Y OTRO PARA LA CONEXIÓN A LA RED PRIVADA O RED LAN.

POR LO TANTO, CUANDO EL FIREWALL RECIBE UN PAQUETE IP POR EL INTERFAZ WAN QUE VA DIRIGIDO A LA INTERFAZ LAN, LE APLICA EL **CONJUNTO DE REGLAS DE TRÁFICO ENTRANTE (INCOMING).**

POR OTRO LADO, CUANDO EL FIREWALL RECIBE UN PAQUETE IP EN EL INTERFAZ LAN DIRIGIDO A LA RED WAN, LE APLICA EL **CONJUNTO DE REGLAS DE TRÁFICO SALIENTE (OUTCOMING).**

5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

EL FIREWALL CONOCE ORIGEN Y DESTINO DEL PAQUETE IP, CON SOLO OBSERVAR LAS DIRECCIONES DEL MISMO, QUE **OCUPAN LOS BYTES 13-16 Y 17-20 DE CADA PAQUETE IP.**



5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

LAS REGLAS PUEDEN ESPECIFICAR MULTITUD DE CONDICIONES, QUE DEPENDERÁN DE CADA CORTAFUEGOS CONCRETO, PERO SIEMPRE **HAN DE CONTENER AL MENOS LAS SIGUIENTES CINCO INFORMACIONES**:

- **PROTOCOLO DE TRANSPORTE: TCP O UDP.**
- **PUERTO DE COMUNICACIONES: SIRVE PARA IDENTIFICAR LA APLICACIÓN.**
- **DIRECCIÓN IP ORIGEN: QUIÉN ORIGINA EL PAQUETE.**
- **DIRECCIÓN IP DESTINO: A QUIÉN VA DESTINADO EL PAQUETE.**
- **ACCIÓN: PERMITIDO O PROHIBIDO.**

DE ESTA MANERA, RESULTA INMEDIATO DEFINIR REGLAS PARA PERMITIR EL ACCESO DESDE UN CLIENTE EXTERNO A UN SERVIDOR WEB INTERNO, O REGLAS PARA PERMITIR QUE UN SERVIDOR DE CORREO PRIVADO PUEDA ENVIAR CORREO AL EXTERIOR.

5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

EJEMPLOS:

REGLAS ENTRANTES PARA PERMITIR EXCLUSIVAMENTE EL ACCESO A UN SERVIDOR WEB INTERNO, CUYA DIRECCIÓN IP PÚBLICA ACCESIBLE ES 84.122.10.15

Protocolo	Puerto	IP Origen	IP Destino	Acción
TCP, UDP	*	*	*	prohibir
TCP	80	*	84.122.10.15	permitir

5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

EJEMPLOS:

REGLAS SALIENTES PARA PERMITIR EXCLUSIVAMENTE QUE UN SERVIDOR DE CORREO CON DIRECCIÓN IP 192.168.10.23 PUEDA ENVIAR CORREO AL EXTERIOR

Protocolo	Puerto	IP Origen	IP Destino	Acción
TCP, UDP	*	*	*	prohibir
TCP	25	192.168.10.23	*	permitir

5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

SI EL CORTAFUEGOS DISPONE DE MÁS DE DOS ADAPTADORES DE RED, QUE PERMITAN **GESTIONAR DIFERENTES SUBREDES**, SE PODRÁN **DEFINIR REGLAS DE ACCESO ENTRE ELLAS**, CON SOLO EMPLEAR LAS DIRECCIONES ORIGEN Y DESTINO ADECUADAS, QUE DEBEN SER DEL RANGO DE DIRECCIONES AL QUE PERTENECE EL INTERFAZ DE RED.

UN ÚLTIMO COMENTARIO SE REFIERE A LAS **POSIBLES ACCIONES PARA PROHIBIR EL TRÁFICO**, Y QUE, DEPENDIENDO DEL FIREWALL, PODRÍA ADMITIR DOS OPCIONES. ASÍ, AL RECHAZAR UN PAQUETE, **SE PUEDE INFORMAR AL REMITENTE** DE ELLO, **O** PARA RECHAZARLO, **SIMPLEMENTE PUEDE NO RESPONDERSE**.

DESDE EL PUNTO DE VISTA DE LA SEGURIDAD, ESTA DISTINCIÓN ES RELEVANTE

CONTENIDOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD**
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD

SE DEBERÍAN **MANTENER REGISTROS DE**:

- **LAS FECHAS Y HORAS DE LOS EVENTOS** CLAVE, COMO INICIO Y FIN DE CONEXIONES DE ENTRADA.
- **LA IDENTIDAD DE QUIÉN REALIZA LA CONEXIÓN** CUANDO SEA POSIBLE; POR EJEMPLO, SI LA CONEXIÓN ES AL PROPIO CORTAFUEGOS, PARA MODIFICAR SU CONFIGURACIÓN, DEBE CONSERVARSE EL REGISTRO DEL USUARIO.
- **LAS ALARMAS ACTIVADAS DEL SISTEMA DE CONTROL DE ACCESO** AL CORTAFUEGOS.
- LOS CAMBIOS EN LA CONFIGURACIÓN DEL CORTAFUEGOS.
- **LA ACTIVACIÓN O DESACTIVACIÓN DE FUNCIONALIDADES DE SEGURIDAD** DEL CORTAFUEGOS, COMO SISTEMAS ANTIVIRUS QUE INCORPORE, O LAS FUNCIONALIDADES DE DETECCIÓN Y/O PREVENCIÓN DE INTRUSIONES.

6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD

SE DEBERÍAN **MANTENER REGISTROS DE**:

- **REGISTROS DE LOS INTENTOS DE COMUNICACIONES RECHAZADAS**, POR EJEMPLO, REGISTRAR LAS DIRECCIONES IP QUE PERSISTENTEMENTE INICIAN COMUNICACIONES, PARA LAS QUE LAS REGLAS DE ACCESO TIENEN MARCADA UNA ACCIÓN DE “PROHIBIR”, DE LOS PROTOCOLOS (PUERTOS) EMPLEADOS.
- **LAS DIRECCIONES DE RED DE LAS CONEXIONES ESTABLECIDAS Y RECHAZADAS**, Y DE LOS PROTOCOLOS (PUERTOS) EMPLEADOS.
- **LAS ACTIVIDADES DE LOS USUARIOS CON PRIVILEGIOS**, COMO EL ADMINISTRADOR O EL PERSONAL QUE OPERE EL CORTAFUEGOS, DEBEN REGISTRARSE ESPECIALMENTE, Y REVISARSE DE MANERA REGULAR
- **LOS FALLOS DEL EQUIPO SE DEBEN REGISTRAR Y ANALIZAR ESPECIALMENTE**, Y POR SUPUESTO, ASEGURAR QUE SE CORRIGEN LOS PROBLEMAS.

6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD

DEBE **PRESTARSE ESPECIAL ATENCIÓN A LOS REGISTROS DEL FIREWALL RELACIONADOS CON EL ACCESO A INFORMACIÓN CONFIDENCIAL**.

LOS **ADMINISTRADORES DEL FIREWALL NO DEBEN TENER CAPACIDAD PARA BORRAR O DESACTIVAR EL REGISTRO DEL EQUIPO**.

SE DEBE **CONTROLAR LAS ALTERACIONES QUE SE DETECTEN A LOS FICHEROS DE LOS REGISTROS**, Y TAMBIÉN SE DEBE **CONTROLAR LA CAPACIDAD DE ALMACENAMIENTO DISPONIBLE DEL SISTEMA DE FICHEROS**. TAMBIÉN PUEDE SER DE INTERÉS EL EMPLEO DE HERRAMIENTAS DE FILTRADO, QUE AYUDEN A SELECCIONAR LOS REGISTROS DE INTERÉS QUE SE ANALIZARÁN DETENIDAMENTE, Y SE CONSERVARÁN COPIADOS APARTE.

CONTENIDOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. **ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS**

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

LA REVISIÓN MEDIANTE **MONITORIZACIÓN, VERIFICACIÓN Y PRUEBAS DEL SISTEMA DE PROTECCIÓN DE LA RED** FRENTE A LAS AMENAZAS PROCEDENTES DE INTERNET ES UNA TAREA PRINCIPAL DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN.

DE OTRA MANERA, SE PRODUCIRÁ UNA SENSACIÓN DE SEGURIDAD FALSA, QUE PODRÍA LLEGAR A SER MUY PERJUDICIAL.

UN CORTAFUEGOS ES UN ELEMENTO CRÍTICO PARA LA EMPRESA, Y **DEBE EXISTIR UN PROCEDIMIENTO FORMAL DE REVISIÓN REGULAR**, QUE PODRÍA LLEGAR A SER CONTINUA, DEPENDIENDO DE LOS RIESGOS QUE MITIGUE ESTA CONTRAMEDIDA.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

LA NORMA **ISO 17799:2005** ESTABLECE LAS SIGUIENTES **RECOMENDACIONES:**

- DEBE EXISTIR UN PROCEDIMIENTO FORMAL DE MONITORIZACIÓN DEL CORTAFUEGOS, ASÍ COMO DE REVISIÓN REGULAR DE LOS RESULTADOS DE DICHA MONITORIZACIÓN; AMBAS TAREAS SON VITALES.
- LOS RECURSOS QUE SE DEDIQUEN A LA MONITORIZACIÓN, GENERALMENTE TRADUCIDOS EN LA FRECUENCIA Y EXHAUSTIVIDAD DE LA REVISIÓN, SE DEBEN ASIGNAR TRAS UNA EVALUACIÓN DEL RIESGO, PERO SIEMPRE SE DEBEN CUMPLIR LOS REQUISITOS QUE PUEDAN VENIR DERIVADOS DEL CUMPLIMIENTO DE LA LEGISLACIÓN QUE PUDIERA APLICAR. ENTRE LOS FACTORES DE RIESGO A CONSIDERAR, DESTACARÍAN:
- LA CRITICIDAD DE LOS PROCESOS DE LAS APLICACIONES PROTEGIDAS/FILTRADAS POR EL FIREWALL
  - EL VALOR DE LA INFORMACIÓN INVOLUCRADA
  - LOS ANTECEDENTES DE ATAQUES O INTRUSIONES Y LA FRECUENCIA DE ESTOS
  - LAS REDES QUE ESTÁN INTERCONECTADAS, ESPECIALMENTE SI SON PÚBLICAS
  - LA CONFIGURACIÓN DE LOS REGISTROS.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

RECOMENDACIONES:

- SE DEBEN MONITORIZAR LOS ACCESOS AUTORIZADOS (QUIÉN Y CUÁNDO ACCEDE, A QUÉ SE ACCEDE, Y PARA QUÉ SE ACCEDE).
- SE DEBEN MONITORIZAR ESPECIALMENTE LAS OPERACIONES QUE REQUIERAN DEL USO DE PRIVILEGIOS (COMO EL INICIO Y APAGADO, O LA CARGA DE PLANTILLAS DE CONFIGURACIÓN).
- SE DEBEN MONITORIZAR LOS ACCESOS NO AUTORIZADOS, COMO: LAS COMUNICACIONES RECHAZADAS EN BASE A LAS REGLAS DE FILTRADO EXISTENTES, LOS INTENTOS DE ACCESO INTERNOS, LOS ACCESOS EXTERNOS RECHAZADOS, LAS COMUNICACIONES RECHAZADAS SEGÚN CONDICIONES EXPRESAMENTE ESPECIFICADAS EN LA POLÍTICA DE SEGURIDAD (HORARIOS, DESTINOS EXPRESAMENTE PROHIBIDOS, ETC.), O LAS ALARMAS QUE PUEDA INICIAR EL SUBSISTEMA DE DETECCIÓN DE INTRUSIONES.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

RECOMENDACIONES:

- SE DEBEN MONITORIZAR LAS ALARMAS O FALLOS DEL EQUIPO, COMO: ALERTAS O MENSAJES EN EL VISOR DE SUCESOS O CONSOLA DE CONTROL, EXCEPCIONES, ALARMAS DE GESTIÓN, ALARMAS POR CONTROL DE ACCESOS U OTRAS SEGÚN TERMINOLOGÍA, Y CATEGORIZACIÓN CONCRETA DEL FIREWALL QUE SE EMPLEE.
- SE DEBEN MONITORIZAR LOS CAMBIOS DE CONFIGURACIÓN (O LOS INTENTOS).

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

ADEMÁS DEL MONITOREO EN TIEMPO REAL, **SE DEBERÍAN EMPLEAR LAS HERRAMIENTAS DE ANÁLISIS DE RED Y ESCANEO DE PUERTOS.**

SI BIEN PUEDEN EXISTIR GARANTÍAS DEL CORRECTO FUNCIONAMIENTO DEL EQUIPO, SOLO LA EVIDENCIA DE UNA PRUEBA PERMITE ASEGURAR QUE ES ASÍ.

ADEMÁS, SON ESTAS PRECISAMENTE LAS HERRAMIENTAS BÁSICAS QUE UN POTENCIAL INFRACTOR EMPLEARÁ, DE MANERA QUE RESULTA NATURAL ANTICIPAR ESOS DESCUBRIMIENTOS PARA ADOPTAR LAS MEDIDAS NECESARIAS.

CONTENIDOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

RESUMEN

INTERNET ES LA PRINCIPAL FUENTE DE AMENAZAS PARA LA RED DE LA EMPRESA, Y A LA VEZ, RESULTA IMPRESCINDIBLE.

POR TANTO, SE DEBE REDUCIR EN LO POSIBLE ESTA VULNERABILIDAD, PRIMERO, MANTENIENDO CONTROLADOS Y DEFINIDOS LOS PUNTOS DE INTERCONEXIÓN Y, EN SEGUNDO LUGAR, EMPLEANDO EN DICHOS PUNTOS PASARELAS DE SEGURIDAD GENERALMENTE CONOCIDAS COMO **CORTAFUEGOS O FIREWALLS**.

POR SU FUNCIONAMIENTO, SON HABITUALES EL EMPLEO DE **FIREWALLS DE FILTRADO DE PAQUETES** (DE MANERA ESTÁTICA O DE MANERA DINÁMICA), O BIEN **FIREWALLS DE APLICACIÓN**, FORMADOS POR SERVIDORES PROXY QUE INTERRUMPEN LA COMUNICACIÓN ENTRE CLIENTES Y SERVIDORES A MODO DE BUFFER, O APLICACIÓN INTERMEDIA.

RESUMEN

POR SU CONSTRUCCIÓN, SE PUEDEN ENCONTRAR DISEÑOS QUE VAN DESDE UN SENCILLO ROUTER PROPORCIONADO POR EL ISP, HASTA SUBREDES FILTRADAS QUE PERMITEN LA EXISTENCIA DE ZONAS INTERMEDIAS (**ZONAS DESMILITARIZADA, DMZ**), DONDE GENERALMENTE SE DEBEN UBICAR LOS SERVIDORES QUE TENGAN QUE SER ACCEDIDOS DESDE EL EXTERIOR, O SUS REEMPLAZOS (ES DECIR **SERVIDORES PROXY** PARA EL ACCESO EXTERNO); SIN OLVIDAR LOS **FIREWALLS PERSONALES**, QUE SE UBICAN EN CADA CLIENTE DE LA RED PRIVADA.

EL EMPLEO DE FIREWALLS PROTEGE EL PERÍMETRO, CONTROLANDO EL ACCESO A LA RED PRIVADA DESDE INTERNET, Y VICEVERSA.

PESE A ELLO, PERSISTE EL PROBLEMA DEL ACCESO A LA INFORMACIÓN, CUANDO ESTA CIRCULA LIBREMENTE POR INTERNET, O CUANDO CIRCULA POR LA RED PRIVADA, SI EL ATAQUE PROCEDE DE LA PROPIA RED PRIVADA.

RESUMEN

PARA ELLO, SE EMPLEAN **REDES PRIVADAS VIRTUALES**, QUE CONSTITUYEN CONEXIONES (**TÚNELES**) SEGUROS ENTRE EMISOR Y RECEPTOR, GRACIAS AL EMPLEO DE AUTENTICACIÓN Y ENCRIPTACIÓN.

ENTRE LOS PROTOCOLOS VPN MÁS USADOS, DESTACAN **PPTP** Y **L2TP**, FUNCIONANDO EN CAPA 2, E **IPSEC**, FUNCIONANDO EN CAPA 3.

EL USO CONJUNTO DE FIREWALLS Y VPN, PARA SEPARAR LA LAN DE INTERNET O PARA SEPARAR SUBREDES LAN O DOMINIOS LÓGICOS DE SEGURIDAD INTERNOS, COMPLETAN LAS SALVAGUARDAS QUE PERMITEN CERRAR PERFECTAMENTE LA INFRAESTRUCTURA (FÍSICA Y LÓGICA) EN TORNO A LOS ACTIVOS CONTENIDOS.

COMO OTRAS CONTRAMEDIDAS, SE DEBE MONITORIZAR SU EFICACIA Y RENDIMIENTO MEDIANTE REGISTROS DE AUDITORÍA Y VERIFICACIONES REGULARES DE SU BUEN FUNCIONAMIENTO, DESCONFIANDO DEL COMPORTAMIENTO CONOCIDO.

ESTO ES TODO