IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

UD05

DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. **INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS**
2. COMPONENTES DE UN CORTAFUEGOS DE RED
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
4. ARQUITECTURAS DE CORTAFUEGOS DE RED
5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

UNO DE LOS **ASPECTOS FUNDAMENTALES** DE LAS AUDITORÍAS DE LOS SISTEMAS DE INFORMACIÓN ES LA **EVALUACIÓN DE SU NIVEL DE SEGURIDAD.**

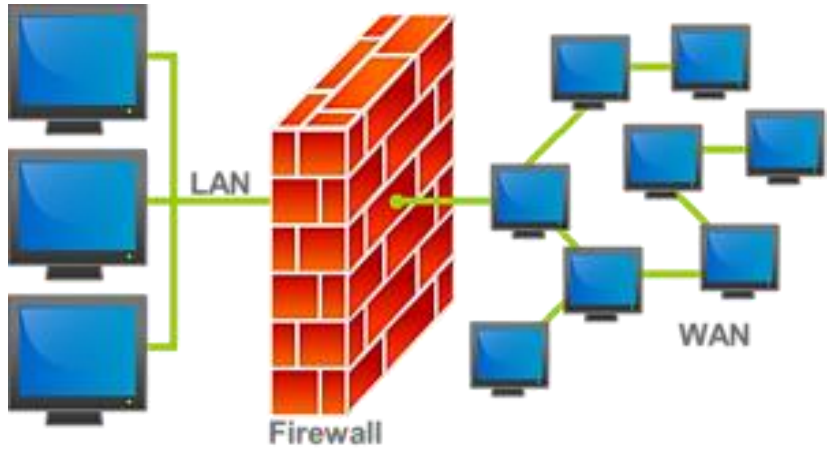
ESTE GRADO DE SEGURIDAD NO SOLO DEBE SER A NIVEL DE LAS VULNERABILIDADES DE LAS APLICACIONES INSTALADAS EN LOS EQUIPOS, SINO QUE **DEBE CONTENER UNA SERIE DE MEDIDAS QUE INTENTEN BLOQUEAR LA ENTRADA DE ATAQUES** QUE PUEDAN AFECTAR A LA INFORMACIÓN.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

DEBE IMPLANTARSE UN **SISTEMA DE PROTECCIÓN QUE DETECTE LOS POSIBLES ATACANTES Y QUE EVITE Y PREVENGA SU ENTRADA.**

UNA DE LAS MEDIDAS MÁS EFICIENTES Y UTILIZADAS ES LA IMPLANTACIÓN DE **CORTAFUEGOS DE RED**.

EN ESTE CAPÍTULO, SE DESCRIBEN LOS DISTINTOS **TIPOS DE CORTAFUEGOS** JUNTO CON SUS **COMPONENTES, UTILIDADES Y ARQUITECTURAS** PRINCIPALES.



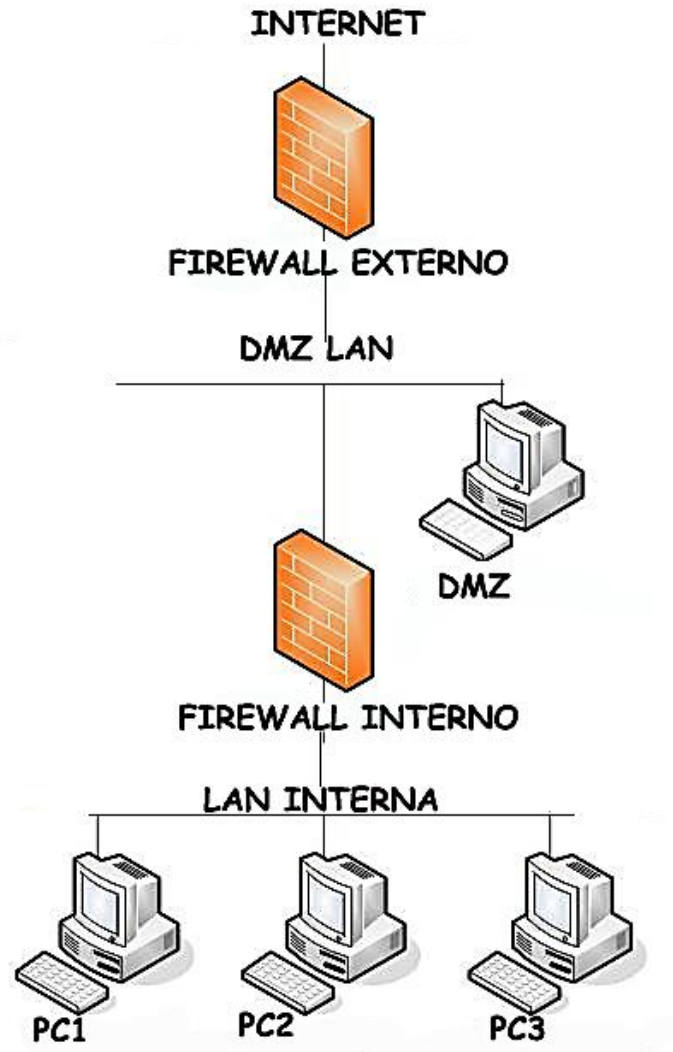
1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS

LOS SISTEMAS DE INFORMACIÓN HAN PASADO DE SER UTILIZADOS EN REDES LOCALES A PODER TRANSMITIR CUALQUIER TIPO DE INFORMACIÓN A TRAVÉS DE INTERNET.

ESTO HA HECHO QUE HAYAN AUMENTADO LAS AMENAZAS QUE PUEDEN AFECTAR A LOS SISTEMAS.

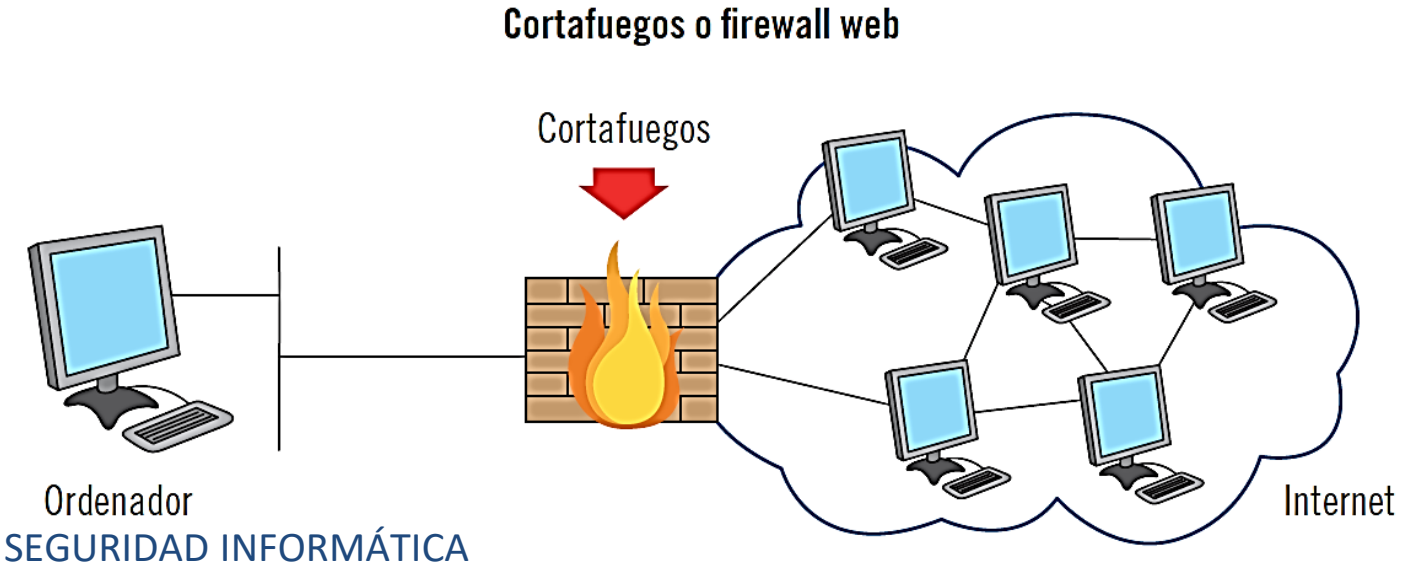
POR ESTE MOTIVO, SE DISEÑARON **LOS CORTAFUEGOS O FIREWALLS.**



1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS

UN **CORTAFUEGOS O FIREWALL** ES UN SISTEMA COMPUESTO POR **UNO O VARIOS DISPOSITIVOS CUYA FUNCIÓN PRINCIPAL ES LA SEPARACIÓN ENTRE LA RED LOCAL DE UN SISTEMA DE INFORMACIÓN Y LA RED EXTERIOR** PARA IMPEDIR LA ENTRADA DE ATAQUES Y AUMENTAR EL NIVEL DE SEGURIDAD.

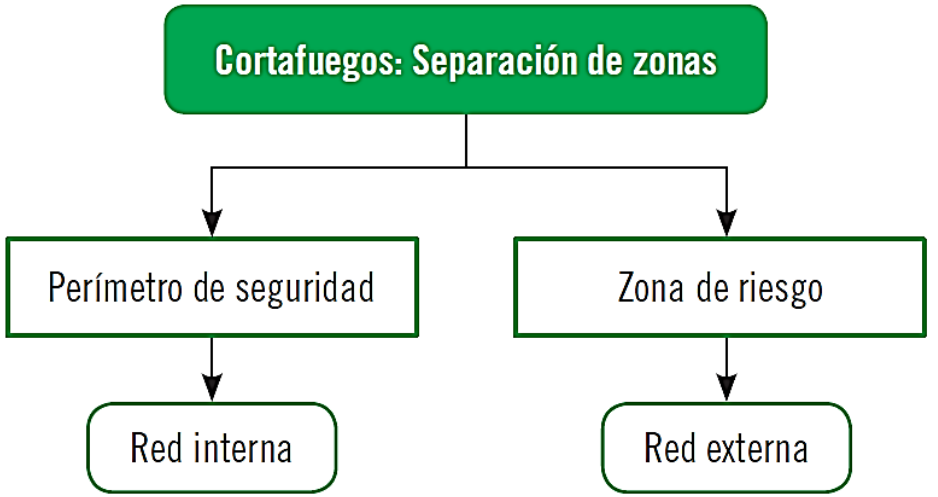


1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS

EL CORTAFUEGOS UTILIZA LOS CONCEPTOS DE PERÍMETRO DE SEGURIDAD Y ZONA DE RIESGO PARA DETERMINAR LAS REDES INTERNA Y EXTERNA DE UN SISTEMA DE INFORMACIÓN:

- **PERÍMETRO DE SEGURIDAD**
- **ZONA DE RIESGO**



1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

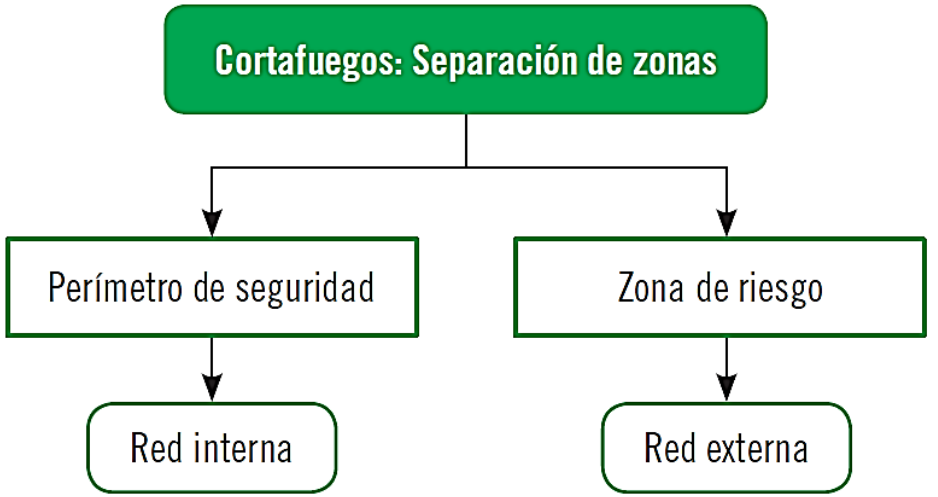
PRINCIPIOS GENERALES DE CORTAFUEGOS

PERÍMETRO DE SEGURIDAD

ESPACIO PROTEGIDO POR EL CORTAFUEGOS, SUELE SER PROPIEDAD DE LA ORGANIZACIÓN Y SE CORRESPONDE CON SU RED INTERNA.

ZONA DE RIESGO

ES LA RED FRENTE A LA QUE SE PROTEGE EL PERÍMETRO DE SEGURIDAD CON EL CORTAFUEGOS.

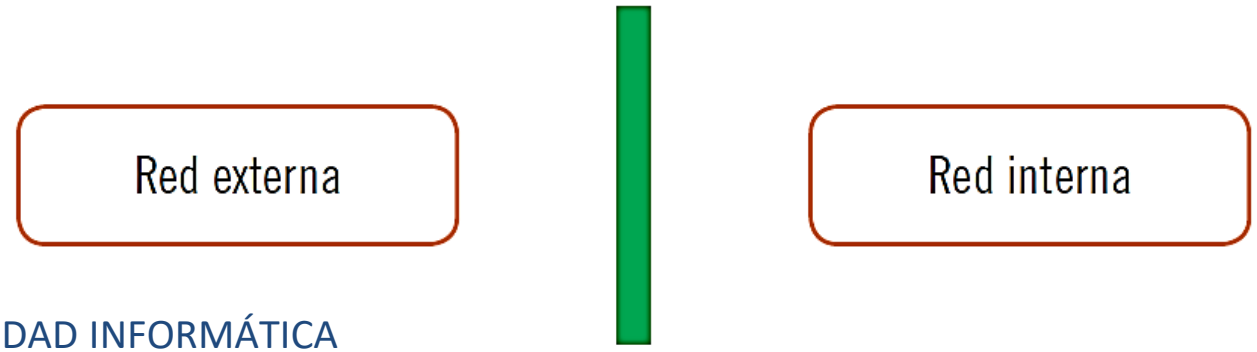


1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS

ESTÁ CLARO QUE LA PROTECCIÓN COMPLETA Y MÁS EFECTIVA SERÍA EL **AISLAMIENTO TOTAL DE LA RED INTERNA** DE LA RED EXTERNA CON LA NO CONEXIÓN DE LOS DISPOSITIVOS A INTERNET.

ESTE FORMATO DE PROTECCIÓN ES MUY EFICAZ, YA QUE IMPIDE QUÉ ENTRE CUALQUIER INTRUSO NO AUTORIZADO A LA RED INTERNA, **PERO CONLLEVA PÉRDIDAS DE CONECTIVIDAD IMPORTANTES DEBIDAS AL AISLAMIENTO TOTAL.**

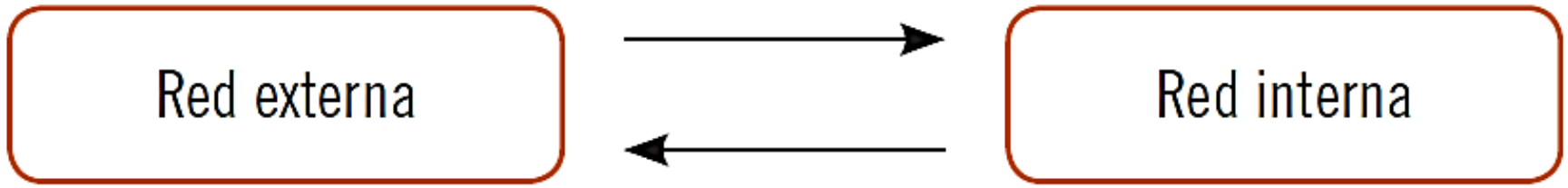


1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS

OTRA OPCIÓN ES MANTENER **EL SISTEMA** DE INFORMACIÓN DE LA ORGANIZACIÓN **CONECTADO CON LA RED EXTERNA SIN PROTECCIÓN.**

ESTA CONFIGURACIÓN YA **EVITA EL PROBLEMA DE LA FALTA DE CONECTIVIDAD, PERO DEJA AL SISTEMA COMPLETAMENTE VULNERABLE** ANTE POSIBLES INCIDENTES DE SEGURIDAD E INTRUSIONES.



1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS

LA MEJOR ALTERNATIVA, DESPUÉS DE VER LAS VENTAJAS E INCONVENIENTES DE LOS FORMATOS ANTERIORES, ES LA UTILIZACIÓN DE UN **CORTAFUEGOS.**

CON ESTA CONFIGURACIÓN SE **MANTIENE LA CONECTIVIDAD DEL SISTEMA CON EL EXTERIOR, PERO SE RESUELVEN PROBLEMAS DE SEGURIDAD** CON LA IMPLANTACIÓN DEL CORTAFUEGOS, QUE IMPIDE ACCESOS NO AUTORIZADOS.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS

LA PROTECCIÓN QUE OFRECE UN CORTAFUEGOS SE DEFINE EN TRES OBJETIVOS BÁSICOS:

- **ESTABLECER UN ENLACE CONTROLADO** ENTRE LA RED INTERNA Y LA RED EXTERNA DE UN SISTEMA DE INFORMACIÓN.
- **PROTEGER A LA RED INTERNA** DE POSIBLES ATAQUES E INTRUSIONES PROCEDENTES DE LA RED EXTERNA (INTERNET).
- **ESTABLECER UN PUNTO ÚNICO DE DEFENSA** CON UNA UBICACIÓN ESTRATÉGICA (AUMENTANDO LO MÁXIMO POSIBLE TANTO LA CONECTIVIDAD COMO LA SEGURIDAD DEL SISTEMA).

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

PARA MAXIMIZAR LA FIABILIDAD Y EFICIENCIA DE UN CORTAFUEGOS, ES FUNDAMENTAL QUE SU DISEÑO E IMPLANTACIÓN SE TOMEN DE UN MODO RAZONADO, DEBIÉNDOSE ESTUDIAR TODOS LOS ASPECTOS DE LA ORGANIZACIÓN QUE PUEDAN SER INFLUYENTES.

EL DISEÑO DE LA ESTRUCTURA DE UN CORTAFUEGOS DEBE REALIZARSE TENIENDO EN CUENTA **TRES OBJETIVOS FUNDAMENTALES**:

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

- **TODO EL TRÁFICO DE DATOS** DESDE LA RED INTERNA HACIA EL EXTERIOR **DEBE PASAR POR EL CORTAFUEGOS**.
- **SOLO SE PERMITIRÁ PASAR** A LA RED LOCAL **EL TRÁFICO AUTORIZADO** ESPECÍFICAMENTE POR LA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN.
- **EL CORTAFUEGOS DEBE SER INMUNE A POSIBLES PENETRACIONES DE INTRUSOS**, MEDIANTE LA UTILIZACIÓN DE SISTEMAS CONFIABLES ACORDES Y DE SISTEMAS OPERATIVOS SEGUROS.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

ADEMÁS DE LOS OBJETIVOS A CONSIDERAR EN EL DISEÑO DEL CORTAFUEGOS, **DEBEN TENERSE EN CUENTA LOS SIGUIENTES SERVICIOS DE CONTROL DE ACCESOS** QUE DEBEN PODER CUBRIRSE:

- **CONTROL DE SERVICIOS**
- **CONTROL DE DIRECCIÓN**
- **CONTROL DE USUARIOS**
- **CONTROL DE COMPORTAMIENTO**

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

- **CONTROL DE SERVICIOS**

  ESTABLECE *A QUÉ TIPO DE SERVICIOS DE LA ORGANIZACIÓN SE PUEDE ACCEDER* DESDE LAS REDES INTERNAS Y EXTERNAS.

- **CONTROL DE DIRECCIÓN**

  ESTABLECE *LAS DIRECCIONES DE ENTRADA Y SALIDA EN LAS QUE SE PERMITIRÁ EL TRÁFICO* DE DATOS DESDE/HACIA LA RED EXTERNA.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

- **CONTROL DE USUARIOS**

  ESTABLECE CONTROLES DE ACCESO PARA DETERMINAR *A QUÉ SERVICIOS PUEDE ACCEDER CADA USUARIO*.

- **CONTROL DE COMPORTAMIENTO**

  ESTABLECE EL *USO CONCRETO DE CIERTOS SERVICIOS* PARTICULARES.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

CUANDO SE VA A IMPLANTAR Y CONFIGURAR UN CORTAFUEGOS EN UN SISTEMA DE INFORMACIÓN, *HAY QUE TOMAR TRES DECISIONES FUNDAMENTALES:*

- **POLÍTICAS DE SEGURIDAD**
- **MONITORIZACIÓN**
- **ECONOMÍA**

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

POLÍTICA DE SEGURIDAD

LA PRIMERA DECISIÓN TRATA SOBRE LA **POLÍTICA DE SEGURIDAD DEL CORTAFUEGOS Y DEL NIVEL DE PROTECCIÓN** QUE SE PRETENDE IMPLANTAR.

CADA ORGANIZACIÓN DEBE ESTABLECER LA PROTECCIÓN DEL CORTAFUEGOS, ATENDIENDO A LA UTILIZACIÓN DE LA RED Y A LAS CARACTERÍSTICAS DE LOS USUARIOS.

NO ES LO MISMO QUE LA EMPRESA DESEE BLOQUEAR TODO EL TRÁFICO DE UNA RED QUE PRETENDA BLOQUEAR SOLO SITIOS WEB.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

MONITORIZACIÓN

LA SEGUNDA DECISIÓN HACE REFERENCIA AL **GRADO DE MONITORIZACIÓN Y CONTROL** QUE PRETENDE ESTABLECER LA ORGANIZACIÓN.

EN EL MOMENTO DE DEFINIR LA POLÍTICA DE SEGURIDAD A ESTABLECER, LA EMPRESA TENDRÁ QUE DEFINIR EL GRADO DE SEGURIDAD DEL CORTAFUEGOS, **DECIDIENDO QUÉ TIPO DE INFORMACIÓN SE VA A PERMITIR Y CUÁL SE VA A DENEGAR**.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

MONITORIZACIÓN

SE DISTINGUEN DOS POSTURAS OPUESTAS PARA DECIDIR LA MONITORIZACIÓN DEL FIREWALL:

- **POLÍTICA RESTRICTIVA:** EN LA QUE SE *DENIEGA TODO LO QUE NO SE PERMITE.*
- **POLÍTICA PERMISIVA:** EN LA QUE SE *PERMITE TODO LO QUE NO SE DENIEGA.*

UNA POLÍTICA RESTRICTIVA ES MÁS ACONSEJABLE EN SEGURIDAD, PERO CON SU APLICACIÓN ES POSIBLE QUE LAS LIMITACIONES DE ACCESO A CIERTOS SITIOS SEAN EXCESIVAS E IMPIDAN EL DESARROLLO DE LAS TAREAS HABITUALES DE LA ORGANIZACIÓN.

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS

PRINCIPIOS GENERALES DE CORTAFUEGOS. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

ECONOMÍA

EL ÚLTIMO PUNTO **ES PURAMENTE ECONÓMICO**. SEGÚN LA VALORACIÓN DE LOS ACTIVOS Y DE LA INFORMACIÓN OBJETIVO QUE SE DESEE PROTEGER, LOS COSTES A ASUMIR POR LA IMPLANTACIÓN SERÁN MENORES O SUPERIORES.

ES EVIDENTE QUE, CUANTO MAYOR SEA EL VALOR DE LOS ACTIVOS A PROTEGER, MAYOR SERÁ EL GASTO QUE DEBERÁ SOPORTAR LA ORGANIZACIÓN PARA LA IMPLANTACIÓN DEL CORTAFUEGOS Y MAYOR CALIDAD DEBERÁ TENER EL SISTEMA A IMPLANTAR.

CONTENIDOS

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS
2. **COMPONENTES DE UN CORTAFUEGOS DE RED**
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
4. ARQUITECTURAS DE CORTAFUEGOS DE RED
5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

2. COMPONENTES DE UN CORTAFUEGOS DE RED

CUANDO YA SE HAN DECIDIDO LAS CARACTERÍSTICAS PRINCIPALES DEL CORTAFUEGOS A IMPLANTAR, EL SIGUIENTE PASO ES DECIDIR QUÉ **MECANISMOS** SE VAN A INCORPORAR A DICHO CORTAFUEGOS **PARA CUMPLIR CON LAS POLÍTICAS DE SEGURIDAD** DEFINIDAS POR LA ORGANIZACIÓN.

TODOS **LOS CORTAFUEGOS ESTÁN COMPUESTOS POR TRES COMPONENTES** SOBRE LOS QUE SE DEBERÁN IMPLANTAR LOS MECANISMOS DE PROTECCIÓN:

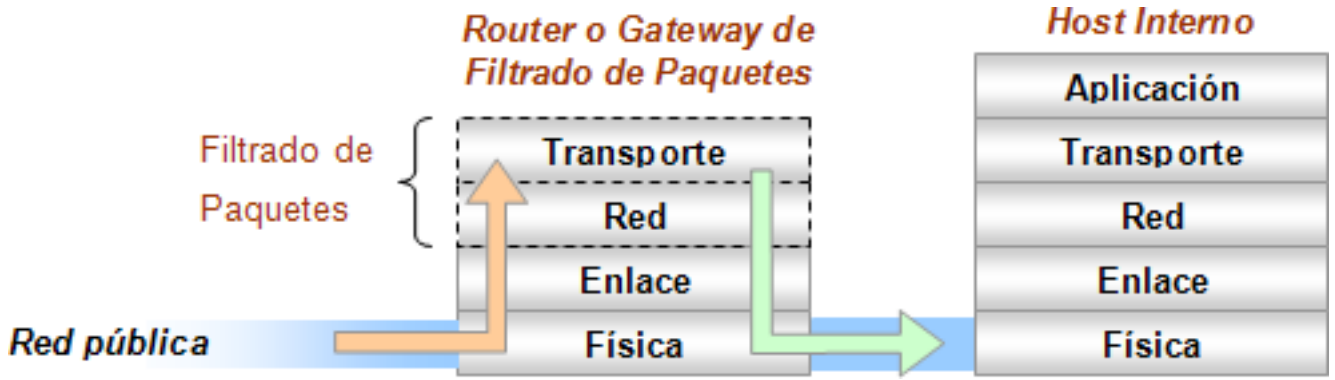
- **FILTRADO DE PAQUETES**
- **PROXY DE APLICACIÓN**
- **MONITORIZACIÓN DE LA ACTIVIDAD**

2. COMPONENTES DE UN CORTAFUEGOS DE RED

FILTRADO DE PAQUETES

GENERALMENTE, LOS CORTAFUEGOS UTILIZAN **REGLAS DE FILTRADO DE PAQUETES** CON EL OBJETIVO DE DISMINUIR LA CARGA DE LA RED.

EL FILTRADO DE PAQUETES SE UTILIZA PARA CUMPLIR CON LOS OBJETIVOS DE SEGURIDAD DE UNA RED ESTABLECIDOS POR LA ORGANIZACIÓN, **EVITANDO LOS ACCESOS NO AUTORIZADOS, PERO PERMITIENDO EN TODO MOMENTO LOS ACCESOS AUTORIZADOS**.



2. COMPONENTES DE UN CORTAFUEGOS DE RED

FILTRADO DE PAQUETES

EL FUNCIONAMIENTO DEL COMPONENTE DE FILTRADO DE PAQUETES ES BASTANTE SENCILLO:

- EN UN PRIMER MOMENTO **SE ANALIZA LA CABECERA DE CADA PAQUETE DE DATOS** QUE PRETENDE ENTRAR EN LA RED LOCAL.
- SEGÚN LAS REGLAS PREESTABLECIDAS Y ATENDIENDO AL ANÁLISIS DEL PAQUETE, **SE LE PERMITIRÁ EL ACCESO O SERÁ BLOQUEADA**. LOS ASPECTOS MÁS HABITUALES POR ANALIZAR SON:
  - PROTOCOLO UTILIZADO.
  - DIRECCIÓN DE ORIGEN Y DIRECCIÓN DE DESTINO.
  - PUERTO DE DESTINO.

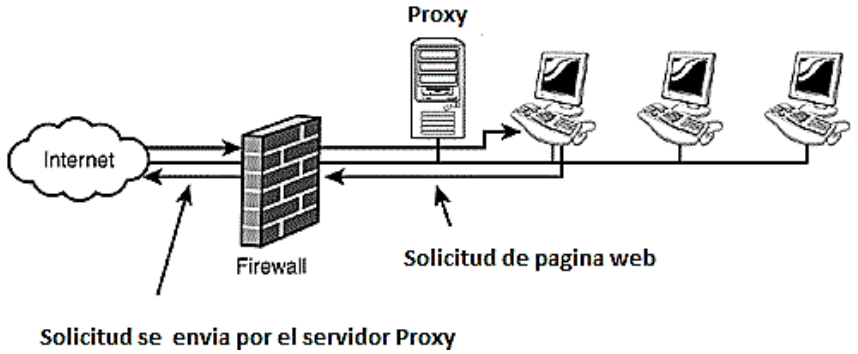
2. COMPONENTES DE UN CORTAFUEGOS DE RED

PROXY DE APLICACIÓN

LOS CORTAFUEGOS SUELEN INCORPORAR PAQUETES DE **APLICACIONES SOFTWARE QUE REENVÍEN O BLOQUEEN CONEXIONES A UNOS SERVICIOS** CONCRETOS.

ESTAS APLICACIONES SOFTWARE SE DENOMINAN **SERVICIOS PROXY** Y LAS MÁQUINAS EN LAS QUE SON EJECUTADAS SON LAS **PASARELAS DE APLICACIÓN**.

LOS SERVICIOS PROXY PERMITEN AUMENTAR EL NIVEL DE SEGURIDAD DE LA RED.



2. COMPONENTES DE UN CORTAFUEGOS DE RED

PROXY DE APLICACIÓN

VENTAJAS

PERMISIÓN EXCLUSIVA DE SERVICIOS CON PROXY

EL SERVICIO PROXY **SOLO PERMITIRÁ EL USO DE LOS SERVICIOS** CON ESTOS PROTOCOLOS, **DENEGANDO EL RESTO DE SERVICIOS**.

FILTRADO DE PROTOCOLOS

OFRECEN OPCIONES DE FILTRADO DE DATOS, YENDO **MÁS ALLÁ DEL FILTRADO** POR LAS CARACTERÍSTICAS DE LA CABECERA **DEL PAQUETE**.

SIMPLIFICACIÓN DE REGLAS DE FILTRADO

FACILITAN LA TAREA DE ESTABLECER Y DEFINIR LAS REGLAS DE FILTRADO POR SU MAYOR SIMPLICIDAD. HAY QUE **PERMITIR EL TRÁFICO DE DATOS HACIA LA PASARELA** Y **BLOQUEAR EL RESTO DE DATOS**.

2. COMPONENTES DE UN CORTAFUEGOS DE RED

PROXY DE APLICACIÓN

DESVENTAJAS

- **CADA SERVICIO REQUIERE UN SERVICIO PROXY PROPIO.**
- **ES MÁS COSTOSO QUE LOS FILTROS DE PAQUETES SIMPLES.**
- **TAMBIÉN TIENEN MENOR RENDIMIENTO QUE LOS FILTROS DE PAQUETES**.

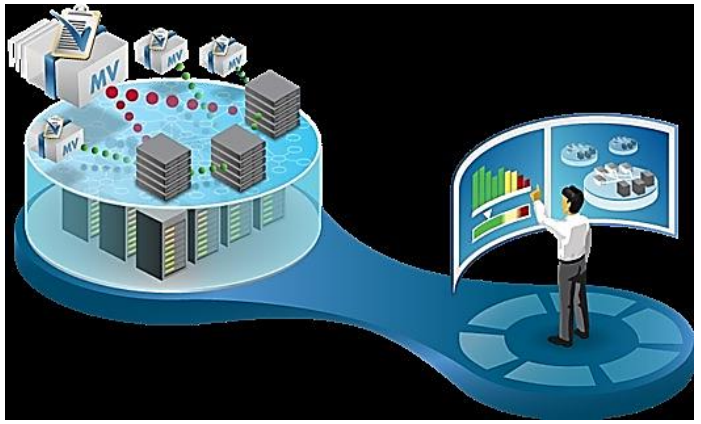
LOS SERVICIOS PROXY **PUEDEN CONVERTIRSE EN UN CUELLO DE BOTELLA DE REDES**, YA QUE DEBEN PASAR POR ELLOS TODAS LAS SOLICITUDES Y PAQUETES DE DATOS.

2. COMPONENTES DE UN CORTAFUEGOS DE RED

MONITORIZACIÓN DE LA ACTIVIDAD

LA MONITORIZACIÓN DE LA ACTIVIDAD DEL CORTAFUEGOS ES IMPRESCINDIBLE PARA LA SEGURIDAD DE LOS ELEMENTOS QUE PROTEGE, **PERMITE OBTENER INFORMACIÓN SOBRE**:

- TODOS **LOS ATAQUES QUE SE HAN PRODUCIDO** (O SE ESTÁN PRODUCIENDO).
- LA **PRESENCIA DE PAQUETES DE DATOS SOSPECHOSOS** (INDEPENDIENTEMENTE DE SI FINALMENTE SON ATAQUES REALES O NO).



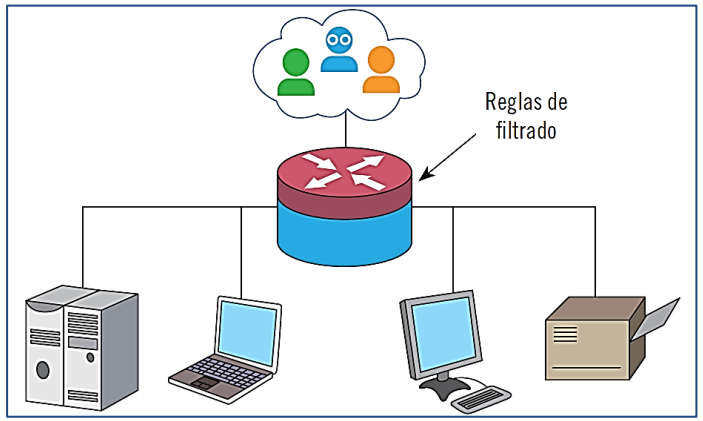
CONTENIDOS

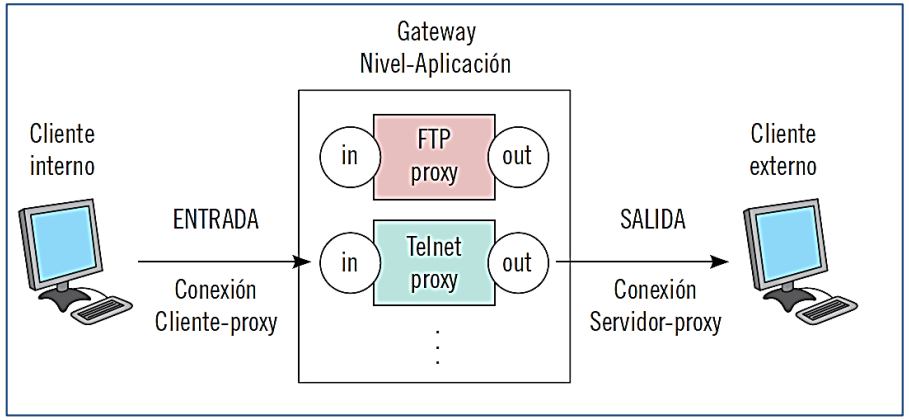
1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS
2. COMPONENTES DE UN CORTAFUEGOS DE RED
3. **RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD**
4. ARQUITECTURAS DE CORTAFUEGOS DE RED
5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

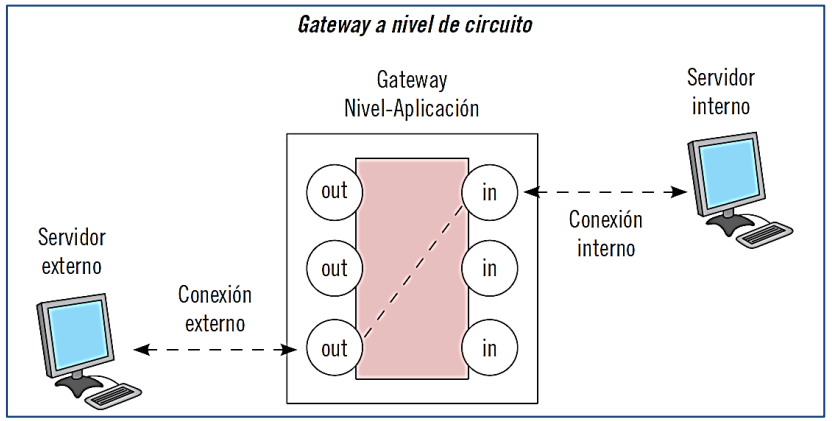
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

SE DESTACAN TRES **TIPOS DE CORTAFUEGOS** ATENDIENDO A SU UBICACIÓN Y FUNCIONALIDAD:

- **ROUTER CON FILTRADO DE PAQUETES**
- **GATEWAY A NIVEL DE APLICACIÓN**
- **GATEWAY A NIVEL DE CIRCUITOS**



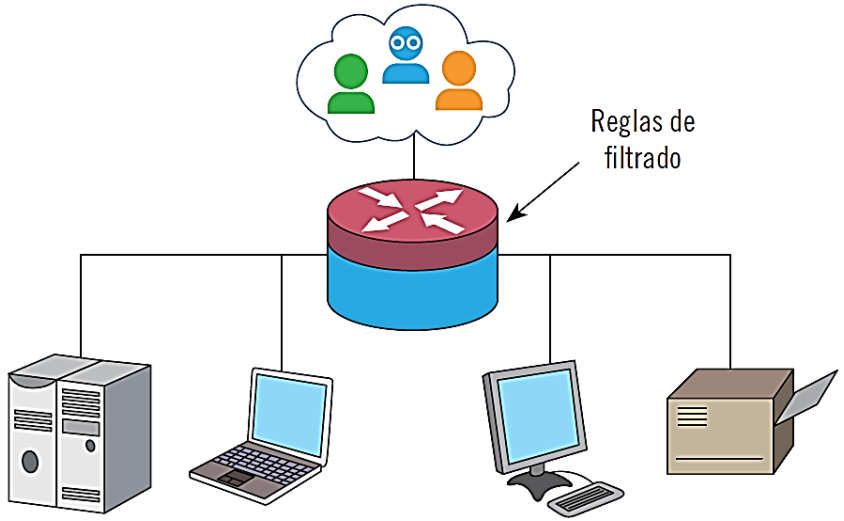




3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

ROUTER CON FILTRADO DE PAQUETES

LOS ROUTERS CON FILTRADO DE PAQUETES SON UN TIPO DE CORTAFUEGOS QUE **FILTRAN LOS PAQUETES IP ENTRANTES, ATENDIENDO A UNA SERIE DE REGLAS PREDEFINIDAS**: SEGÚN LA DEFINICIÓN DE ESTAS REGLAS, ESTOS ROUTERS DESCARTAN EL PAQUETE O LO REENVÍAN.



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

ROUTER CON FILTRADO DE PAQUETES

EL FILTRO **SE CONFIGURA A TRAVÉS DE UNA SERIE DE REGLAS BASADAS EN LOS ENCABEZADOS DE LOS PAQUETES** DE DATOS.

VENTAJAS

- SIMPLICIDAD.
- NO SON VISIBLES PARA LOS USUARIOS.
- DESTACAN POR SU ELEVADA VELOCIDAD.

DESVENTAJAS

- DIFICULTAD PARA LA CORRECTA DEFINICIÓN DE LAS REGLAS DE ACCESO A LOS PAQUETES DE INFORMACIÓN.
- NO REQUIEREN AUTENTIFICACIÓN DE LOS USUARIOS.

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

ROUTER CON FILTRADO DE PAQUETES

SON ESPECIALMENTE **SUSCEPTIBLES A UNOS ATAQUES DETERMINADOS**:

SUPLANTACIÓN DE DIRECCIONES IP POR DIRECCIONES INTERNAS

SE ACONSEJA BORRAR LOS PAQUETES DE DATOS QUE CONTENGAN DIRECCIONES INTERNAS QUE PROVIENEN DEL EXTERIOR.

ATAQUES DE ENCAMINAMIENTO DE FUENTE

AL BLOQUEAR CIERTAS DIRECCIONES IP, LOS ROUTERS DE FILTRADO NO PUEDEN IMPEDIR LOS ATAQUES DE ENCAMINAMIENTO DE FUENTE. PARA SOLUCIONAR ESTE PROBLEMA, SE ACONSEJA ELIMINAR PAQUETES DE DATOS QUE USAN ESTA OPCIÓN.

FRAGMENTOS DE REDUCIDO TAMAÑO

ESTE TIPO DE CORTAFUEGOS FALLA BASTANTE CON PAQUETES DE DATOS CON ENCABEZADOS TCP POR SU FRAGMENTACIÓN.

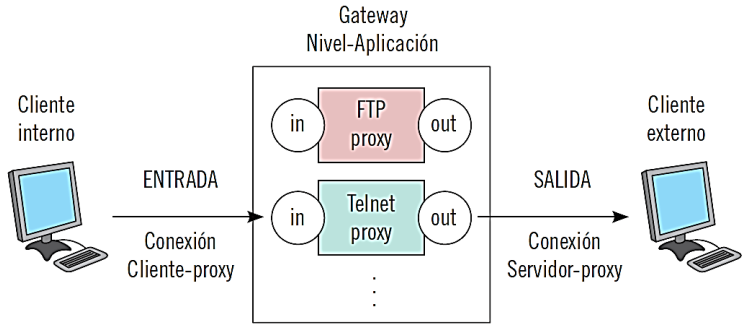
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

GATEWAYS A NIVEL DE APLICACIÓN

SE ASOCIAN AL COMPONENTE DE **SERVIDORES PROXY** DE LOS CORTAFUEGOS.

SON REPETIDORES DE TRÁFICO A NIVEL DE APLICACIÓN: **CUANDO UN USUARIO SOLICITA UN SERVICIO, LO REALIZA A TRAVÉS DEL PROXY**.

UNA VEZ RECIBIDA LA PETICIÓN, **EL PROXY REALIZA EL PEDIDO AL SERVIDOR REAL** Y DEVUELVE LA INFORMACIÓN SOLICITADA AL USUARIO.



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

GATEWAYS A NIVEL DE APLICACIÓN

VENTAJAS

- OFRECE MAYOR SEGURIDAD QUE LOS ROUTERS DE FILTRADO DE PAQUETES.
- REVISA SOLO LAS APLICACIONES PERMITIDAS, AUMENTANDO SU EFICACIA.
- REVISA TODO EL TRÁFICO DE RED ENTRANTE. EVITA EL TRÁFICO DIRECTO ENTRE REDES.

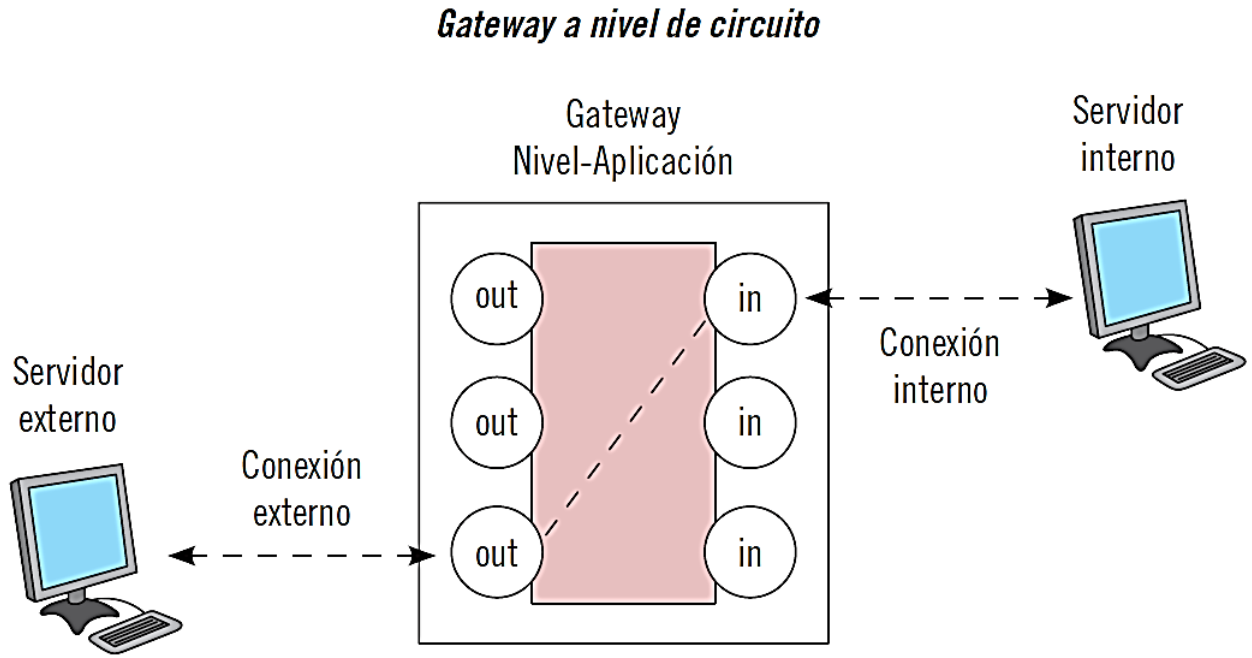
DESVENTAJAS

- PUEDE PROVOCAR CUELLOS DE BOTELLA POR SOBRECARGA DE PROCESAMIENTO EN CADA CONEXIÓN.

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

GATEWAYS A NIVEL DE CIRCUITO

SON SISTEMAS QUE REDIRIGEN LOS PAQUETES DE DATOS CUANDO SE HA COMPROBADO QUE SE HA ESTABLECIDO LA CONEXIÓN.



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

GATEWAYS A NIVEL DE CIRCUITO

PARA ESTABLECER LA CONEXIÓN, ESTOS GATEWAYS VALIDAN EL INICIO DE LA COMUNICACIÓN PARA VERIFICAR SI SE REALIZA CORRECTAMENTE SEGÚN EL PROTOCOLO DE TRASPORTES.

CUANDO YA SE HA VALIDADO LA COMUNICACIÓN, TODOS LOS PAQUETES QUE SE REENVÍEN A CONTINUACIÓN NO SON VERIFICADOS (**SOLO SE REVISAN LAS CABECERAS DE LOS PAQUETES)**.

EN TÉRMINOS GENERALES, LOS GATEWAYS A NIVEL DE CIRCUITO ESTABLECEN FUNCIONES QUE DETERMINAN QUÉ CONEXIONES SERÁN PERMITIDAS PARA LA TRANSMISIÓN DE DATOS.

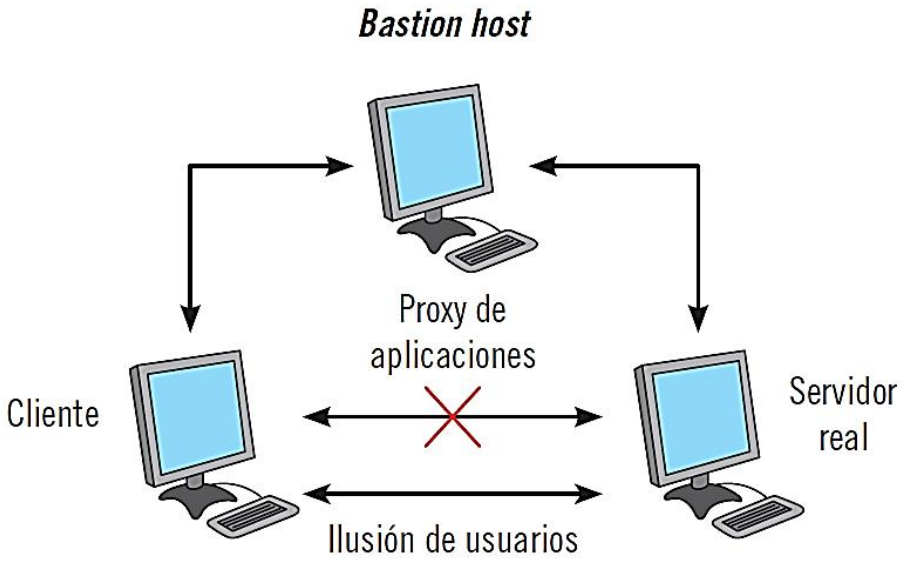
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

HOST BASTIÓN

ES UN PUNTO CRÍTICO DEL SISTEMA EN LA SEGURIDAD DE LA RED IDENTIFICADO POR EL ADMINISTRADOR DEL CORTAFUEGOS.

NO ES UN TIPO DE CORTAFUEGOS EN SÍ, PERO ES INTERESANTE MENCIONARLO PORQUE **SIRVE COMO PLATAFORMAS PARA:**

- **GATEWAYS A NIVEL DE APLICACIÓN**
- **GATEWAYS A NIVEL DE CIRCUITO**

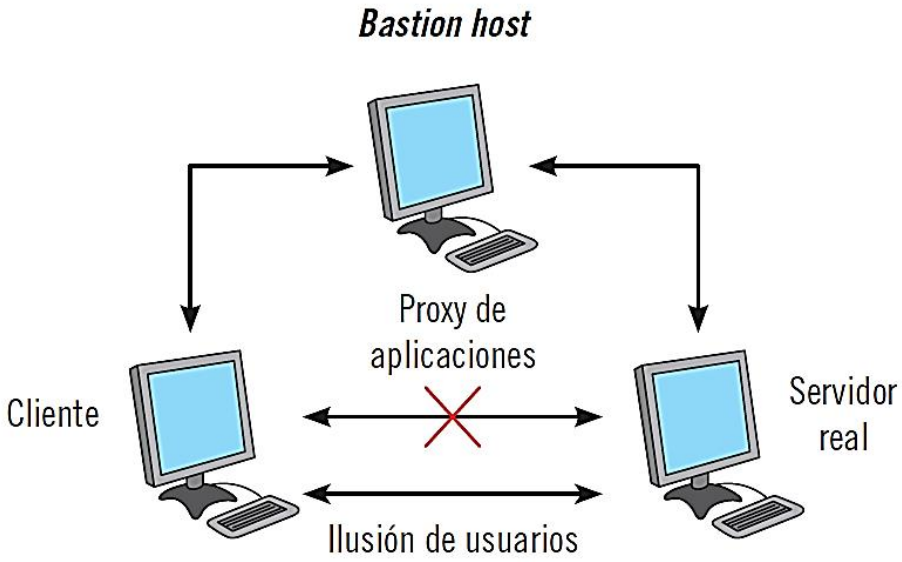


3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

HOST BASTIÓN

SE TRATA DE **UNA APLICACIÓN UBICADA EN UN PUNTO CRÍTICO DE UN SERVIDOR PARA PROTEGER** A LA RED INTERNA DE LA ORGANIZACIÓN.

ESTE PUNTO CRÍTICO **HA SIDO CONFIGURADO PREVIAMENTE** PARA QUE ATRAIGA LOS POSIBLES ATAQUES QUE INTENTEN ACCEDER AL SISTEMA.



CONTENIDOS

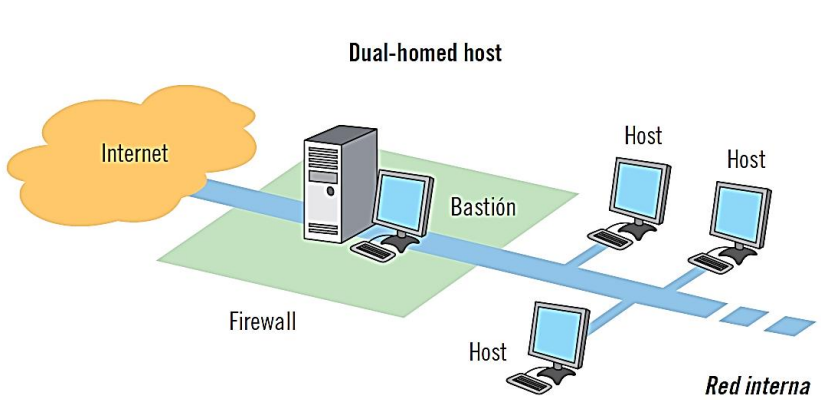
1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS
2. COMPONENTES DE UN CORTAFUEGOS DE RED
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
4. **ARQUITECTURAS DE CORTAFUEGOS DE RED**
5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

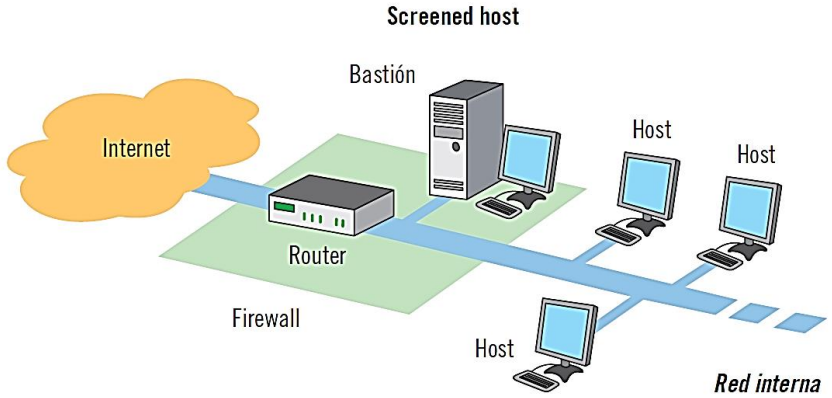
4. ARQUITECTURAS DE CORTAFUEGOS DE RED

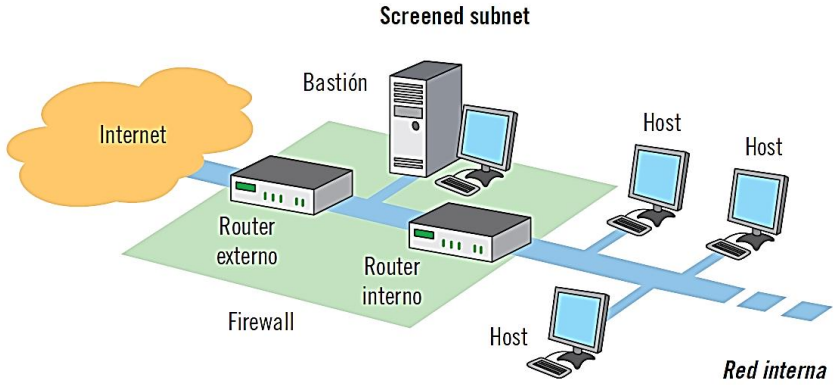
ADEMÁS DE LA UTILIZACIÓN DE LOS CORTAFUEGOS SIMPLES, HAY VARIAS POSIBILIDADES DE FIREWALLS MÁS COMPLEJOS QUE PERMITEN EL AUMENTO DE LA SEGURIDAD DEL PERÍMETRO DE SEGURIDAD.

LAS ARQUITECTURAS COMPLEJAS MÁS COMUNES SON LAS SIGUIENTES:

- **DUAL-HOMED HOST**
- **SCREENED HOST**
- **SCREENED SUBNET (DMZ)**





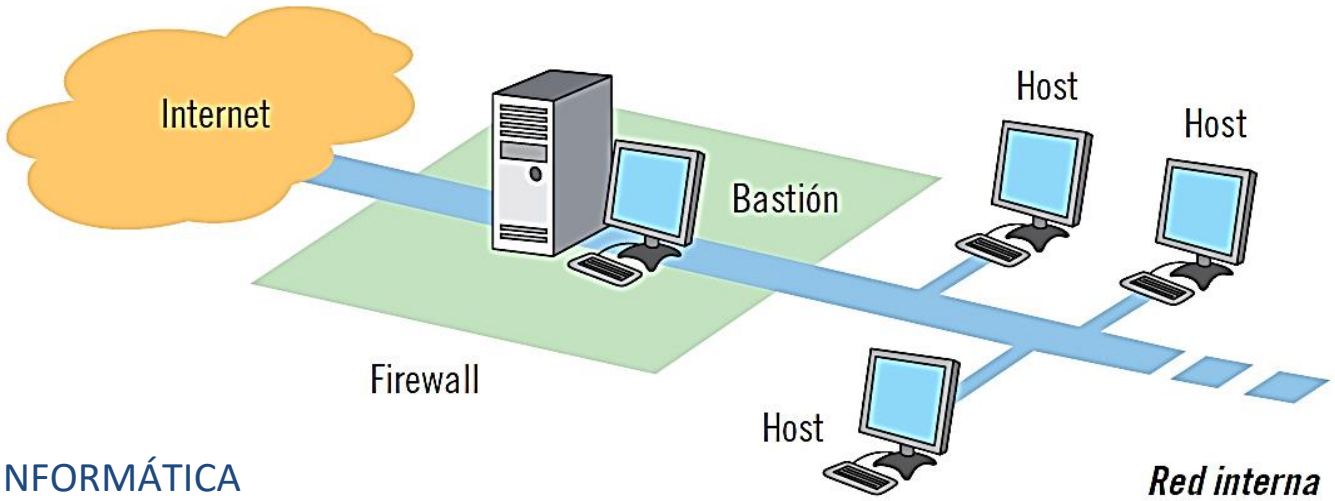


4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS DUAL-HOMED HOST

LAS ARQUITECTURAS DE CORTAFUEGOS DUAL-HOMED HOST OFRECEN UNA MAYOR PROTECCIÓN QUE LOS CORTAFUEGOS SIMPLES Y **ESTÁN COMPUESTAS POR DOS TARJETAS DE RED:**

- UNA SE CONECTA A LA RED INTERNA.
- LA OTRA SE CONECTA A LA RED EXTERNA DE LA ORGANIZACIÓN.

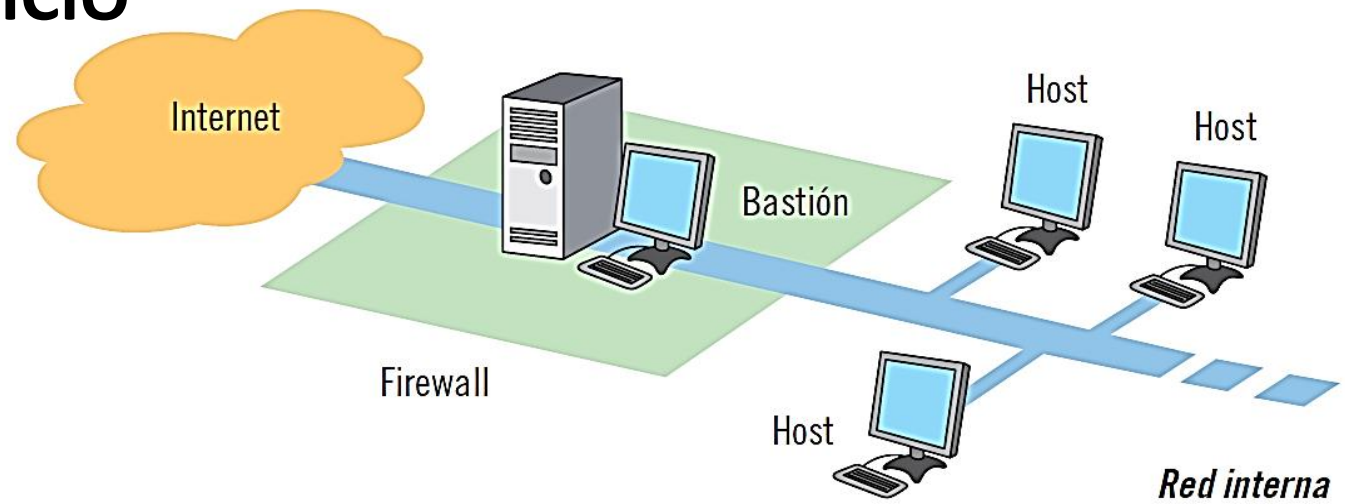


4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS DUAL-HOMED HOST

CON ESTA ARQUITECTURA SE EVITA QUE, SI EL ROUTER SE VE COMPROMETIDO, SE PERMITA EL ACCESO DEL TRÁFICO DE RED A LA RED INTERNA, YA QUE **TODA LA INFORMACIÓN ENTRE INTERNET Y LA RED INTERNA DEBE PASAR PREVIAMENTE POR EL HOST BASTION**.

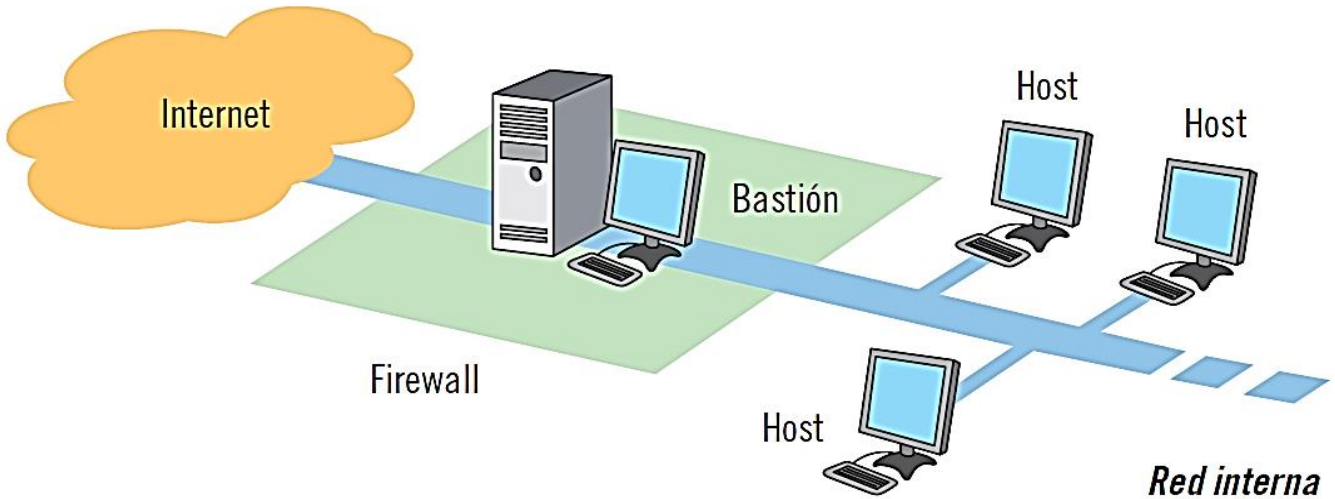
ESTOS SISTEMAS DEBEN EJECUTAR POR LO MENOS **UN SERVIDOR PROXY PARA CADA SERVICIO**



4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS DUAL-HOMED HOST

EL FIREWALL **ACTÚA COMO INTERMEDIARIO ENTRE LAS REDES INTERNA Y EXTERNA**: LOS SISTEMAS CONECTADOS EN CADA BANDO DEL HOST BASTION SE COMUNICAN A TRAVÉS DE ESTE, SIN HABER POSIBILIDAD DE COMUNICARSE DIRECTAMENTE.



4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS DUAL-HOMED HOST

LOS SERVICIOS DEL HOST BASTION PUEDEN REALIZARSE DE DOS FORMAS DISTINTAS:

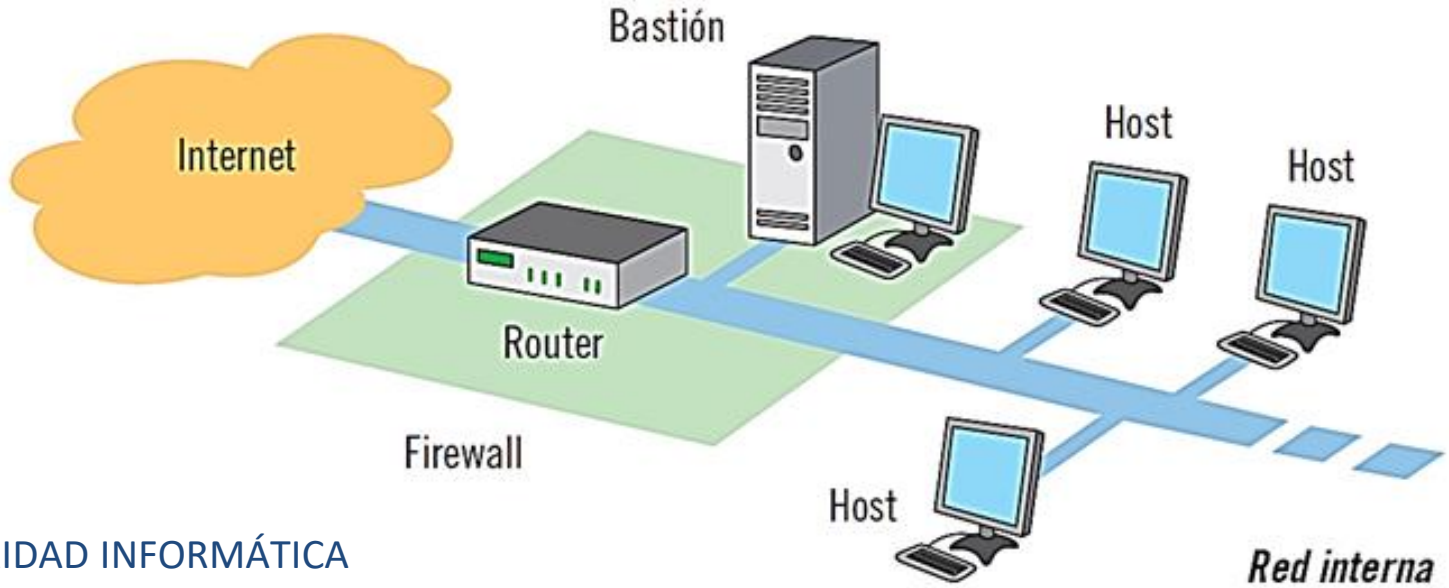
- LOS **USUARIOS EN LA RED INTERNA CON CUENTAS EN EL HOST BASTION** PERMITEN QUE ESTOS PUEDAN INICIAR SESIÓN Y UTILIZAR LOS SERVICIOS DE LA RED EXTERNA. ES BASTANTE VULNERABLE, YA QUE DEPENDE DE LA CONTRASEÑA ESTABLECIDA POR EL USUARIO.
- MEDIANTE LA EJECUCIÓN DE **SERVICIOS PROXY PARA CADA UNO DE LOS SERVICIOS** QUE SE QUIERAN PERMITIR. AQUÍ SE AUMENTA LA SEGURIDAD DE LA RED INTERNA, YA QUE ES COMPLETAMENTE INDEPENDIENTE DE LA ACTIVIDAD DE LOS USUARIOS EN EL ESTABLECIMIENTO DE CONTRASEÑAS.

4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS CON SCREENED HOST (SINGLE-HOMED HOST)

LOS CORTAFUEGOS SINGLE-HOMED HOST **ESTÁN FORMADOS POR DOS SISTEMAS DE PROTECCIÓN** QUE FILTRAN CONEXIONES A NIVEL DE CIRCUITO Y A NIVEL DE APLICACIÓN:

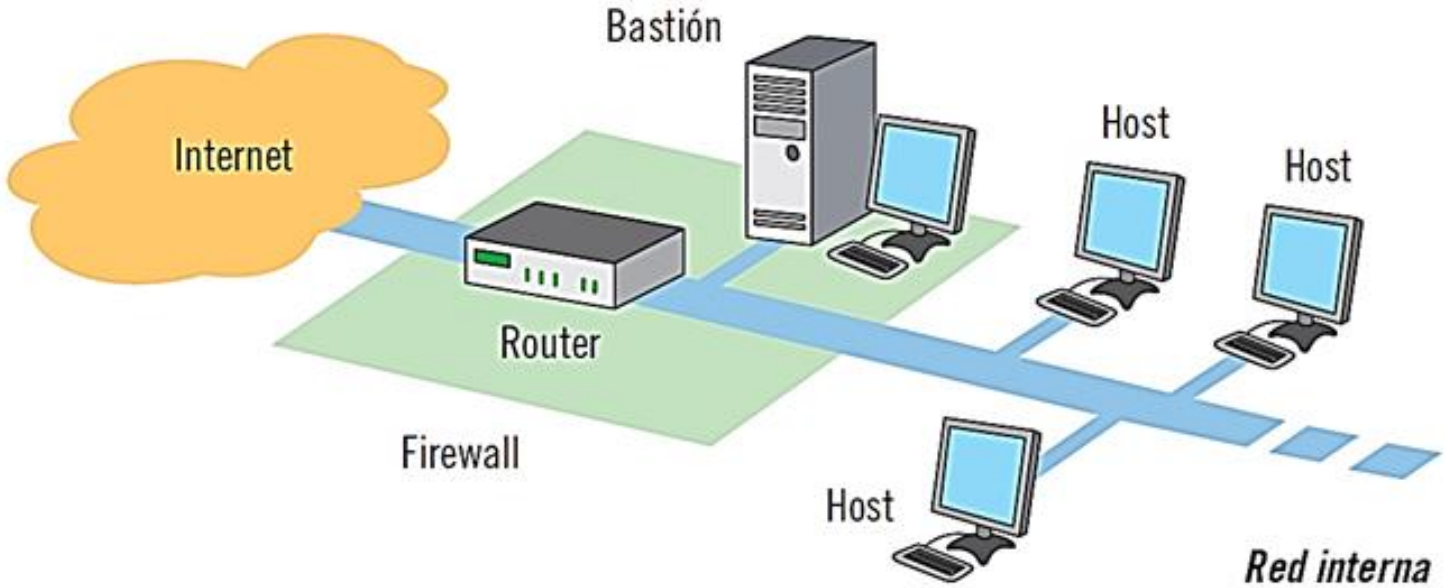
- **UN ROUTER CON FILTRADO DE PAQUETES.**
- **UN HOST BASTION.**



4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS CON SCREENED HOST (SINGLE-HOMED HOST)

EL ROUTER SE CONFIGURA ESPECÍFICAMENTE PARA QUE **TODOS LOS PAQUETES DE DATOS QUE PROVIENEN DE LA RED EXTERNA DEBAN PASAR OBLIGATORIAMENTE POR EL HOST BASTION**, LO QUE OBLIGA A LA ORGANIZACIÓN AL ESTABLECIMIENTO DE ELEVADOS SISTEMAS DE PROTECCIÓN A DICHO BASTIÓN.



4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS CON SCREENED HOST (SINGLE-HOMED HOST)

HAY VARIAS ALTERNATIVAS DE CONFIGURACIÓN DEL ROUTER DE FILTRADO DE PAQUETES:

- **ESTABLECER PERMISOS PARA QUE SOLO HOSTS DETERMINADOS PUEDAN ABRIR CONEXIONES A LA RED EXTERNA** PARA SERVICIOS CONCRETOS Y PREESTABLECIDOS.
- **DESHABILITAR TODAS LAS CONEXIONES DE LOS HOSTS A LA RED EXTERNA**, DE MODO QUE SOLO SEA EL HOST BASTION EL QUE PUEDA ESTABLECER ESTAS CONEXIONES.
- **DIRIGIR CIERTOS PAQUETES DE DATOS DEL EXTERIOR A LOS HOSTS INTERNOS** DIRECTAMENTE A TRAVÉS DEL ROUTER.

4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS CON SCREENED HOST (SINGLE-HOMED HOST)

LA ELECCIÓN DE UNA ALTERNATIVA U OTRA DEPENDERÁ DE LA POLÍTICA DE SEGURIDAD ESTABLECIDA POR LA ORGANIZACIÓN:

- SI LA ORGANIZACIÓN ESTABLECE UNA **POLÍTICA MUY RESTRICTIVA** SE ELEGIRÁ LA OPCIÓN DE DESHABILITAR LAS CONEXIONES EXTERNAS.
- SIN EMBARGO, SI LA ORGANIZACIÓN TIENE DEFINIDA UNA **POLÍTICA DE SEGURIDAD MENOS RESTRICTIVA**, SE PERMITIRÁ LA CONEXIÓN DIRECTA DE CIERTOS PAQUETES DE DATOS.

4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS CON SCREENED HOST (SINGLE-HOMED HOST)

SON MÁS FLEXIBLES QUE LAS ARQUITECTURAS SIMPLES, YA QUE PERMITEN QUE CIERTOS SERVICIOS QUE NO ESTARÍAN PERMITIDOS POR LA ESTRUCTURA CON SERVICIOS PROXY PUEDAN REDIRIGIRSE A LA RED INTERNA A TRAVÉS DEL ROUTER DE UN MODO DIRECTO.

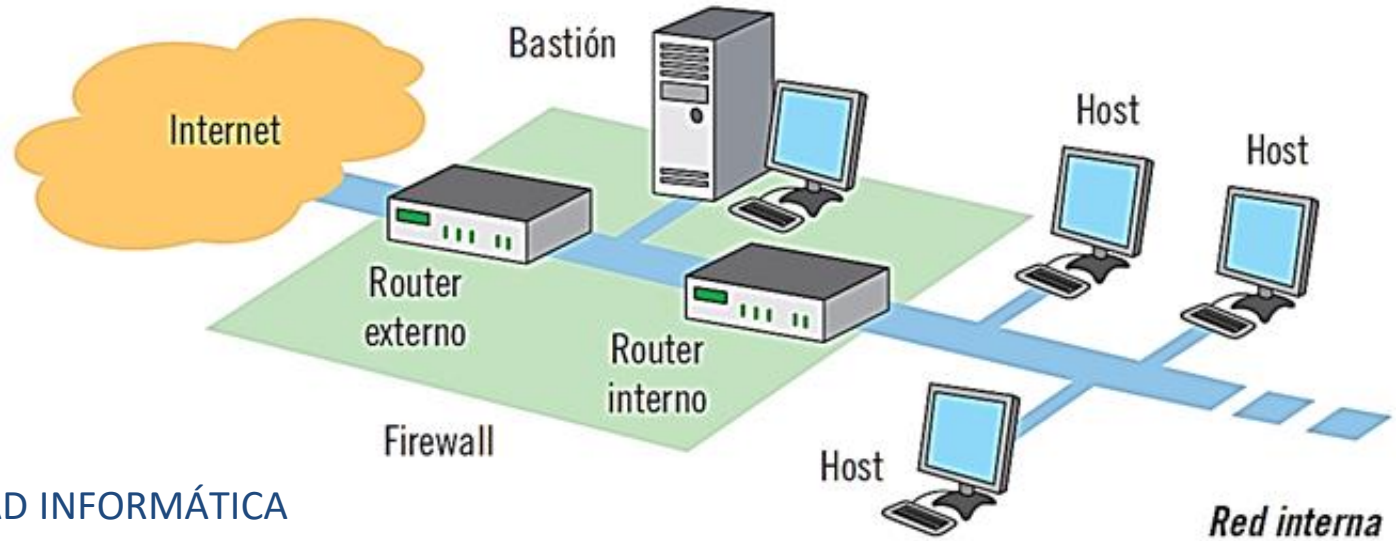
EN COMPARACIÓN CON LAS ARQUITECTURAS DUAL-HOMED HOST, **LAS SCREENED HOST SON MÁS SEGURAS,** AL AÑADIR UNA NUEVA CAPA DE SEGURIDAD: MIENTRAS QUE LAS DUAL-HOMED HOST SOLO FILTRAN LA INFORMACIÓN POR EL HOST BASTION, LAS SCREENED HOST, ADEMÁS DE FILTRAR LA INFORMACIÓN POR EL HOST BASTION, AÑADEN UN ROUTER EXTRA DE FILTRADO.

4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS SCREENED SUBNET (DMZ)

AÑADEN UN ELEMENTO MÁS DE SEGURIDAD QUE EVITE EL ACCESO A LA RED POR VULNERACIÓN DEL HOST BASTION.

ESTE ELEMENTO DE SEGURIDAD SE ESTABLECE CON **UNA RED DE PERÍMETRO EN LA QUE SE CONECTA EL HOST BASTION, LA RED LLAMADA ZONA DESMILITARIZADA-DMZ.**

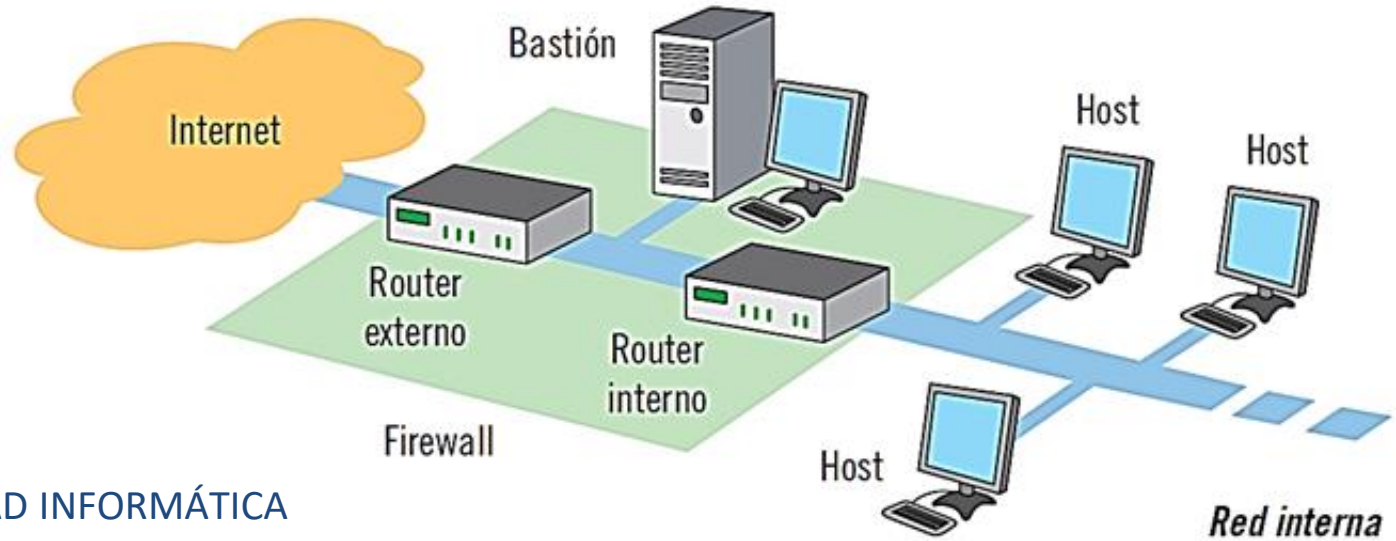


4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS SCREENED SUBNET (DMZ)

SE AÑADE OTRO ROUTER ENTRE EL HOST BASTION Y LA RED INTERNA, DE MODO QUE EL HOST BASTION SE UBICA ENTRE:

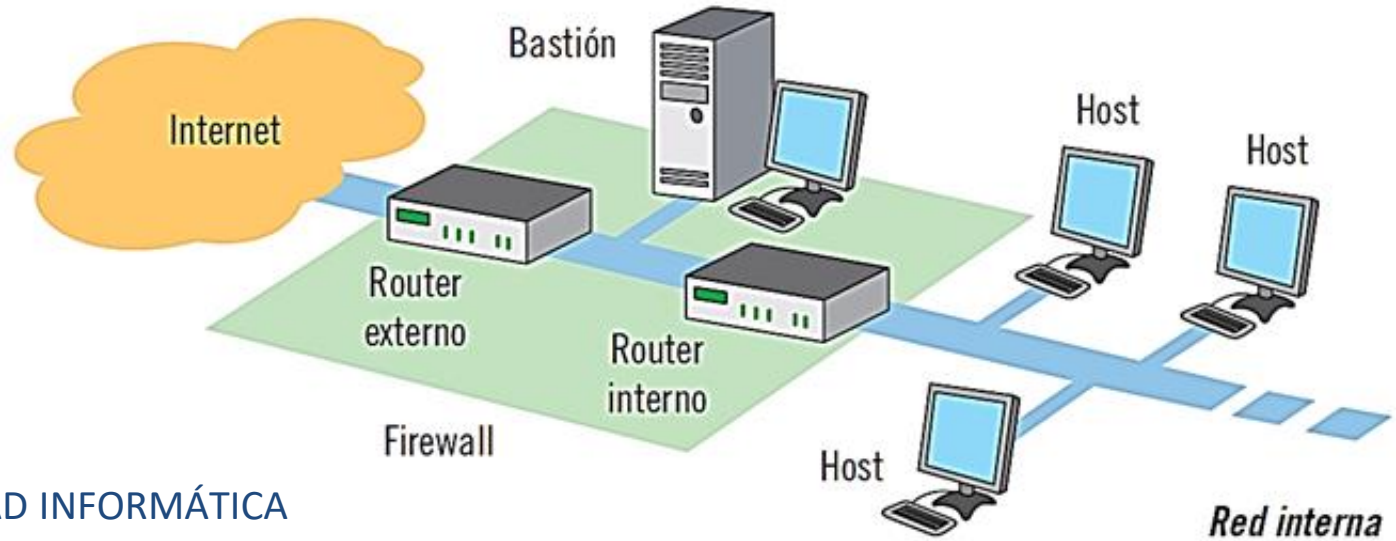
- UN ROUTER INTERNO SITUADO ENTRE LA RED INTERNA Y LA RED PERIMETRAL.
- UN ROUTER EXTERNO UBICADO ENTRE LA RED PERIMETRAL Y LA RED EXTERNA.



4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS SCREENED SUBNET (DMZ)

EN ESTA ARQUITECTURA TAMBIÉN **SE OCULTA EL TRÁFICO DE PAQUETES DE DATOS EN LA RED LOCAL** Y SE ESTABLECE COMO UNA DE LAS ARQUITECTURAS MÁS SEGURAS DE LAS DESCRITAS HASTA EL MOMENTO.



4. ARQUITECTURAS DE CORTAFUEGOS DE RED

ARQUITECTURAS DE CORTAFUEGOS SCREENED SUBNET (DMZ)

ESTE NIVEL DE PROTECCIÓN ADICIONAL ESTÁ FUNDAMENTADO EN LAS FUNCIONES DE LOS ROUTERS INTERNOS Y EXTERNOS Y DEL HOST BASTION:

EL ROUTER EXTERNO ADMINISTRA EL ACCESO DEL TRÁFICO DE DATOS DE LA RED EXTERNA A LA RED PERIMETRAL. SU FUNCIÓN PRINCIPAL ES PROTEGER A LA RED INTERNA Y A LA RED PERIMETRAL DE ATAQUES EXTERNOS.

EL ROUTER INTERNO, ADMINISTRA EL ACCESO DE LA RED PERIMETRAL A LA RED INTERNA PARA PROTEGER A LA RED INTERNA DE LAS REDES EXTERNA Y PERIMETRAL. CON ESTE ROUTER SE IMPLANTA UN NIVEL ADICIONAL DE SEGURIDAD QUE SIGUE PROTEGIENDO A LA RED INTERNA EN CASO DE VULNERARSE EL ROUTER EXTERNO.

EL HOST BASTION SE ESTABLECE COMO PUNTO DE CONTACTO PARA LAS CONEXIONES DE DATOS PROCEDENTES DE LA RED EXTERNA.

CONTENIDOS

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS
2. COMPONENTES DE UN CORTAFUEGOS DE RED
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
4. ARQUITECTURAS DE CORTAFUEGOS DE RED
5. **OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED**

5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

A PARTIR DE ESTAS ARQUITECTURAS, SE PUEDEN ESTABLECER DISTINTAS CONFIGURACIONES SEGÚN LAS NECESIDADES DE PROTECCIÓN DE CADA ORGANIZACIÓN:

- **UTILIZACIÓN DE VARIOS HOST BASTIONS**
- **RED PERIMETRAL CON UN SOLO ROUTER**
- **UTILIZACIÓN DEL HOST BASTION COMO ROUTER EXTERNO**

5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

UTILIZACIÓN DE VARIOS HOST BASTIONS

UNA DE LAS POSIBLES CONFIGURACIONES ALTERNATIVAS ES LA UTILIZACIÓN DE VARIOS HOST BASTIONS CON ALGUNOS DE LOS SIGUIENTES OBJETIVOS:

- **AUMENTAR EL RENDIMIENTO** DE LOS SERVICIOS DE RED.
- OBTENER SERVICIOS DE APOYO CON LA **INTRODUCCIÓN DE REDUNDANCIA.**
- **SEPARAR SERVICIOS DETERMINADOS** POR NECESITAR NIVELES DISTINTOS DE SEGURIDAD.

5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

RED PERIMETRAL CON UN SOLO ROUTER

OTRA OPCIÓN SERÍA UTILIZAR UN SOLO ROUTER PARA LA IMPLANTACIÓN DE UNA RED PERIMETRAL: **ESTE ROUTER HARÍA LAS FUNCIONES DE ROUTER INTERNO Y EXTERNO A LA VEZ**.

EL REQUISITO FUNDAMENTAL PARA EL ESTABLECIMIENTO DE ESTA ARQUITECTURA ES QUE EL ROUTER SEA CAPAZ DE PROCESAR TODO EL TRÁFICO DE DATOS QUE RECIBA, YA QUE DEBE FILTRAR TANTO LOS DATOS DE LA RED INTERNA COMO LOS DE LA RED EXTERNA.

5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

UTILIZACIÓN DEL HOST BASTION COMO ROUTER EXTERNO

CUANDO SE QUIEREN CONECTAR DOS REDES CON INTERFACES DE RED DISTINTAS, SE PUEDE UTILIZAR EL HOST BASTION COMO ROUTER EXTERNO.

EL HOST BASTION EJECUTA A LA VEZ EL FILTRADO DE PAQUETES DE DATOS Y LOS SERVICIOS PROXY.

EL PRINCIPAL INCONVENIENTE DE ESTA CONFIGURACIÓN ES SU ELEVADO COSTE PARA EL DESEMPEÑO DE LOS SERVICIOS PROXY. ADEMÁS, AUNQUE NO SE EXPONE A VULNERABILIDADES, SÍ ES CIERTO QUE EL HOST BASTION ESTÁ MÁS EXPUESTO A POSIBLES ATAQUES, AL NO HABER NINGUNA BARRERA ENTRE LA RED LOCAL Y ESTE.

CONTENIDOS

1. INTRODUCCIÓN. PRINCIPIOS GENERALES DE CORTAFUEGOS
2. COMPONENTES DE UN CORTAFUEGOS DE RED
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
4. ARQUITECTURAS DE CORTAFUEGOS DE RED
5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

RESUMEN

UN **CORTAFUEGOS** ES UN SISTEMA COMPUESTO POR UNO O VARIOS DISPOSITIVOS CUYA FUNCIÓN PRINCIPAL ES LA SEPARACIÓN ENTRE LA RED LOCAL DE UN SISTEMA DE INFORMACIÓN Y LA RED EXTERIOR, DE MODO QUE SE IMPIDA LA ENTRADA DE ATAQUES Y SE INCREMENTE LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN.

EL **PERÍMETRO DE SEGURIDAD** ES EL ESPACIO PROTEGIDO POR EL CORTAFUEGOS, MIENTRAS QUE **LA ZONA DE RIESGO** ES LA RED FRENTE A LA QUE SE PROTEGE DICHO PERÍMETRO DE SEGURIDAD.

PARA DETERMINAR LA CONFIGURACIÓN DE UN CORTAFUEGOS, DEBEN TENERSE EN CUENTA TRES CARACTERÍSTICAS FUNDAMENTALES: **LA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN, LA MONITORIZACIÓN DEL CORTAFUEGOS Y LA ECONOMÍA** Y PRESUPUESTO QUE SE ESTÁ DISPUESTO A ASUMIR.

RESUMEN

ATENDIENDO A ESTAS CARACTERÍSTICAS, SE PUEDEN IMPLANTAR DISTINTOS TIPOS DE CORTAFUEGOS SEGÚN SU UBICACIÓN Y FUNCIONALIDAD.

LOS **ROUTERS CON FILTRADO DE PAQUETES** SON CORTAFUEGOS QUE FILTRAN LOS PAQUETES DE DATOS ENTRANTES ATENDIENDO A UNA SERIE DE REGLAS PREDEFINIDAS. LOS **GATEWAYS O PASARELAS A NIVEL DE APLICACIÓN** ANALIZAN EL TRÁFICO ATENDIENDO A LOS SERVICIOS SOLICITADOS (PERMITIENDO EL ACCESO SOLO A DETERMINADAS APLICACIONES) Y **LOS GATEWAYS O PASARELAS A NIVEL DE CIRCUITO** REDIRIGEN LOS PAQUETES DE DATOS UNA VEZ VALIDADA LA CONEXIÓN.

LA ELECCIÓN DE IMPLANTAR UN TIPO DE CORTAFUEGOS U OTRO DEPENDERÁ DE LAS PREFERENCIAS DE SEGURIDAD DE LA ORGANIZACIÓN, ADEMÁS DEL VALOR DE LOS ACTIVOS Y DE LA INFORMACIÓN QUE SE DESEA PROTEGER.

RESUMEN

SI ENTRE ESTOS TIPOS DE CORTAFUEGOS NO HAY NINGUNO QUE SE ADAPTE LOS SUFICIENTE A LOS OBJETIVOS DE LA ORGANIZACIÓN, SE PUEDEN IMPLANTAR CORTAFUEGOS CON ARQUITECTURAS MÁS COMPLEJAS, COMO LOS CORTAFUEGOS **DUAL-HOMED HOST**, LOS CORTAFUEGOS **SCREENED HOST** Y LAS ARQUITECTURAS **SCREENED SUBNET** (QUE UTILIZAN ZONA DESMILITARIZADA COMO MEDIDA ADICIONAL DE PROTECCIÓN).

ESTO ES TODO