

T5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

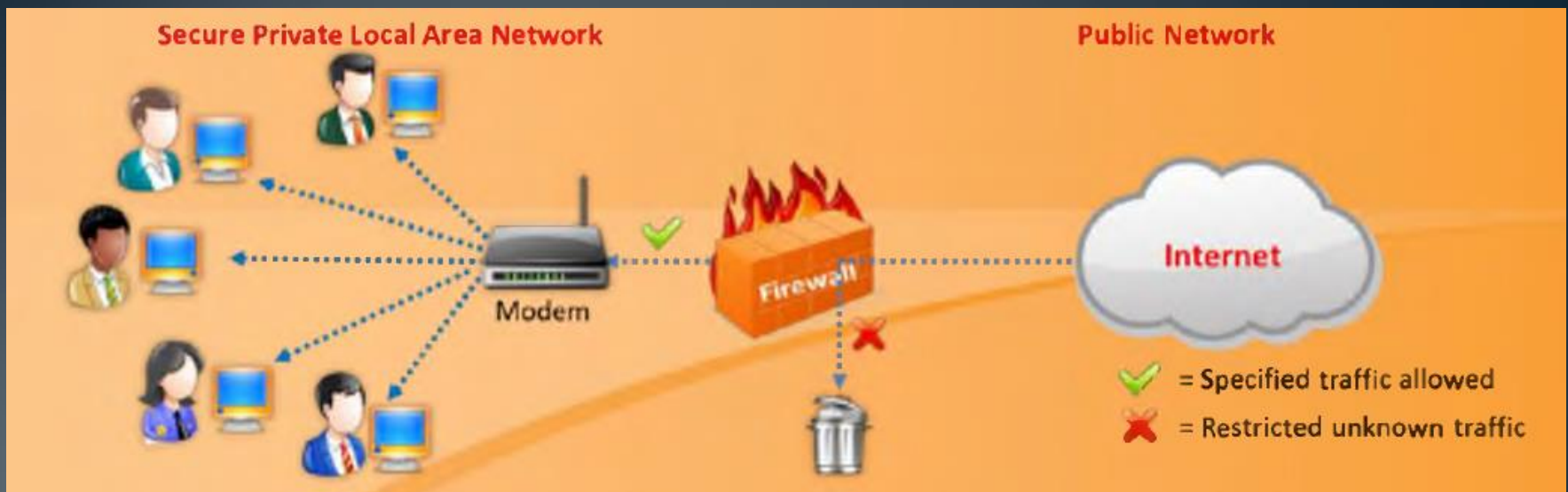


Apartados del BOE

- Principios generales de cortafuegos
- Componentes de un cortafuegos de red
- Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- Arquitecturas de cortafuegos de red
- Otras arquitecturas de cortafuegos de red

Firewall

- Los Firewalls son un conjunto de programas situados en la puerta de enlace de la red y protege a los recurso de una red privada de usuarios de otras redes
- Los firewall poseen un conjunto de herramientas que monitorizan el flujo del tráfico entre redes
- Un firewall situado a nivel de red y trabajando en estrecha colaboración con un router, filtra todos los paquetes de red para determinar cuales deben atravesarla para llegar a su destino
- Un firewall está instalado a menudo lejos del resto de la red de modo que ninguna solicitud entrante puede obtener directamente a un recurso de red privada.
- Si se ha configurado correctamente, los sistemas de un lado del firewall están protegidos de los sistemas en el otro lado del firewall.



- Un firewall es un sistema de detección de intrusiones
- Puede ser configurado para restringir tráfico de POP y SNMP
- Pueden ser configurados para comprobar el tráfico de entrada y enviarlo a un punto denominado «choke point» (cuello de botella) donde se realiza una auditoría de seguridad
- También verifican el tráfico de entrada y de salida a través de reglas del cortafuegos



- Todos los intentos de iniciar sesión en la red se identifican para la auditoría.
- Los intentos no autorizados pueden ser identificados mediante la incorporación de una alarma que se activa cuando un usuario no autorizado intenta iniciar sesión .
- Los cortafuegos pueden filtrar paquetes basados en la dirección y el tipo de tráfico.
- Identifican la fuente , las direcciones de destino , y los números de puerto durante el filtrado de direcciones, y se identifican los tipos de tráfico de red cuando el filtrado de protocolos.
- Los cortafuegos pueden identificar el estado y las características de los paquetes de datos .

Arquitectura de un firewall

- La arquitectura de un firewall se compone de los siguientes elementos:
 - Bastion host
 - Screened subnet
 - Multi-homed firewall

- Bastion Host (servidor bastión)
 - Está diseñado con el propósito de defenderse frente a los ataques.
 - Actúa de mediador entre las redes internas y las externas
 - Un Bastion Host es un sistema informático diseñado y configurado para proteger los recursos de la red de los ataques
 - El tráfico entre y sale de la red a través de un firewall, cuenta con 2 interfaces
 - Interfaz pública directamente conectada a internet
 - Interfaz privada conectada a la intranet



- **Screened subnet**

- Una Screened Subnet es una arquitectura de red que usa un único firewall y 3 interfaces de red
 1. Para conectarse a Internet
 2. Para conectarse a la DMZ (Red desmilitarizada)
 3. Para conectarse con la intranet
- La gran ventaja que se tiene con esta arquitectura es que se separa la red DMZ e Internet de la Intranet, por lo que si el Firewall está comprometido, el acceso a la intranet no sería posible
 - La Screened Subnet o DMZ contiene los nodos que ofrecen servicios como correo, ftp, http.
 - La zona pública está directamente conectada a Internet y no tiene nodos controlados por la organización.
 - La zona privada tiene los sistemas que los usuarios de internet no podrían tener acceso.



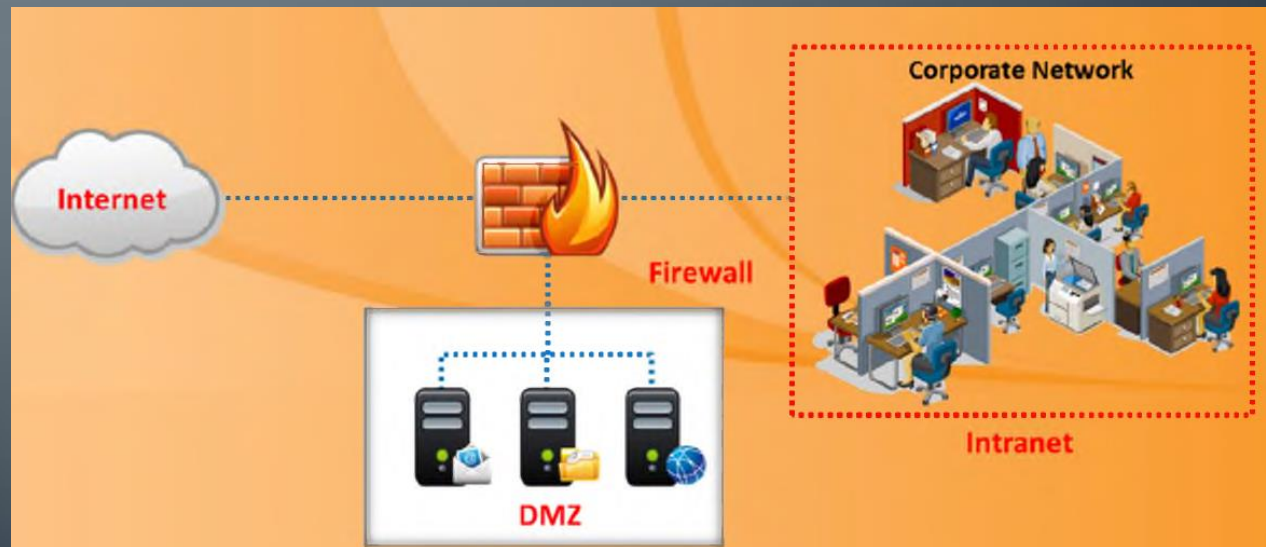
- **Multi-homed firewall**

- Un multi-homed firewall generalmente se refiere a 2 o más redes.
- Cada interfaz está conectada de forma independiente a segmentos de red lógicos y físicos
- Se utiliza para incrementar la eficiencia y la fiabilidad de una red IP
- En este caso, más de 3 interfaces están presente y permiten subdividir aún más los sistemas basados en los objetivos específicos de seguridad de la organización

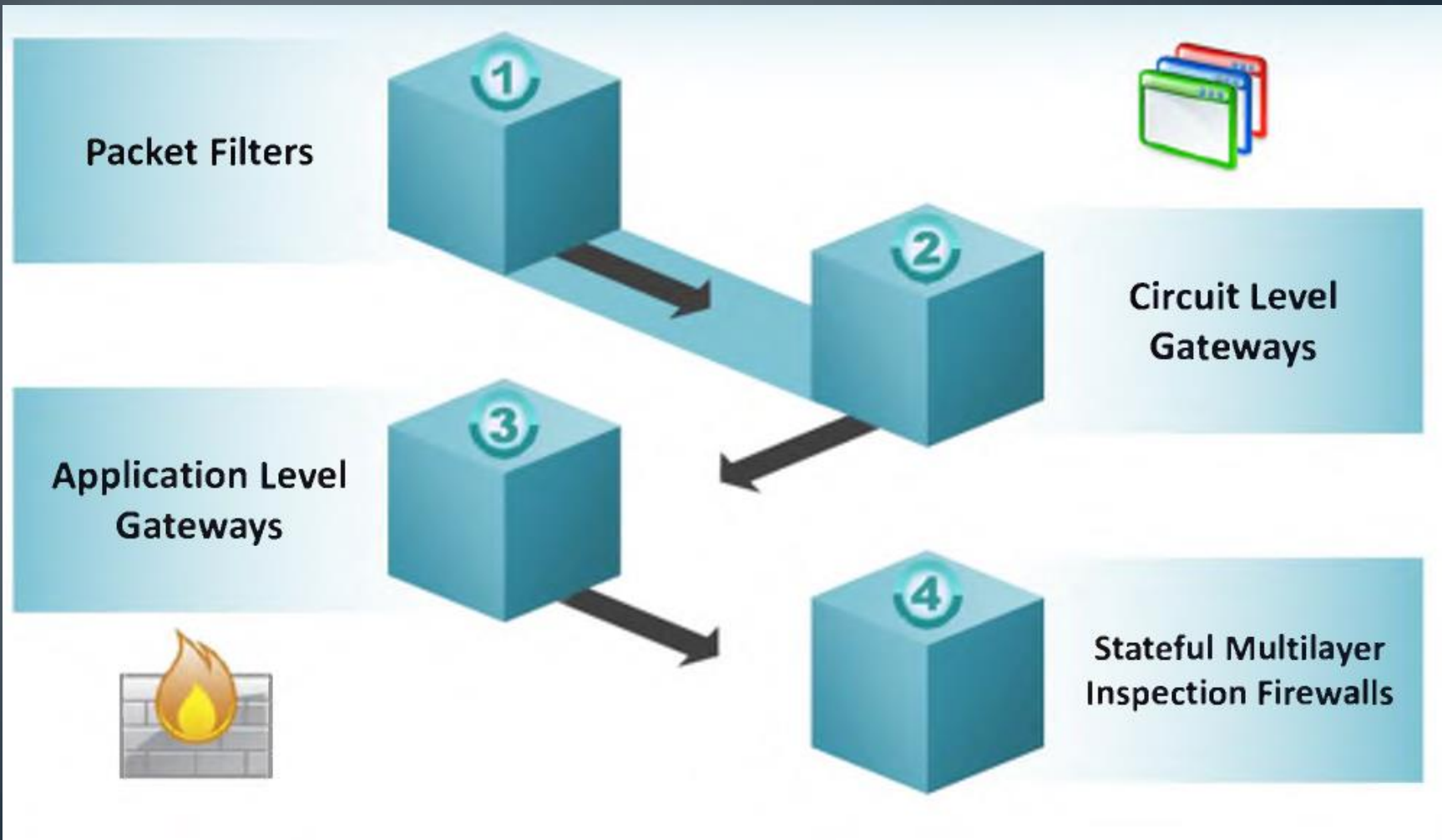


Zona desmilitarizada DMZ

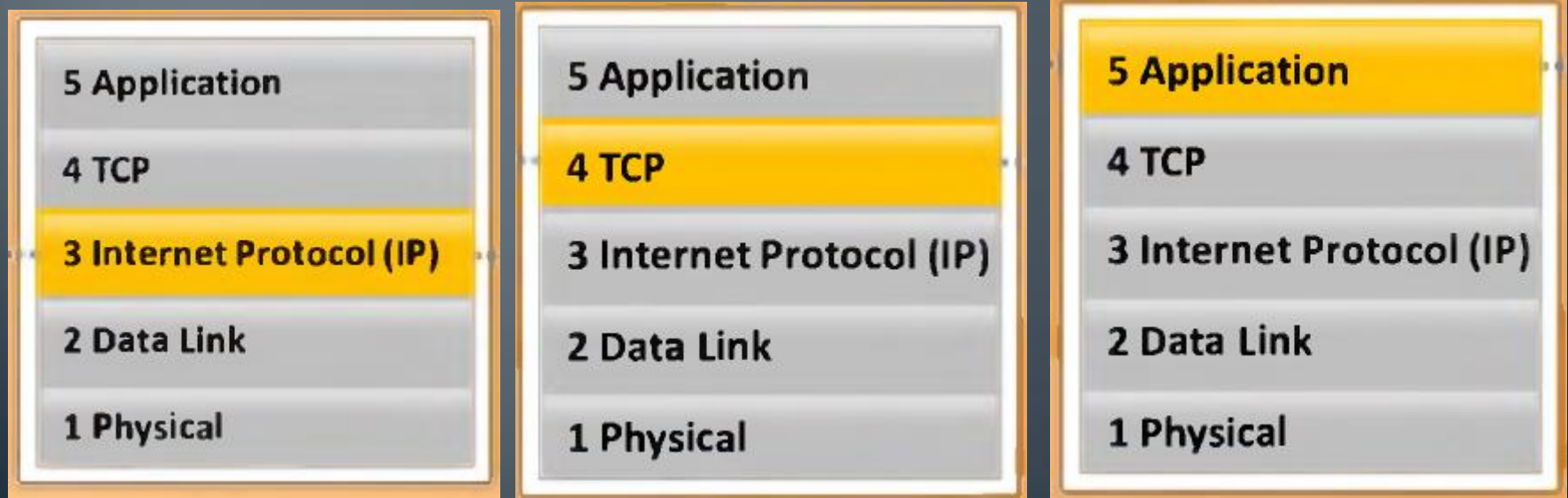
- La DMZ es un host o una red colocada como una red neutral entre la red interna (privada) de una empresa y la externa (pública) para evitar que un usuario desde fuera tenga acceso a los datos privado de la compañía
- Se utiliza como una red intermedia entre la red interna segura y la red insegura de internet



Tipos de Firewall



- Un firewall es un dispositivos HW o programa SW que se utiliza en un sistema para evitar que la información maliciosa lo atraviese y permitiendo sólo la información aprobada.
- Se clasifican principalmente en 4 tipos:
 - Packet filters (filtrado de paquetes)
 - Circuit-level gateways (pasarelas a nivel de circuito)
 - Application-level gateways (pasarelas a nivel de aplicación)
 - Stateful multilayer inspection firewalls (firewalls de inspección dinámica multicapa)



• Packet Filtering Firewall

- Este tipo de Firewall investiga cada paquete que pasa a través de él de forma individualizada y toma la decisión de si debe pasar el paquete o eliminarlo.
- Como se puede deducir de su nombre, los firewalls basados en el filtrado de paquetes, se concentran en paquetes individuales y analizan la información de cabecera y hacia donde se dirigen

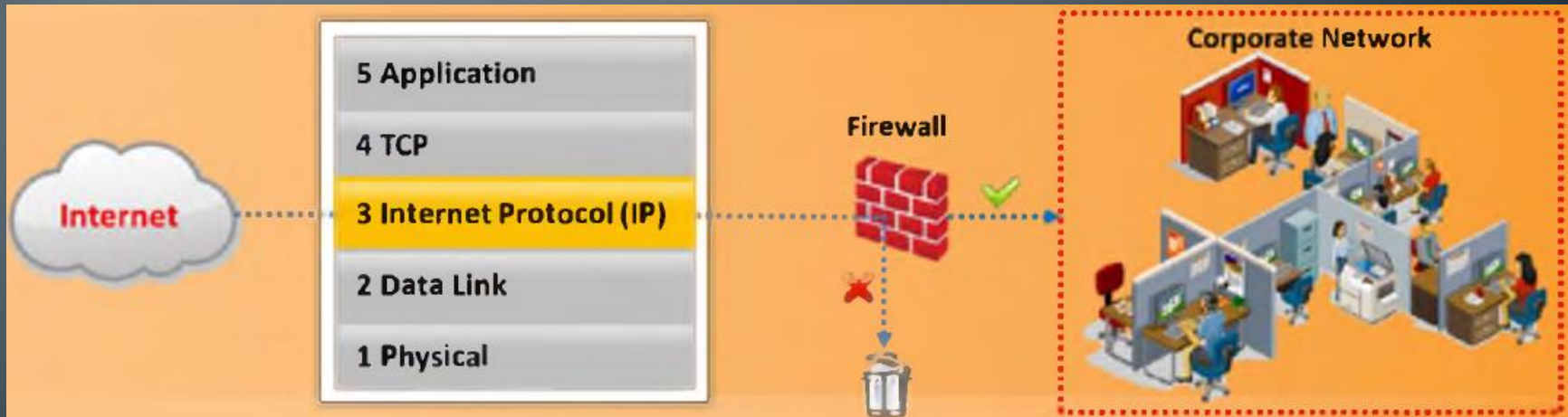


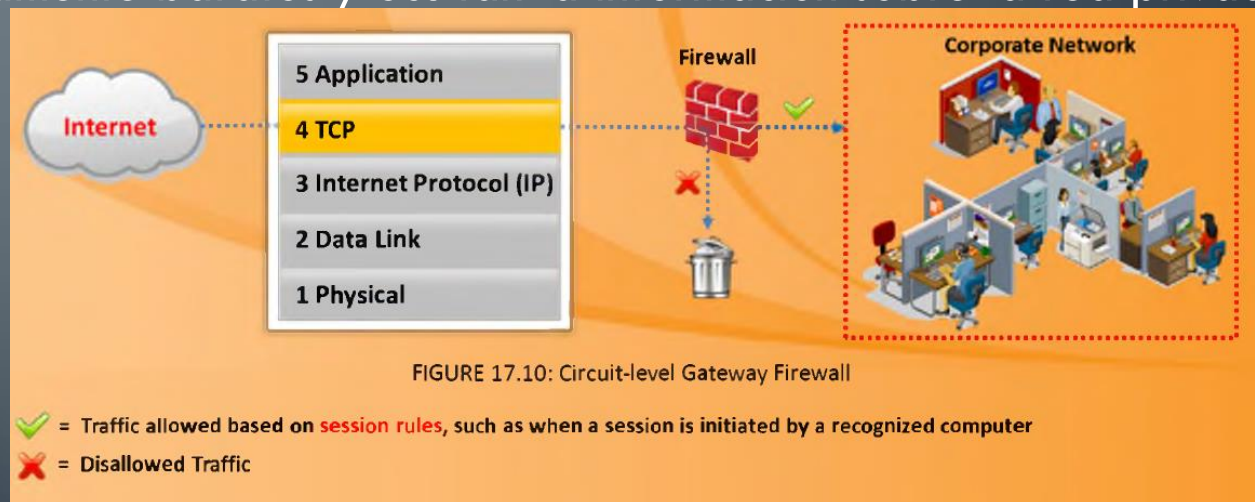
FIGURE 17.9: Packet Filtering Firewall

- ✓ = Traffic allowed based on source and destination **IP address, packet type, and port number**
- ✗ = Disallowed Traffic

- Estos firewall toman la decisión en base a la siguiente información:
 - Dirección IP de origen
 - Dirección IP de destino
 - Puerto TCP/UDP de origen
 - Puerto TCP/UDP de destino
 - Bits del código TCP
 - Protocolo en uso
 - Rumbo de los paquetes
 - Interfaz

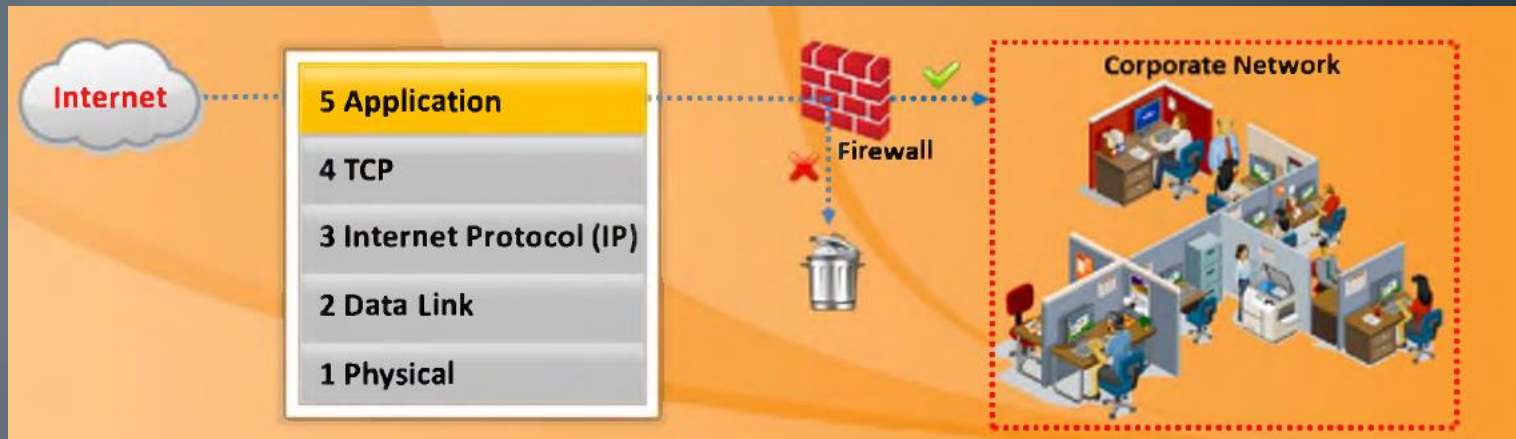
Circuit-Level Gateway

- El firewall trabaja en la capa de sesión del modelo OSI, o también denominada TCP/IP
- Permite los datos entre las redes sin verificarla.
- Bloquea los paquetes entrantes en el host, pero permite que el tráfico pase a través de él
- La información pasada a equipos remotos a través de un Circuit-level Gateway aparece como originado por el Gateway (puerta de enlace predeterminada), funciona como si fuera un proxy.
- Para detectar si una sesión solicitada es válida, se comprueba el TCP handshaking entre los paquetes.
- Son relativamente baratos y ocultan la información sobre la red privada que protegen



- **Application-level Firewall**

- Este tipo de Firewall se concentra en la capa de Aplicación en lugar de sólo los paquetes
- Estos Firewalls analizan la información de la solicitud para tomar decisiones sobre si procede o no transmitir los paquete



- **Stateful Multilayer Inspection Layer**

- Aquí se combinan los aspectos de los 3 tipos de firewall
- Filtran los paquetes en la capa de red, determinan si los paquetes de sesión son legítimos y evalúan el contenido de los paquetes en la capa de aplicación
- Estos firewalls proporcionan lo mejor del filtrado de paquetes y el filtrado a nivel de aplicación
- Los Cisco Pix, tienen esta funcionalidad

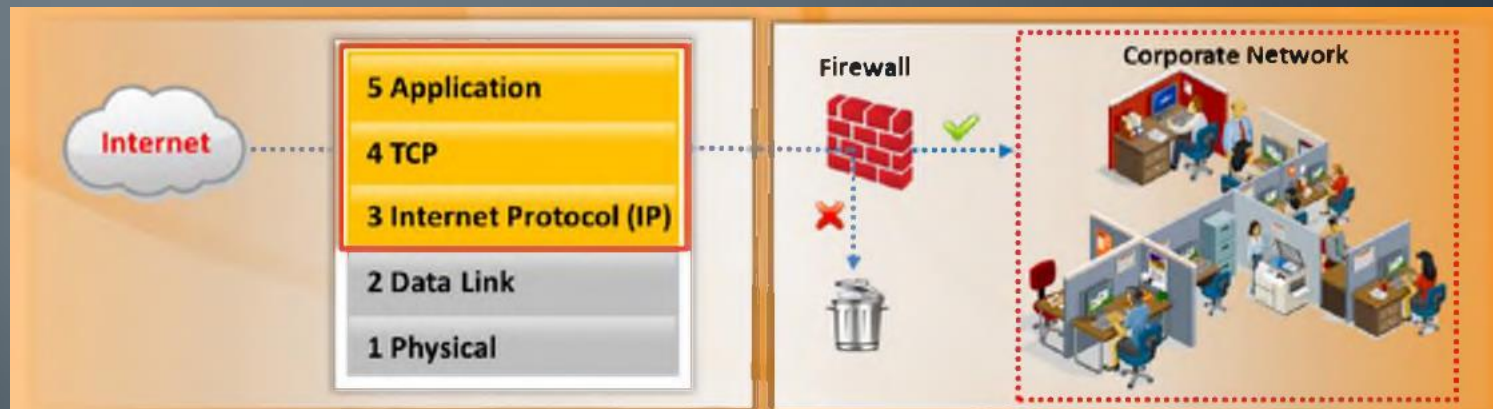


FIGURE 17.12: Stateful Multilayer Inspection Firewall

- ✓ = Traffic is filtered at three layers based on a wide range of the **specified application, session, and packet filtering rules**
- ✗ = Disallowed Traffic

Identificación de Firewalls

- Hay varias técnicas para saber si hay un Firewall en una red
 - Firewall scanning
 - Firewalking
 - Banner grabbing

- Port Scanning

- Escanear sistemáticamente los puertos de un equipo que se conoce como el escaneo de puertos.
- Los atacantes utilizan estos métodos para identificar las posibles vulnerabilidades a fin de comprometer una red. Es uno de los métodos más populares que los atacantes utilizan para la investigación de los puertos utilizados por las víctimas. Una herramienta que puede utilizarse para la exploración de puertos es Nmap.
- Un escaneo de puertos ayuda a que el atacante encontrar qué puertos están disponibles (es decir, lo que el servicio pudiera estar escuchando a un puerto); que consiste en enviar un mensaje a cada puerto, uno a la vez.
- Por ejemplo:
 - [Check Point's Firewall-1](#) escucha en los puertos TCP 256, 257, 258, y 259
 - [Microsoft Proxy Server](#) normalmente escucha en los puertos TCP 1080 y 1745.

- Firewalking

- Es un método utilizado para recopilar información sobre las redes remotas que están detrás de los cortafuegos
- Firewalk es el SW más conocido usado para el Firewalking, tiene 2 fases
 - Fase de descubrimiento
 - Fase de escaneo/exploración

- Banner Grabbing

- Los Banners son mensajes que envían los servicios de red durante la conexión del servicio. Anuncian que el servicio que se está ejecutando en el sistema. Esta técnica lo utilizan los atacantes para detectar el sistema operativo de una máquina.
- Esta técnica permite descubrir los servicios que corren a través de los Firewalls.
- Los 3 servicios principales que envían estos banners son:
 - FTP
 - TELNET
 - Servidores Web

```
C:\>telnet www.corleone.com 80
```

```
HTTP/1.0 400 Bad Request
```

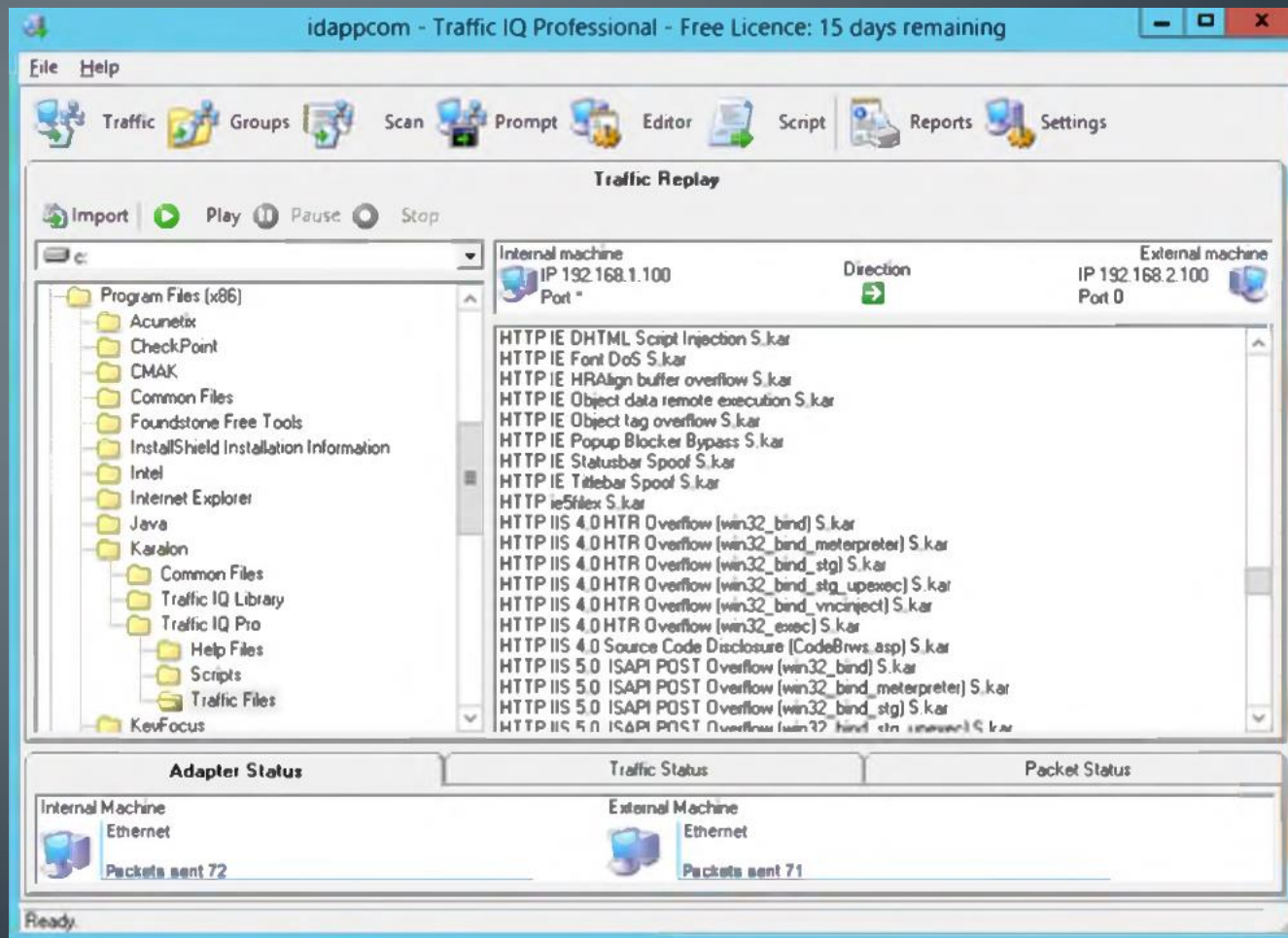
```
Server: Netscape - Commerce/1.1.2
```

Firewalls... que no son de Windows

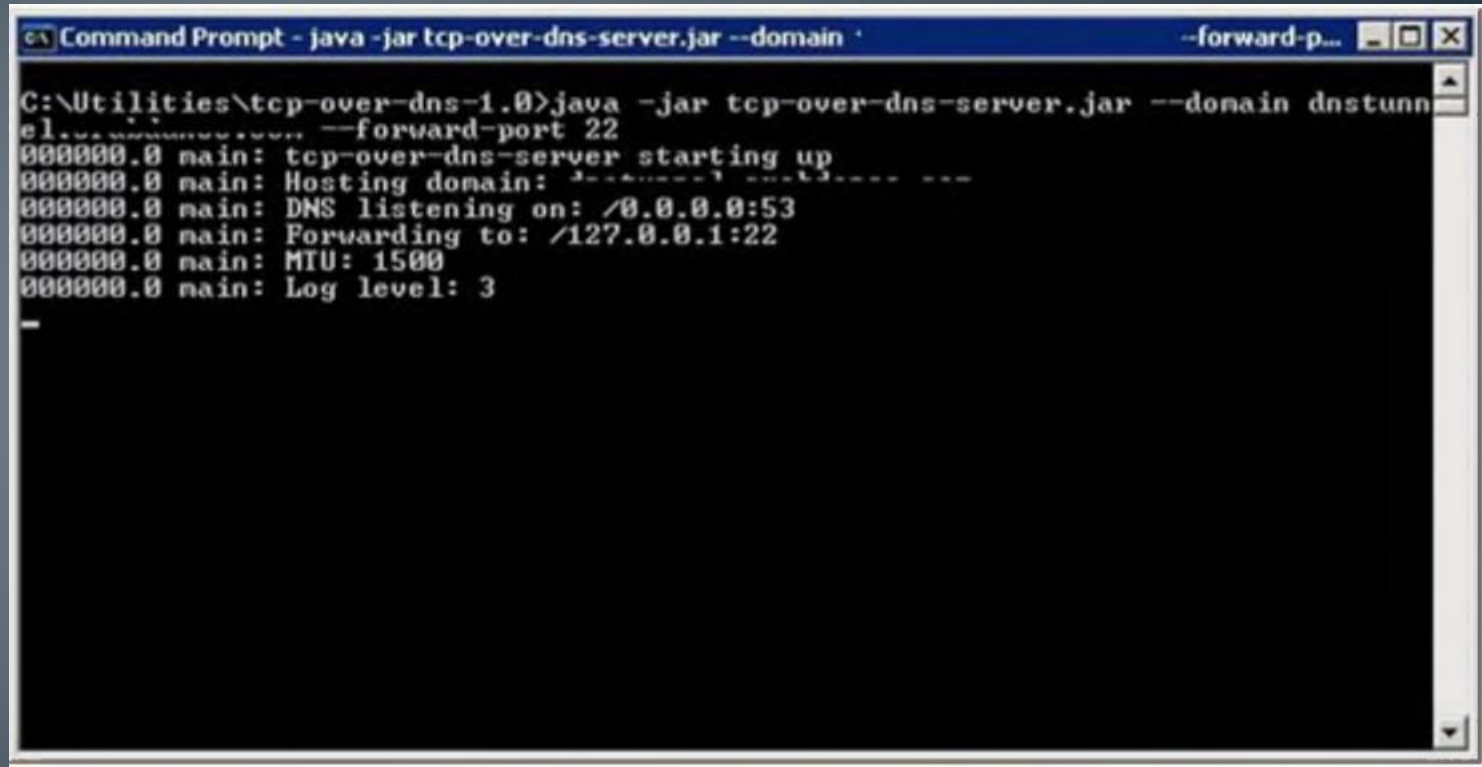
- Check Point Firewall Software Blade <http://www.checkpoint.com>
- eScan Enterprise <http://www.escanav.com>
- Jetico Personal Firewall <http://www.ietico.com>
- Outpost Security Suite <http://free.agnitum.com>
- Novell BorderManager <http://www.novell.com>
- Firewall UTM <http://www.esoft.com>
- Sonicwall <http://www.tribecaexpress.com>
- Comodo Firewall <http://personalfirewall.comodo.com>
- Online Armor <http://www.online-armor.com>
- FortiGate-5101C <http://www.fortinet.com>

Herramientas para evadir Firewalls

- Traffic IQ Professional → <http://idappcom.com>



- Tcp-over-dns



```
Command Prompt - java -jar tcp-over-dns-server.jar --domain '
--forward-p...
C:\Utilities\tcp-over-dns-1.0>java -jar tcp-over-dns-server.jar --domain dnstunn
el.dnstunnel.com --forward-port 22
000000.0 main: tcp-over-dns-server starting up
000000.0 main: Hosting domain: dnstunnel.dnstunnel.com
000000.0 main: DNS listening on: /0.0.0.0:53
000000.0 main: Forwarding to: /127.0.0.1:22
000000.0 main: MTU: 1500
000000.0 main: Log level: 3
-
```



Snare Agent for Windows

<http://www.intersectalliance.com>



AckCmd

<http://ntsecurity.nu>



Tomahawk

<http://tomahawk.sourceforge.net>



Your Freedom

<http://www.your-freedom.net>



Atelier Web Firewall Tester

<http://www.atelierweb.com>



Freenet

<https://freenetproject.org>



GTunnel

<http://gardennetworks.org>



Hotspot Shield

<http://www.anchorfree.com>



Proxifier

<http://www.proxifier.com>



Vpn One Click

<http://www.vpnoneclick.com>