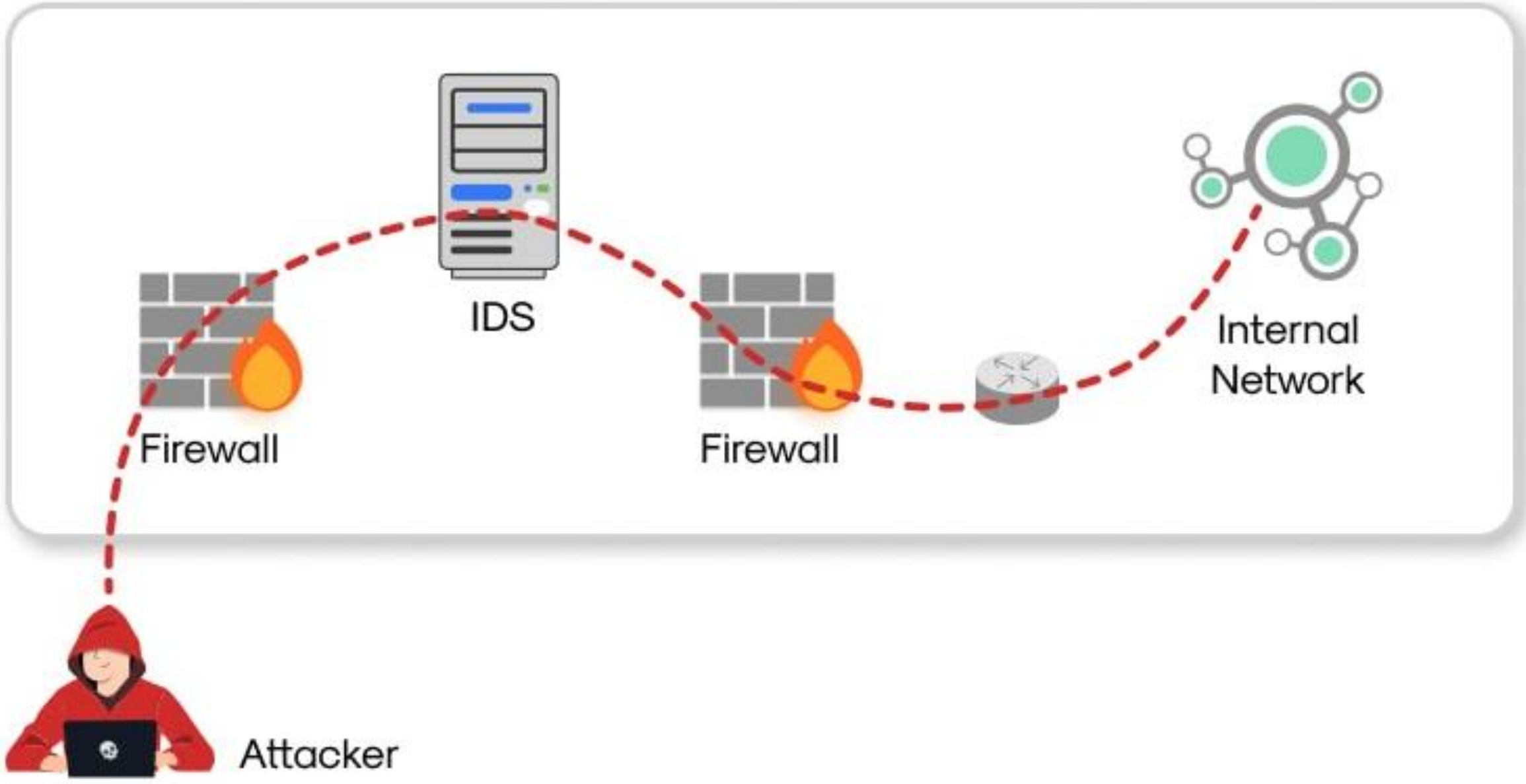
Evasión de Firewall y sistemas de detección

Advanced Evasion Technique



PERSPECTIVAS DE RECONOCIMIENTO PASIVO: DISPOSITIVO OBJETIVO

DATOS PÚBLICOS Y OSINT (Inteligencia de Fuentes Abiertas)

- Ofertas de empleo (ej., "Se busca Admin Checkpoint")
- Asociaciones con proveedores en notas de prensa
- Perfiles de LinkedIn del personal con habilidades en cortafuegos

Perspectiva: Dependencia organizativa de proveedores de seguridad especificos

Perspectiva: La estructura de infraestructura sugiere seguridad en la pasarela

REGISTROS DNS Y WHOIS

- Registros MX apuntando a pasarelas de correo seguras
- Registros NS alojados por proveedores de seguridad (ej., Cloudflare)
- Existencia de subdominios como "vpn", "gw" o "firewall"

DISPOSITIVO OBJETIVO

OBSERVACIÓN DE TRÁFICO PASIVO (Broadcast/Multicast)

- Peticiones ARP para direcciones IP de pasarela
- Anuncios de protocolos de enrutamiento (ej., "hello" de OSPF desde dispositivo de seguridad)
- OUIs de direcciones MAC de proveedores específicos en tramas de difusión

Perspectiva: Visibilidad L2/L3 revela hardware de seguridad en el segmento

Perspectiva: Comportamiento registrado indica filtrado a lo largo del tiempo

DATOS DE ESCANEO HISTÓRICO (Shodan, Censys, Wayback)

- Banners pasados mostrando "Prohibido" o mensajes de cortafuegos
- Historial de puertos bloqueados o servicios filtrados en IP objetivo
- Páginas de error en caché mencionando políticas de seguridad

PERSPECTIVAS DE RECONOCIMIENTO ACTIVO: DETECTAR UN FIREWALL

SISTEMA ATACANTE

ESCANEO DE PUERTOS (Nmap)

Sonda: Escaneos SYN, ACK, UDP

Perspectiva: Estado "Filtrado"

Perspectiva: Estado "Filtrado"

Sin respuesta (Caída silenciosa): Regla del cortafuegos descarta paquete.

ICMP Inalcanzable (Admin. Prohibido): Cortafuegos rechaza activamente (Tipo 3, Cód. 13).

TRACEROUTE Y ANÁLISIS DE RUTA

Sonda: Paquetes UDP/ICMP (TTL incrementado)

Perspectiva: La ruta se detiene abruptamente

Salto antes del tiempo de espera suele ser la interfaz externa del cortafuegos, bloqueando más sondas.

DISPOSITIVO OBJETIVO

FIREWALL / PASARELA DE SEGURIDAD

FIREWALKING (Traceroute Avanzado)

Sonda: Traceroute con TTL justo tras el cortafuegos, puertos específicos

Perspectiva: Mapeo de Reglas

TTL Excedido (Tipo 11): Puerto pasa a través del cortafuegos.

Tiempo de espera: Puerto bloqueado por regla del cortafuegos.

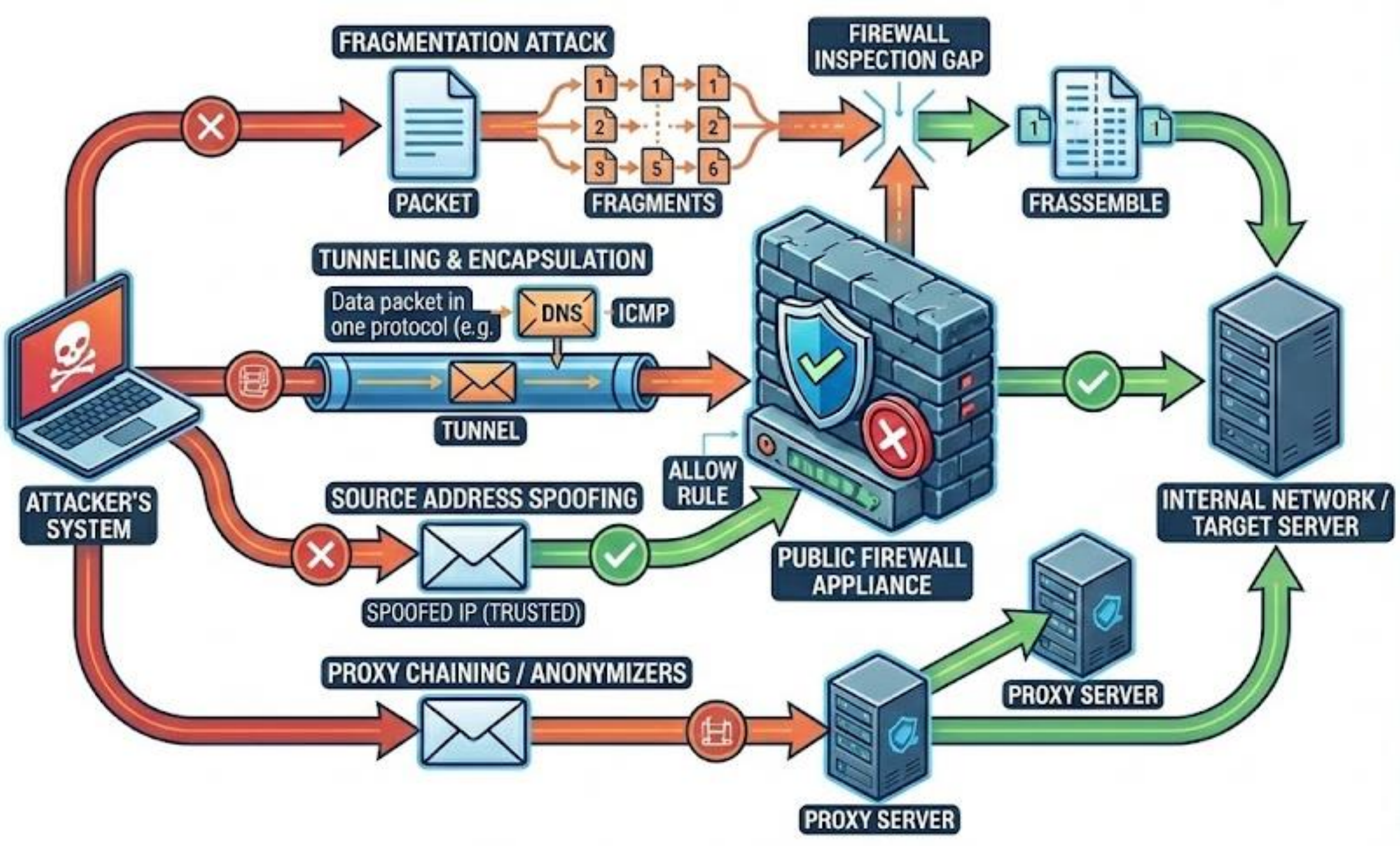
CREACIÓN DE PAQUETES (Scapy)

Sonda: Paquetes TCP FIN, NULL, XMAS

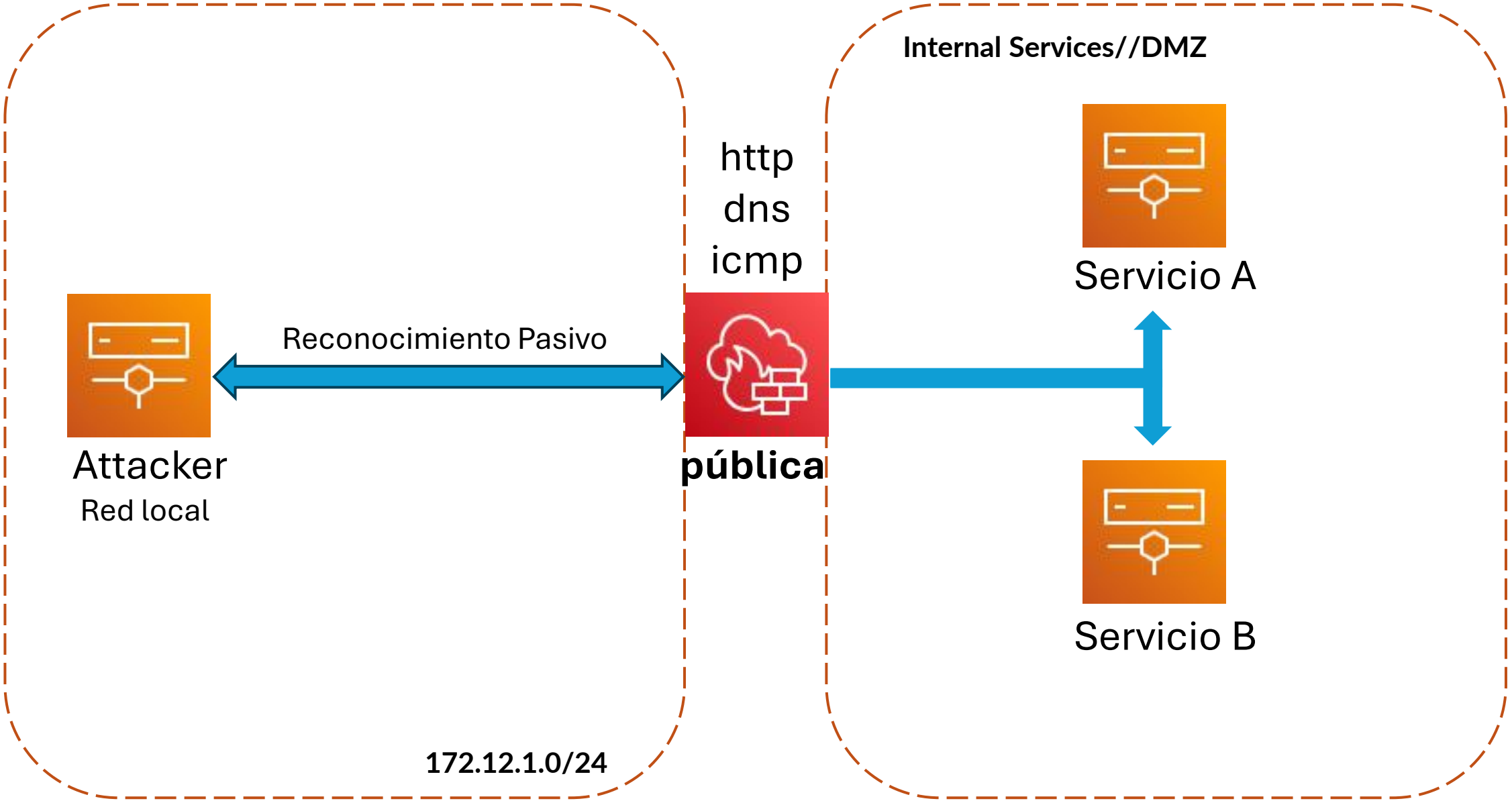
Perspectiva: Análisis de Estado

Sin respuesta (a estas flags): Indica un cortafuegos con estado rastreando la conexión y descartando paquetes fuera de estado.

PERSPECTIVA GLOBAL: ESTADOS 'FILTRADOS' CONSISTENTES Y BLOQUEO DE RUTA CONFIRMAN LA PRESENCIA DEL FIREWALL


FRAGMENTATION ATTACK
PACKET
FRAGMENTS
FIREWALL INSPECTION GAP
FRASSEMBLE
TUNNELING & ENCAPSULATION
Data packet in one protocol (e.g.
DNS
ICMP
TUNNEL
ATTACKER'S SYSTEM
ALLOW RULE
SOURCE ADDRESS SPOOFING
SPOOFED IP (TRUSTED)
PUBLIC FIREWALL APPLIANCE
INTERNAL NETWORK / TARGET SERVER
PROXY CHAINING / ANONYMIZERS
PROXY SERVER
PROXY SERVER

Laboratorio & Herramientas


Internal Services//DMZ
http
dns
icmp
Servicio A
Reconocimiento Pasivo
Attacker
Red local
pública
Servicio B
172.12.1.0/24

Código

```
#Basic Scan
nmap -Pn -sS 172.16.1.73
#Fragmented Packets
nmap -Pn -f 172.16.1.73
#Source Port Spoofing
nmap -Pn --source-port 53 172.16.1.73
#Time IDS evasion
nmap -Pn -T0 172.16.1.73
#Scan bypassed
nmap -Pn -A 172.16.1.74
```