# Seguridad Informática

## Tema 8 – Contramedidas de red/protocolo

Universidad Rey Juan Carlos

Isaac Lozano Osorio **isaac.lozano@urjc.es**

16/04/2024

# Índice

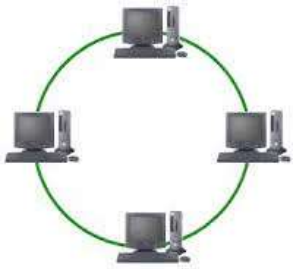
Universidad Rey Juan Carlos

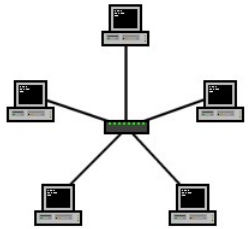
- **Introducción.**
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- Resumen.

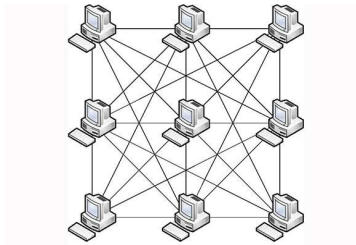
# Introducción

Universidad Rey Juan Carlos

- En la actualidad las topologías de red de las empresas tienen formas muy diferentes:
  - Bus, anillo, estrella, malla, etc.







- La topología debe incorporar las contramedidas de red básicas.

- Proteger el perímetro de la organización y segmentar las diferentes redes internas.

- En función de su grado de interconexión con el mundo exterior y el nivel de seguridad deseado.

# Índice



- Introducción.
- **Firewalls y DMZs.**
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- Resumen.

# Firewalls y DMZs

Universidad Rey Juan Carlos

- La separación/protección de redes se puede implementar con diferentes mecanismos y dispositivos:

| | | |
|---|---|---|
| Tablas de enrutamiento | Routers con listas de control de acceso | Switches inteligentes |
| Firewalls | DMZs | Diodo de datos |

# Firewalls y DMZs

Universidad Rey Juan Carlos

- Un firewall es un dispositivo hardware/software que tiene como objetivo proteger una red de otras redes a las cuales está conectada.
  - Por lo tanto, se debe situar en un punto en el que recoja todo el tráfico entrante y saliente de la red que deben proteger.

- No basta con la presencia del firewall para garantizar la protección de la red, este dispositivo debe estar correctamente configurado.
  - Un error muy habitual es dejar las configuraciones por defecto del dispositivo.

# Firewalls y DMZs

Universidad Rey Juan Carlos

- Su labor es diferenciar las conexiones permitidas de aquellas consideradas sospechosas.

- Un firewall suele funcionar de la siguiente manera:
  - Monitorizando y controlando el tráfico que fluye hacia/desde la red protegida.
  - Aplicando filtros que buscan determinados patrones.
    - Se compara cada unidad de información (paquete, segmento, datagrama o trama) con una serie de reglas predefinidas para ver si encaja en alguna.
  - Aplicando reglas de filtrado que especifican las acciones que deben llevarse a cabo cuando se encuentran estos patrones.

# Firewalls y DMZs

Universidad Rey Juan Carlos

- Los firewalls se pueden clasificar dependiendo de su nivel de funcionamiento:
  - **Firewall de filtrado de paquetes**: se basan en analizar las cabeceras de las unidades de información para filtrar por puerto, dirección, etc.
  - **Stateful firewall**: en base a las políticas de privacidad y del estado de la conexión permitirá, o no, las conexiones.
  - **Proxy firewall**: se basan en un análisis a un nivel más alto que tiene en cuenta los parámetros específicos de cada aplicación.
  - **Firewalls DPI**: pueden filtrar por protocolos/tipos de archivos específicos, como SOAP o XML por ejemplo.

# Firewalls y DMZs

Universidad Rey Juan Carlos

- **Firewall de filtrado de paquetes**: toman decisiones basándose en direcciones de red, puertos o protocolos.
  - Son muy rápidos, porque el procesamiento es muy sencillo.
  - Por lo general, suelen abrirse los puertos manualmente (ACL – *Access Control List*)
  - Reenvían todo el tráfico que fluya en un puerto aprobado.

| Regla | Acción | IP origen | IP destino | Puerto origen | Puerto destino | Protocolo |
|---|---|---|---|---|---|---|
| 1 | Aceptar | 192.168.1.2 | 213.145.2.2 | Any | 25 (SMTP) | TCP |
| 2 | Aceptar | 192.168.1.0/24 | Cualquiera | Any | 80 (HTTP) | TCP |
| 3 | Aceptar | Cualquiera | 192.168.1.4 | Any | 80 (HTTP) | TCP |

# Firewalls y DMZs

Universidad Rey Juan Carlos

- **Stateful firewall** : otra alternativa consiste en crear algún tipo de firewall cuyo comportamiento sea dinámico: *stateful packet inspection* (SPI).
  - Los puertos se abren y se cierran de manera dinámica.
  - Estos firewalls tienen una tabla con detalles como las direcciones IP, los puertos que participan en una conexión, y los números de secuencia.
  - Es un firewall, por lo general, más seguro que el anterior, pero hay que tener en cuenta sus limitaciones.

# Firewalls y DMZs

Universidad Rey Juan Carlos

- **Proxy firewall**: es un dispositivo intermedio entre la red interna y externa que examina y registra todo el tráfico de entrada y salida.
  - Si desde la red interna se solicita un servicio a la red externa, la petición llega al proxy que la analiza, y será el proxy el que haga la petición al servicio.
  - Permite controlar los servicios a los que se accede.
  - Pero se pueden crear cuellos de botella, y/o que el rendimiento de esos servicios decaiga.

# Firewalls y DMZs

Universidad Rey Juan Carlos

- **Firewalls Deep Packet Inspection (DPI)**: realizan un análisis de los datos que se están enviando a nivel de aplicación.
  - Al realizar ese análisis, toma decisiones en función del contenido del paquete y de las reglas definidas por la compañía, el administrador de la red o el ISP.
  - DPI se utiliza en firewall con IDS.
  - Usos legítimos:
    - Permite detectar virus, gusanos, spyware, u otras formas de malware que se esté mandando por la red.
    - También puede detectar envíos masivos de datos.

# Firewalls y DMZs



- También se pueden clasificar en función de las reglas de filtrado que aplican:
  - Políticas permisivas.
  - Políticas restrictivas.
- O dependiendo del tipo de activo que protegen. Por ejemplo, firewall de perímetro o red (hardware), pero también hay firewalls de sistema o nodos (software).

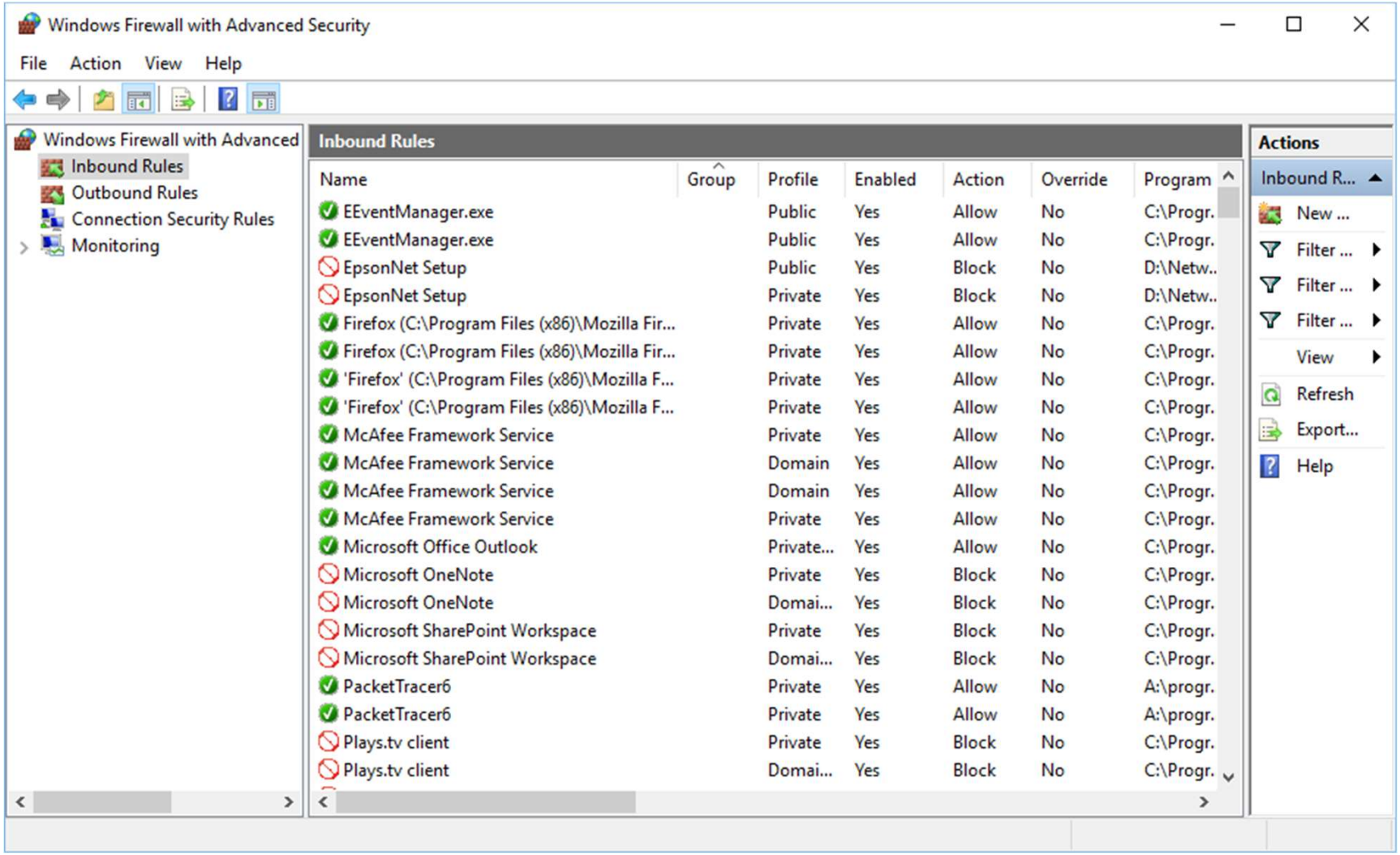
COMODO Firewall


Avast

kaspersky

# Firewalls y DMZs

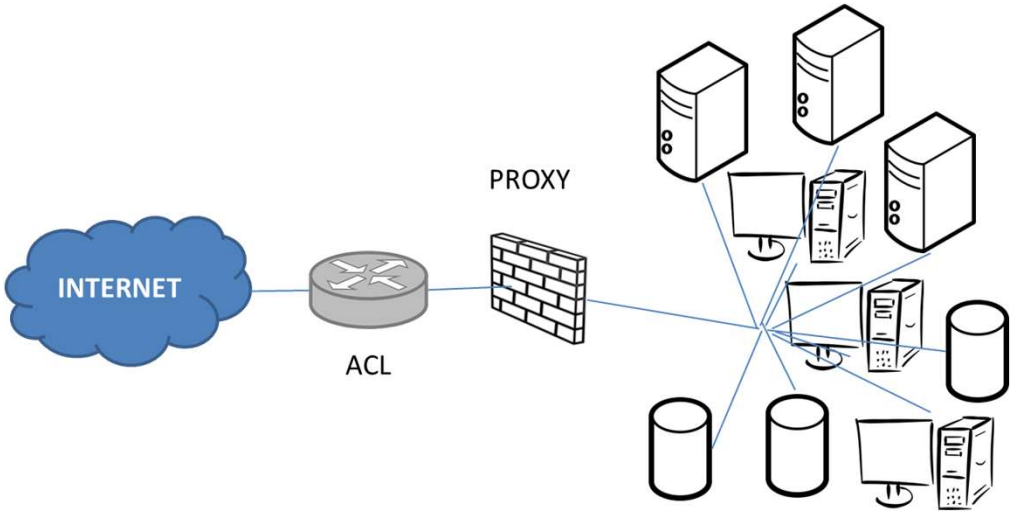
Universidad Rey Juan Carlos



# Firewalls y DMZs

Universidad Rey Juan Carlos

- Tanto el firewall como los proxys, son los elementos que están entre las dos redes, y por tanto se les conoce como “nodos bastión”.
- Hay que tener especial cuidado con su configuración, y su protección.
- Su objetivo fundamental será la de proteger la red interna de cualquier acceso desde la red externa.

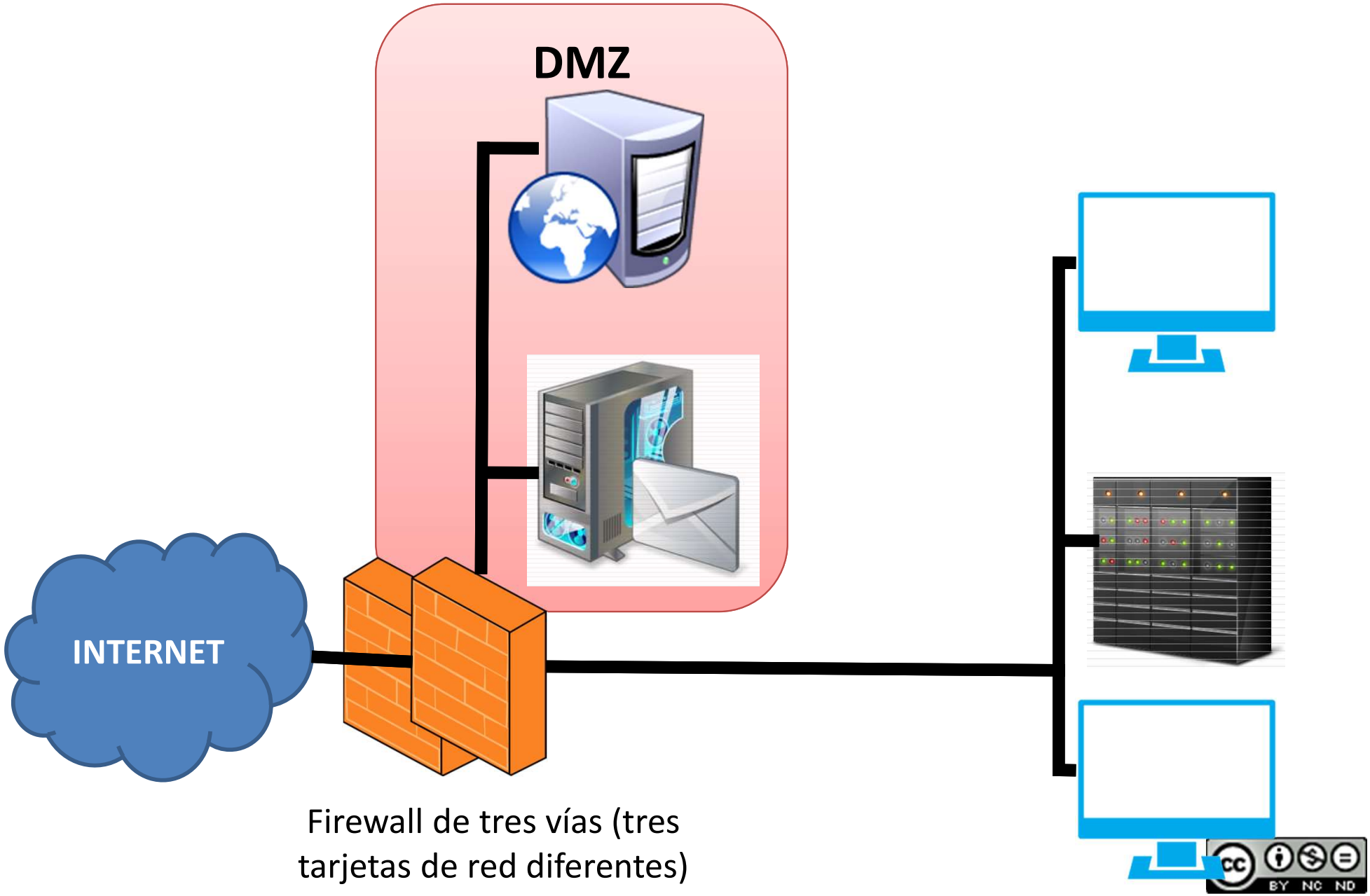


# Firewalls y DMZs

Universidad Rey Juan Carlos

- Una DMZ es una Zona Desmilitarizada.
- Se trata de una red que se coloca entre la red de ordenadores interior de una organización y una red exterior (normalmente Internet).
  - La zona desmilitarizada permite que servidores interiores utilicen servicios de la red exterior, mientras protege la red interior.
- Se puede implementar con un firewall de tres vías o con dos firewalls.

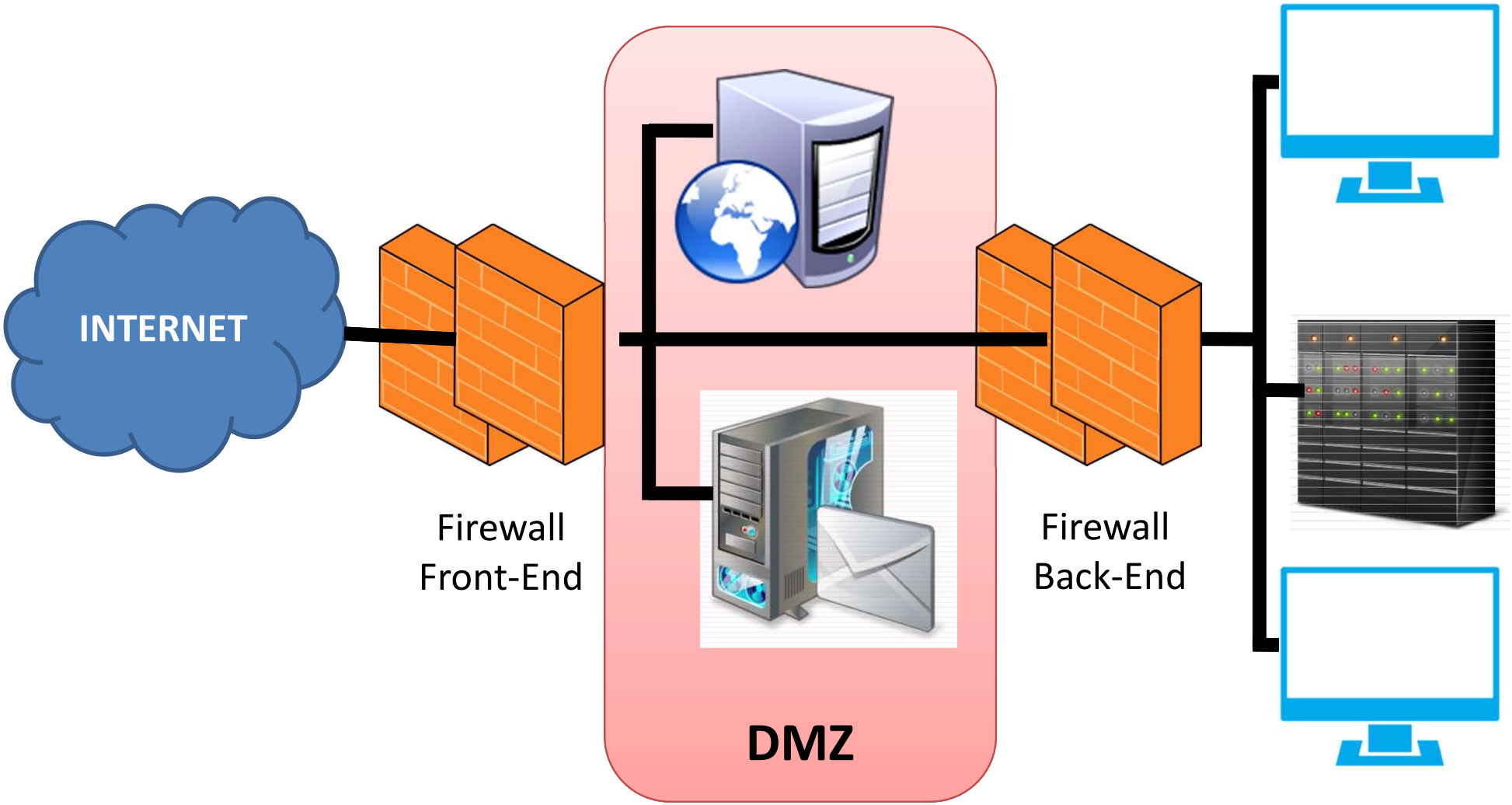
# Firewalls y DMZs




Firewall de tres vías (tres tarjetas de red diferentes)

# Firewalls y DMZs

Universidad Rey Juan Carlos



# Índice

# Honeypots

Universidad Rey Juan Carlos

Honeypot: recurso relacionado con la seguridad informática cuyo valor es ser puesto a prueba, atacado y/o comprometido

# Honeypots



- Un honeypot permite llevar una traza de los puntos de origen de los ataques.
- Recolectar información sobre las tácticas y herramientas utilizadas por los atacantes.
- Aprender acerca de malware y ataques zero-day.
- Analizar y comprender vulnerabilidades del sistema.
- Desviar o entretener al atacante

# Honeypots

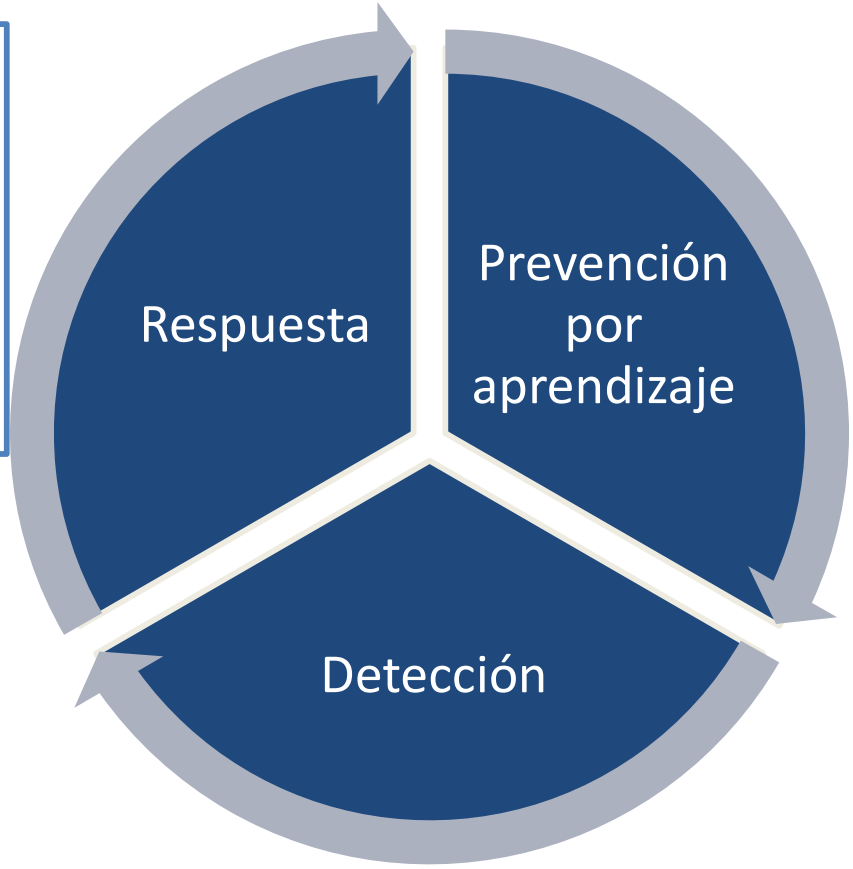
Universidad Rey Juan Carlos

- Un poco de sentido común:
  - Necesitamos que el honeypot sea atacado, tiene que ser un sistema lo más realista posible conectado a nuestra red.
    - Tendremos que generar datos y procesos falsos.
    - Cuidado con dejar configuraciones por defecto: en unos segundos el atacante sabrá que se trata de un honeypot.
  - Debemos separarlo adecuadamente del resto de sistemas para que no se vean comprometidos.
  - ¿Hasta qué punto protegemos al honeypot? Depende de cuál sea nuestro objetivo.
  - Nadie de la organización debe acceder al honeypot, de esta manera todo lo que llegue a este sistema se clasificará como un potencial ataque.

# Honeypots

Universidad Rey Juan Carlos

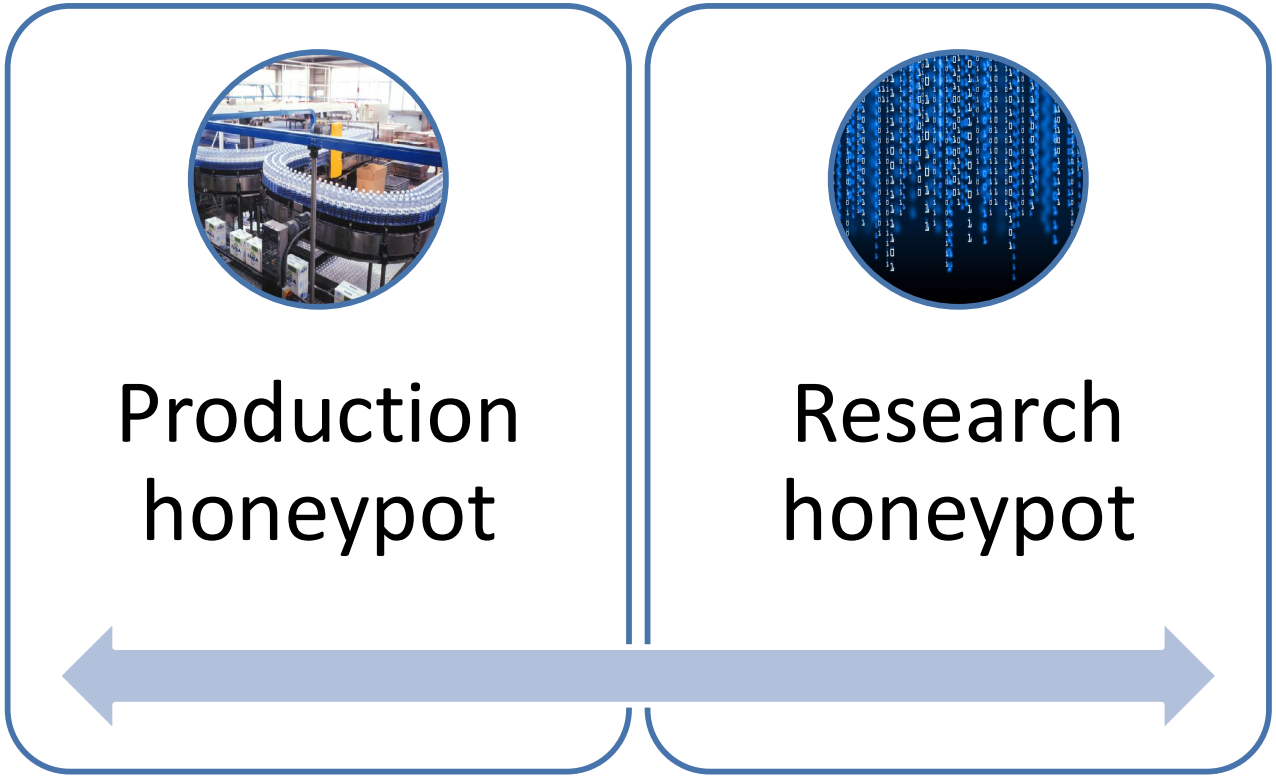
Ya no estamos pensando sólo en la prevención basada en la segmentación de redes



# Honeypots

Universidad Rey Juan Carlos

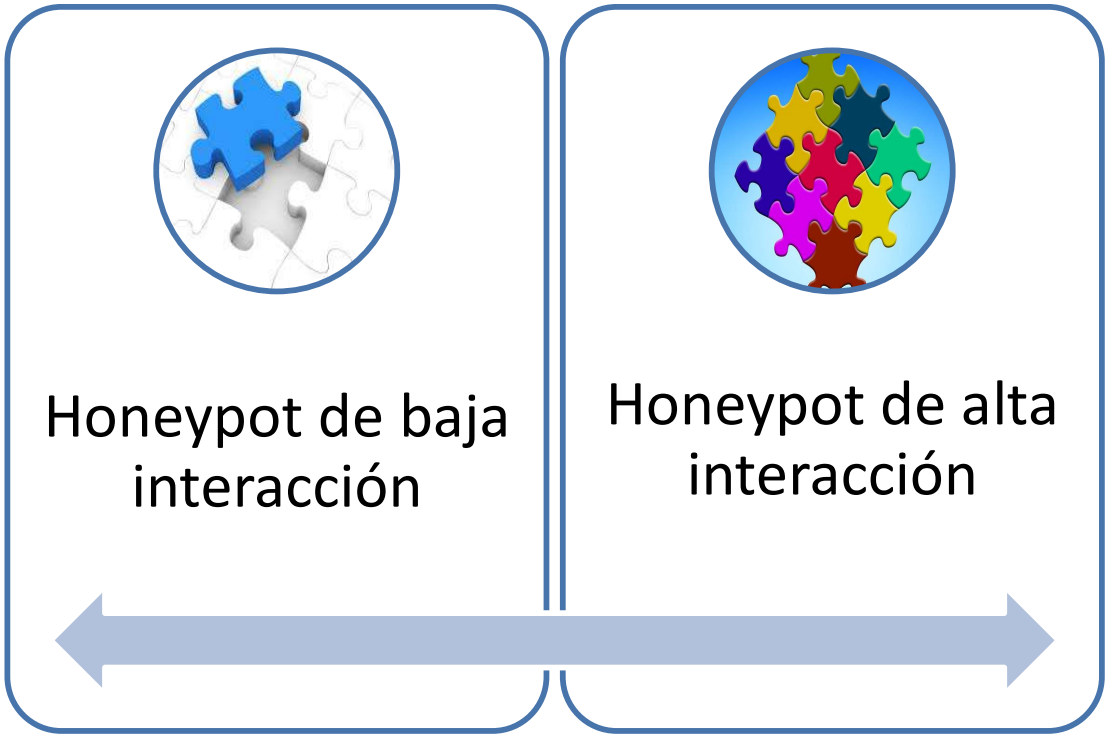
- Suelen distinguirse dos tipos de honeypots:



# Honeypots

Universidad Rey Juan Carlos

- Existe otra clasificación en función del nivel de interacción del honeypot con su entorno:



# Honeypots

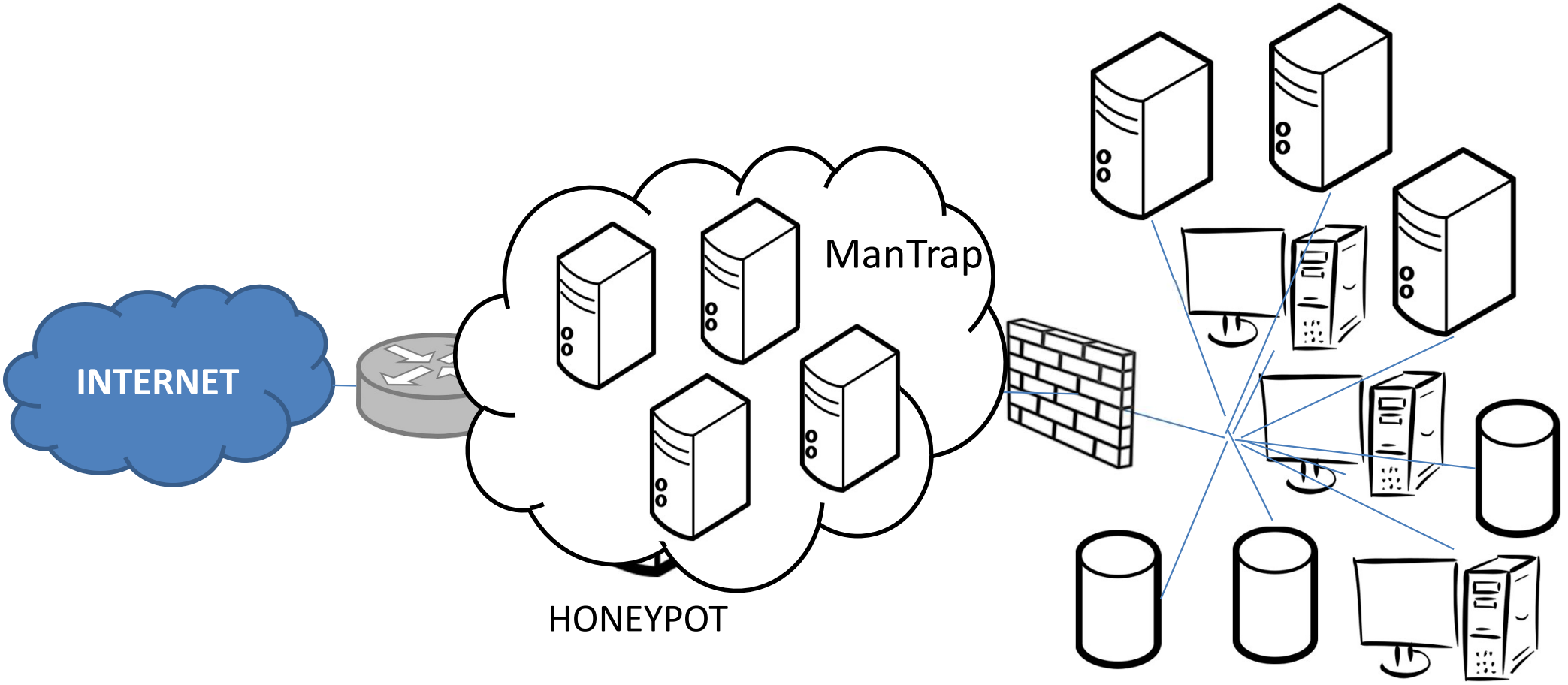
Universidad Rey Juan Carlos

- Los honeypots de **baja interacción** emulan una parte del sistema muy concreto.
  - Podemos encontrar honeypots que se instalan como una aplicación en un host, y permiten detectar y recolectar información sobre ataques concretos.
  - Ejemplo: honeypots para monitorizar puertos.

- Los honeypots de **alta interacción** son sistemas mucho más realistas.
  - Permiten simular un sistema mucho más complejo.
  - Ejemplo: jailed honeypots.

- Actualmente también hay honeypots de **interacción media** que son sistemas complejos pero está virtualizado.

# Honeypots



# Honeypots

Universidad Rey Juan Carlos

- Honeypots centrados en BBDD:
  - ElasticHoney
  - HoneyMySQL
- Honeypots centrados en entornos WEB:
  - Nodepot
  - Google hack honeypot
- Honeypots para IoT:
  - HoneyThing
  - Kako

- TPOT: contiene varios honeypots diferentes.

# Honeypots


elastic
Search Elastic
Dashboard
>T-Pot
Full screen
Share
Clone
Edit
Honeypot Attacks - Top 10
32,449
Cowrie - Attacks
7,764
Honeytrap - Attacks
5,242
Tanner - Attacks
3,893
Dionaea - Attacks
2,738
Adbhoney - Attacks
610
Redishoneypot - Attacks
548
Ciscoasa - Attacks
512
Heralding - Attacks
446
ConPot - Attacks
441
CitrixHoneypot - Attacks
Honeypot Attacks Bar
Attacks
Honeypots
Honeypot Attacks Histogram
Unique Source IPs
Attacks
Unique Source IPs
Timestamp
Attack Map - Dynamic
zoom: 0
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Attacks by Destination Port Histogram
80
22
23
1433
5555
Timestamp
Attacks by Honeypot Histogram
Cowrie
Honeytrap
Tanner
Dionaea
Adbhoney
Timestamp
Attacks by Country Histogram
United States
China
Canada
Netherlands
Germany
Timestamp
Attacker Src IP Reputation
known attacker
mass scanner
anonymizer
bad reputation
bot, crawler
tor exit node
bitcoin node
Attacks by Honeypot
Cowrie
Honeytrap
Tanner
Dionaea
Adbhoney
Redishoneypot
Ciscoasa
P0f OS Distribution
Linux 2.2.x-3.x
Linux 2.2.x-3.x (barebon...
Linux 3.11 and newer
Windows 7 or 8
Windows NT kernel
Linux 3.1-3.10
Mac OS X
Attacks by Country
United States
China
Canada
Netherlands
Germany
United Kingdom
Russia

# Honeypots

Universidad Rey Juan Carlos

Ejemplos de Honeypots:

- Honeytrap: honeypot que observa ataques contra servicios TCP y UDP.
- Dionaea: honeypot de carácter general diseñado para simular vulnerabilidades de red y servicios (SMB, HTTP, FTP, MSSQL, …)
- Cowrie: simula un servidor con SSH y Telnet diseñado para monitorizar los ataques de acceso y la interacción con la Shell.
- Glastopf: orientado a aplicaciones web (webmail, wikis, etc.)
- Conpot: honeypot para ICS que permite simular un entorno industrial completo.
- EMobility: honeypot para ICS que simula un centro de carga eléctrica de vehículos (incluso simula usuarios cargando los vehículos).

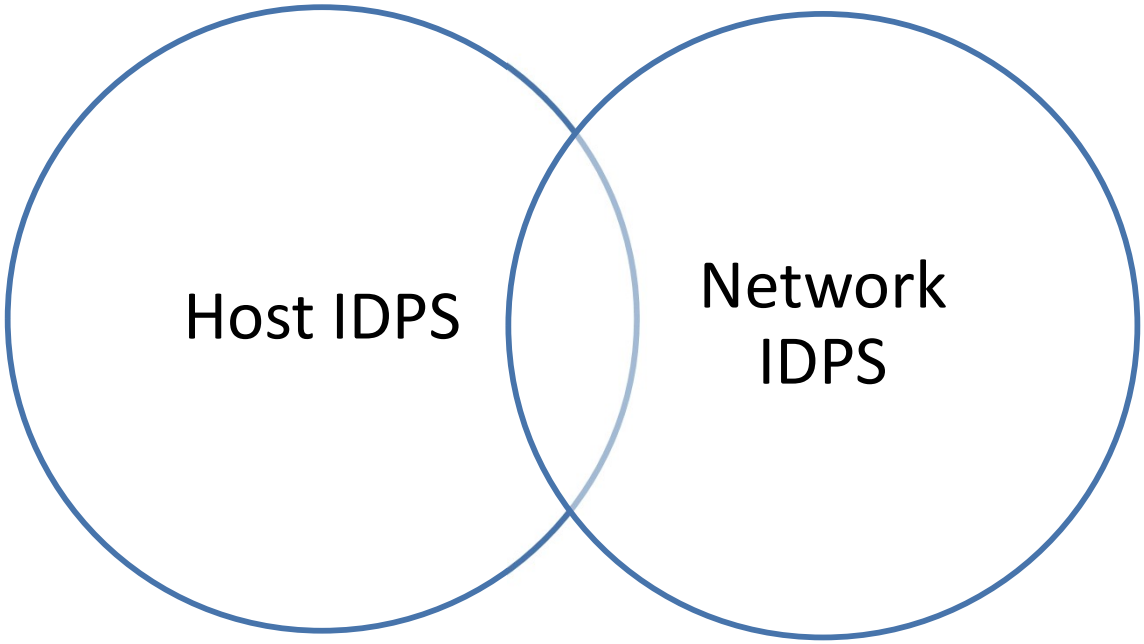
# Honeypots



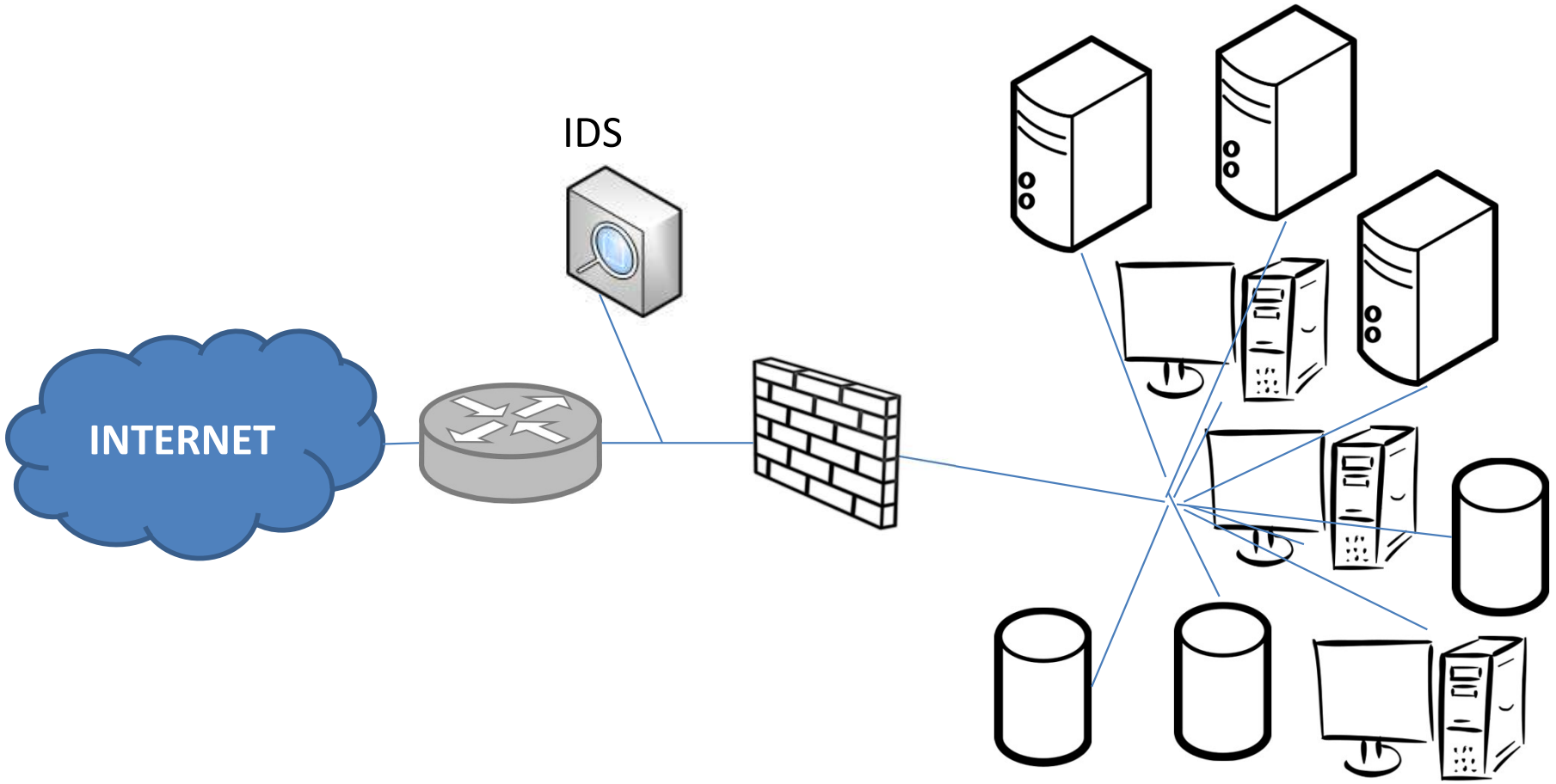
- Una honeynet es un conjunto de honeypots de alta interacción que conforman una red completa con los objetivos de prevención, detección y respuesta ya mencionados.

- Son soluciones costosas de desplegar y mantener, por lo que normalmente se utilizan para investigación.
  - Aunque la aparición de honeynets virtual las han hecho más asequibles para todo tipo de entornos.

- Un honeypot o una honeynet pueden formar parte de una solución IDPS (*Intrusion Detection and Prevention System)* o alimentarla:



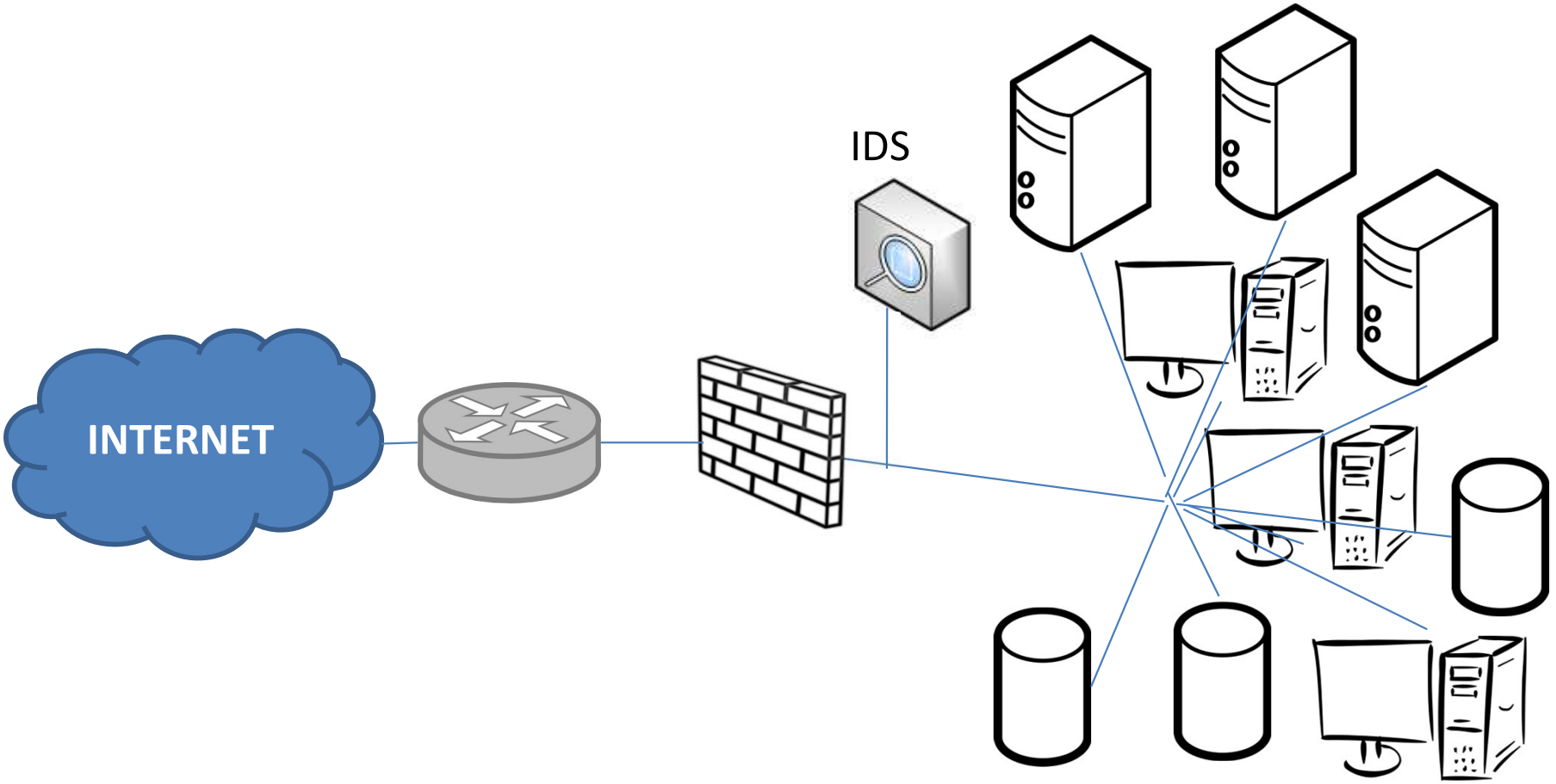
- Dónde colocar el IDS:



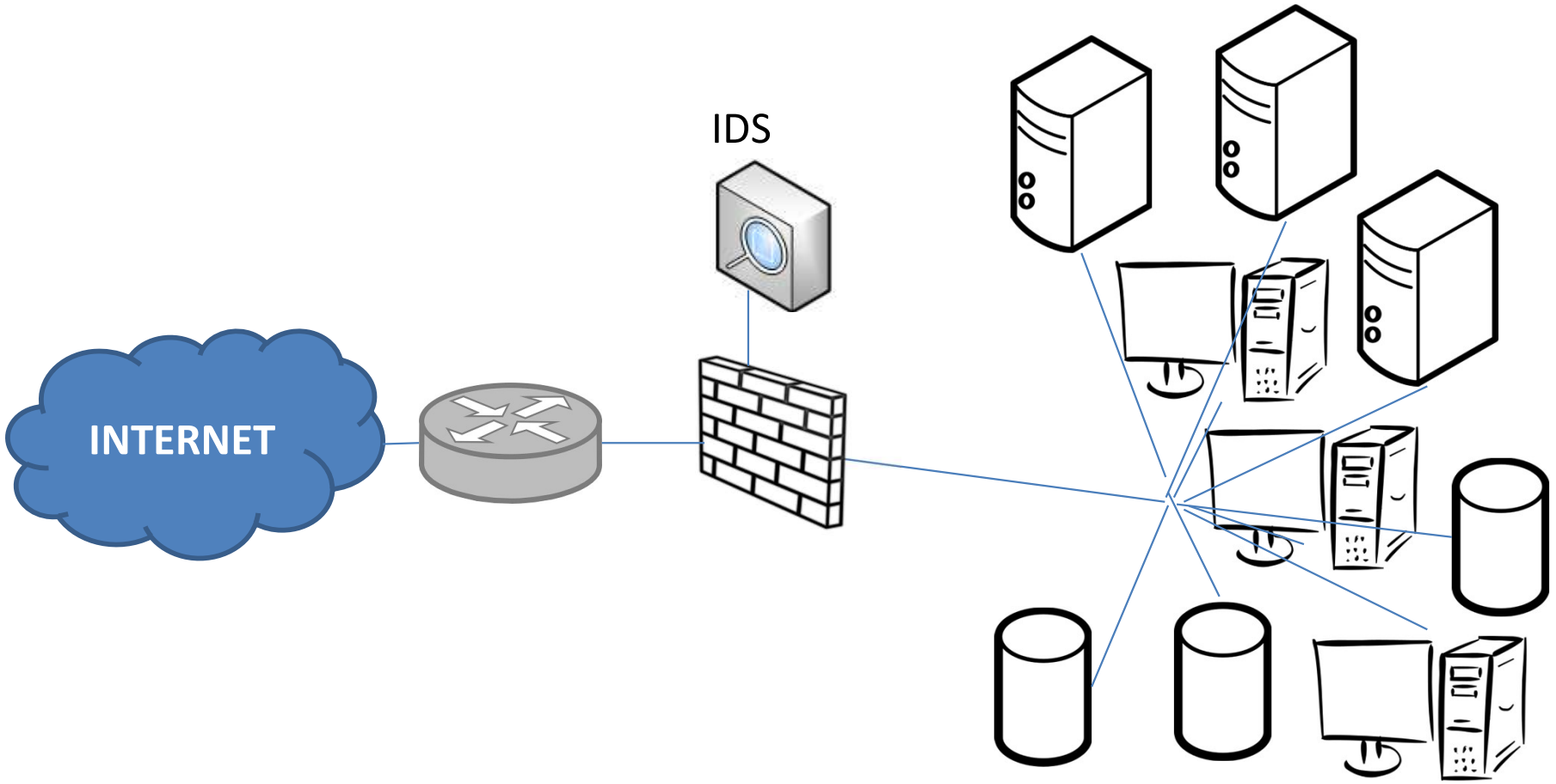
# IDS



- Dónde colocar el IDS:



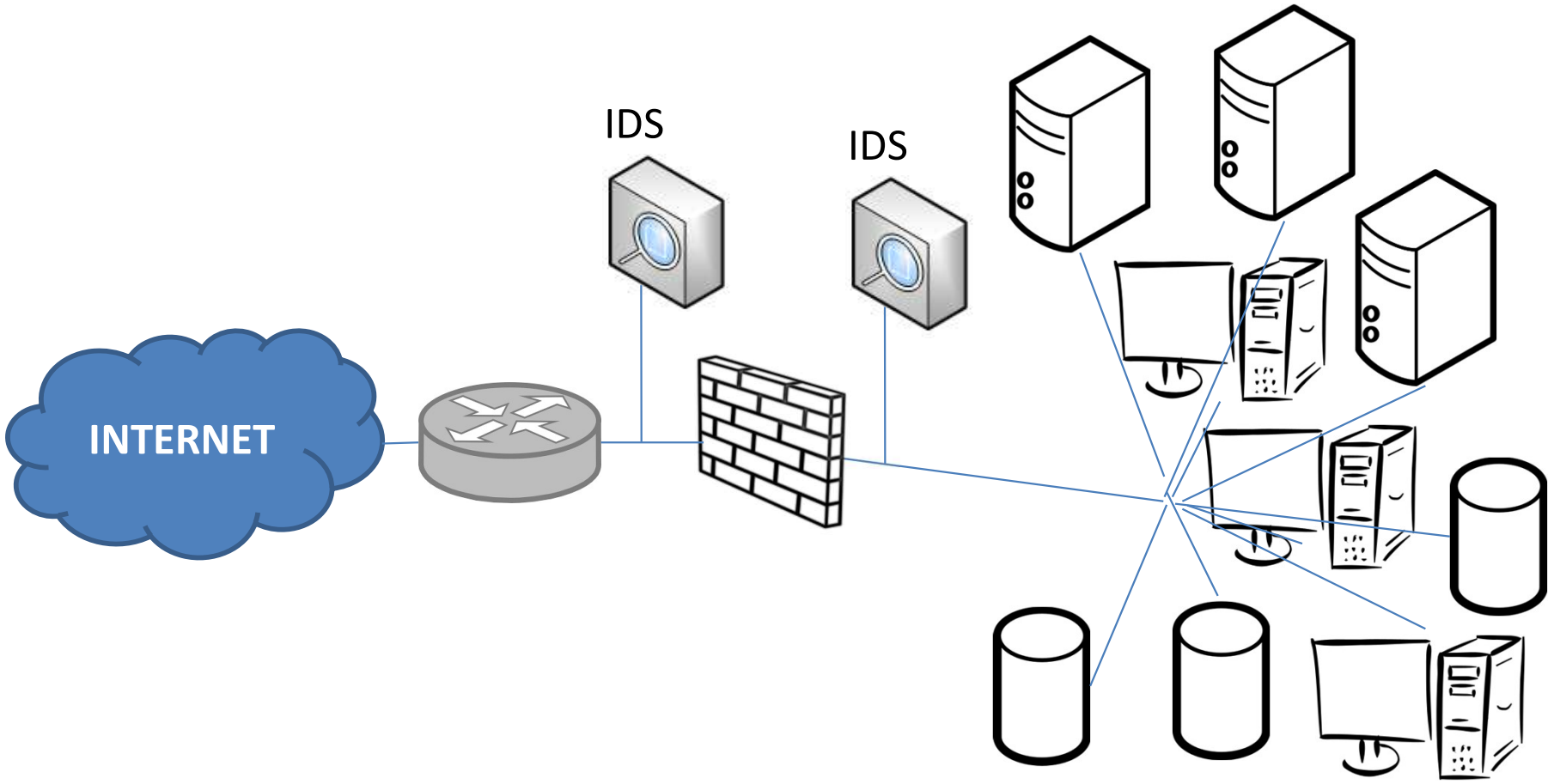
- Dónde colocar el IDS:



# IDS



- Dónde colocar el IDS:



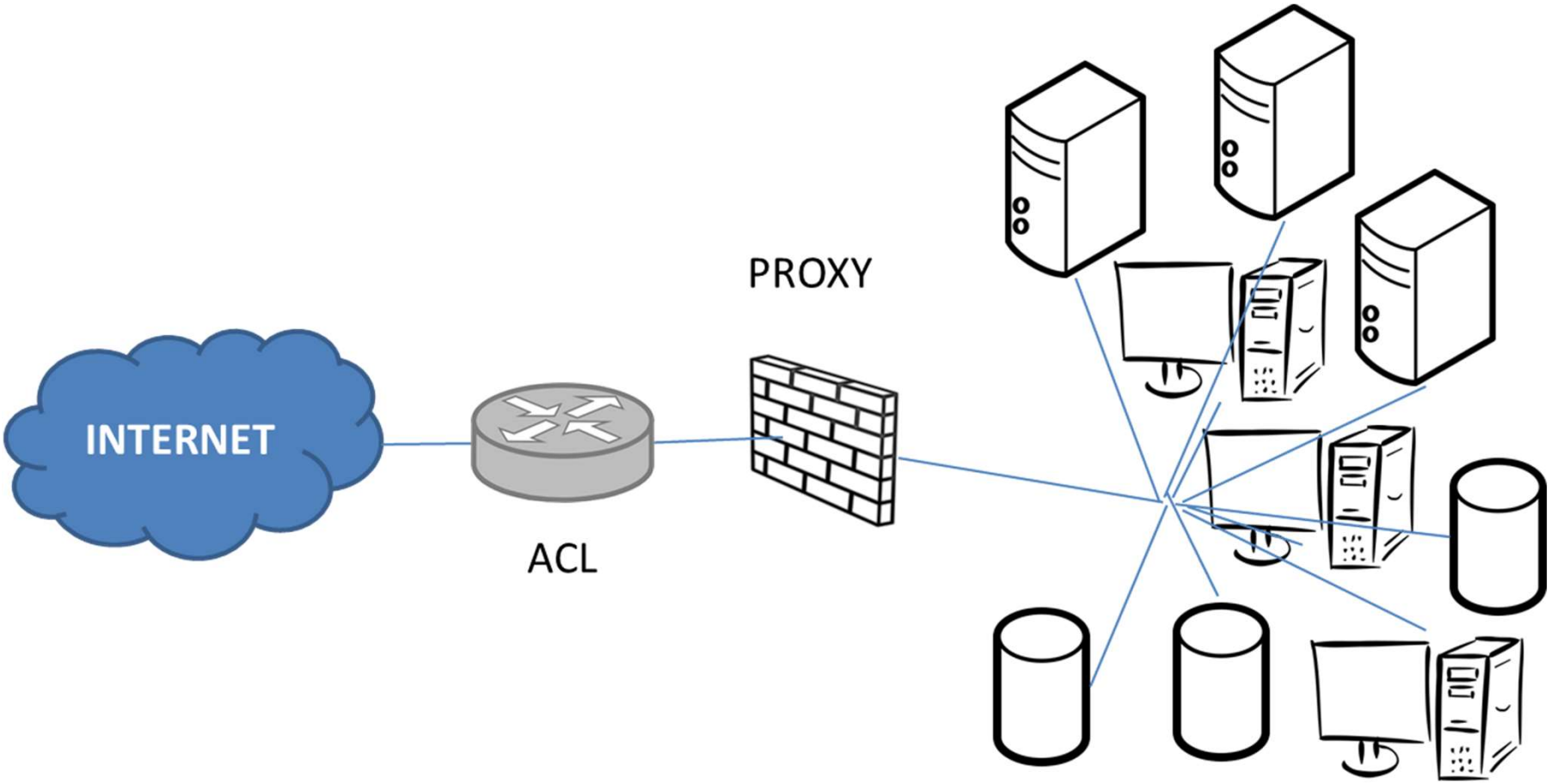
# Índice



- Introducción.
- Firewalls y DMZs.
- Honeypots.
- **Redes Privadas Virtuales (VPN).**
- IPSec.
- SSL/TLS.
- Resumen.

# Redes Privadas Virtuales

Universidad Rey Juan Carlos



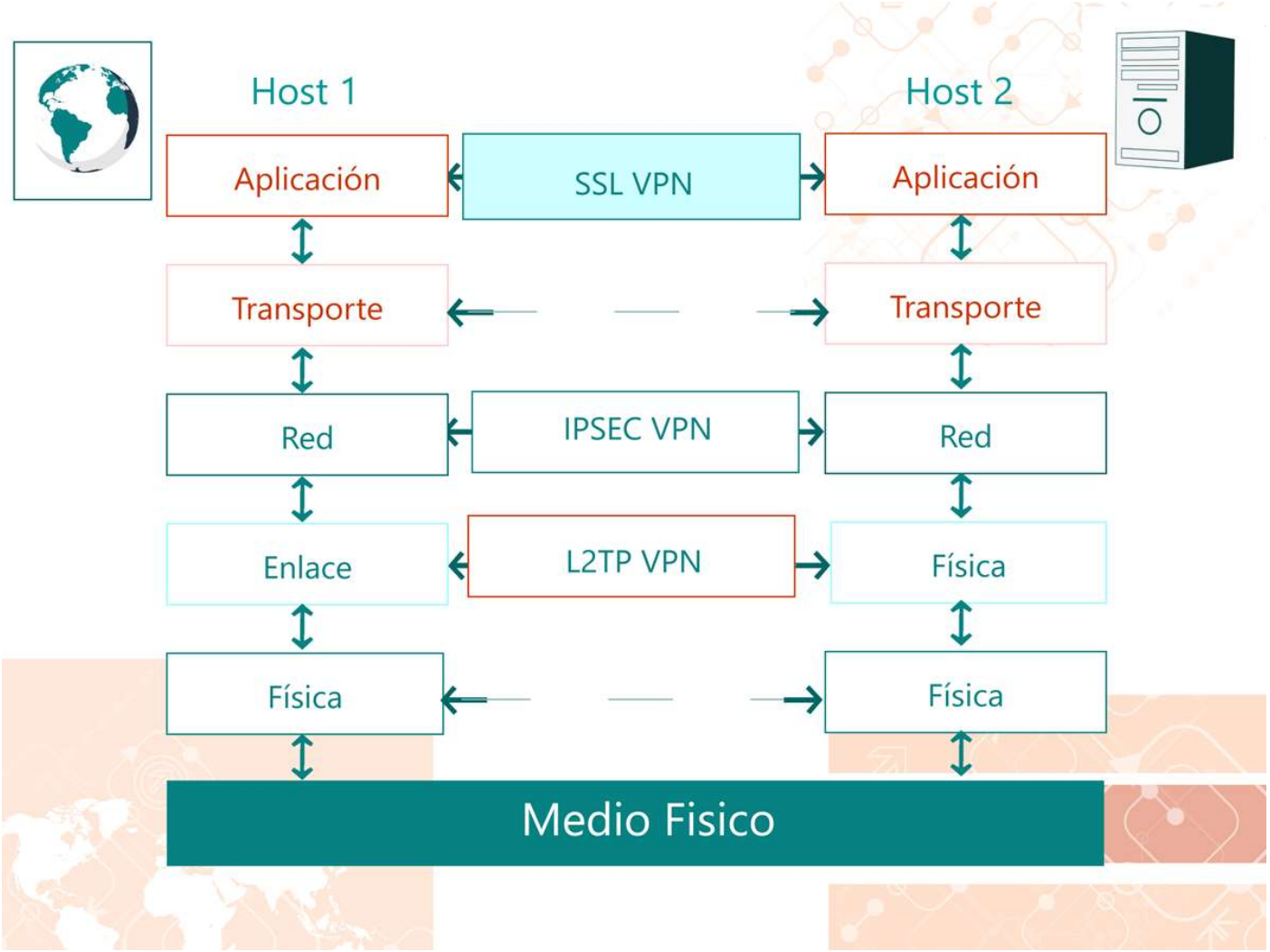
# Redes Privadas Virtuales

Universidad Rey Juan Carlos

- Tipos de VPN:
  - VPN de acceso remoto: para personal de empresas.
  - VPN intranet: comunicar diferentes redes.
  - VPN extranet: dar acceso a terceros (proveedores, clientes, etc.)
  - VPN abierta/cerrada.
- Objetivo: garantizar la seguridad de la comunicación.
- Protocolos que implementan VPN:
  - SSL/TLS, IPSec, PPTP (Point-to-Point Tunelling Protocol), L2TP (Layer 2 Tunneling Protocol), MPPE (Microsoft Point-to-Point Encryption), SSTP (Microsoft Secure Socket Tunneling Protocol), SSH (Secure Shell), etc.

# Redes Privadas Virtuales

Universidad Rey Juan Carlos



# Redes Privadas Virtuales

Universidad Rey Juan Carlos

# Índice



- Introducción.
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- **IPSec.**
- SSL/TLS.
- Resumen.

# IPSec

Universidad Rey Juan Carlos

- Conjunto de mecanismos de seguridad que se pueden implementar, o utilizar, junto con IP versión 4 (optativo) o con IPv6 (soporte nativo).
- IPSec provee de la capacidad de asegurar las comunicaciones a través de LAN, WAN privadas o públicas, y a través de Internet.
- Habilitar IPSec supone que se puede realizar encriptación y autenticación de la información a nivel de red (IP).
  - De manera transparente para los usuarios y las aplicaciones y con una administración centralizada y flexible.

# IPSec

Universidad Rey Juan Carlos

- Servicios:

| | | |
|---|---|---|
| Control de acceso | Integridad de la conexión | Autentificación del origen de la conexión |
| Rechazo de paquetes modificados | Confidencialidad | VPN seguras |

# IPSec



IPSec aumenta la seguridad mediante:

- La **autenticación** mutua de dos equipos antes del intercambio de datos.
- El **cifrado de los datos** intercambiados mediante cifrado de datos estándar (DES, 3DES o AES).
- El establecimiento de una **asociación de seguridad** (SA) entre los dos equipos.
  - Una SA es el conjunto de algoritmos y parámetros (como la claves) que se están usando para cifrar y autenticar un flujo particular de información en una dirección.
  - Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad.

# IPSec

Universidad Rey Juan Carlos

- IPSec es un protocolo proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores, como UDP y TCP.
- Las cabeceras se colocan después de la cabecera IP y antes de la cabecera TCP u UDP.
- Proporciona servicios de autenticación, “confidencialidad”, integridad y “no repudio”.
- Una vez establecida la conexión, los segmentos TCP y datagramas UDP se envían cifrados y autenticados. Además, se comprueba la integridad para evitar que alguien modifique la información.

# IPSec



- Tenemos dos tipos diferentes de cabeceras:
  - Cabecera de Autenticación (AH, *Authentication Header*).
  - Protocolo de Seguridad Encapsulada (ESP, *Encapsulating Security Protocol*).

- A la hora de establecer la comunicación, o túnel, se debe de elegir una de las dos.

**Cabecera de autenticación (AH)**

- Proporciona autenticación e integridad, pero no proporciona confidencialidad.
- Hace uso de huellas digitales HMAC.
- El protocolo calcula la función hash del contenido del paquete IP.
- Permite autenticar el origen de los datos, y verificar que dichos datos no se han modificado.
- Pero al no cifrar los datos del paquete no proporciona confidencialidad.

**Protocolo de seguridad encapsulada (ESP)**

- Ofrece autenticación, integridad y confidencialidad.
- El área de datos está cifrado usando algoritmos de clave simétrica.
- Generalmente, se usa cifrados de bloque como AES.
- Para ello, se usa el algoritmo Diffie-Hellman para realizar el intercambio de claves.

**Internet Key Exchange (IKE)**

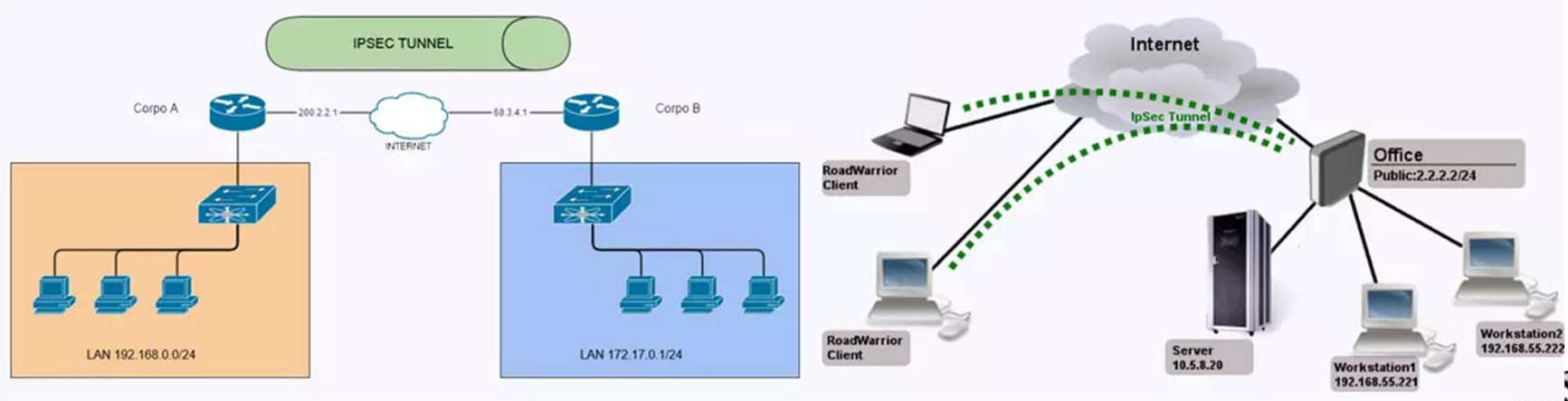
- Es un protocolo que se utiliza para generar y administrar las claves necesarias para establecer las conexiones AH y ESP.
- Los participantes tienen que negociar tipos de cifrado y los algoritmos de autenticación.

**Directivas de seguridad:**

- Son las **reglas de seguridad** que definen los algoritmos de hash, los algoritmos de cifrado y la longitud de la clave soportados.
- Estas reglas también definen las direcciones, protocolos, nombres DNS, subredes o tipos de conexión a los que se aplica la configuración de seguridad.
- Las directivas de IPSec se pueden configurar de acuerdo con los requisitos de seguridad de un usuario, grupo, aplicación, dominio, sitio o empresa global.

# IPSec

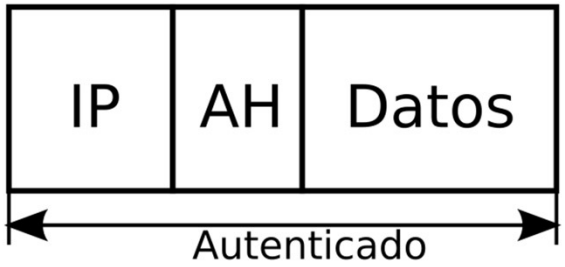
- IPSec puede proporcionar seguridad trabajando en dos modos:
  - Modo transporte o **extremo a extremo**: son los extremos finales de la comunicación (origen y destino) los que se encargan de realizar el procesamiento necesario de la información.
  - **Modo túnel** (a veces llamado puerta a puerta): la seguridad es proporcionada por un único nodo central a uno o varios sistemas (incluso a una red de área local completa).



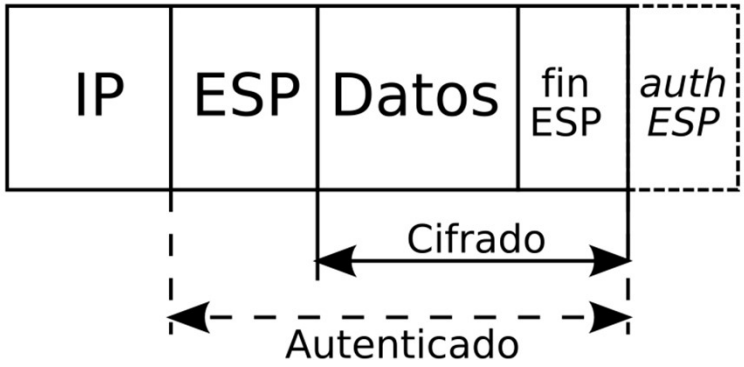
- IPSec utiliza formatos estándar de paquete IP, de manera que los dispositivos de red intermedios no distinguen entre paquetes IP y paquetes IPSec.

Modo Transporte

AH

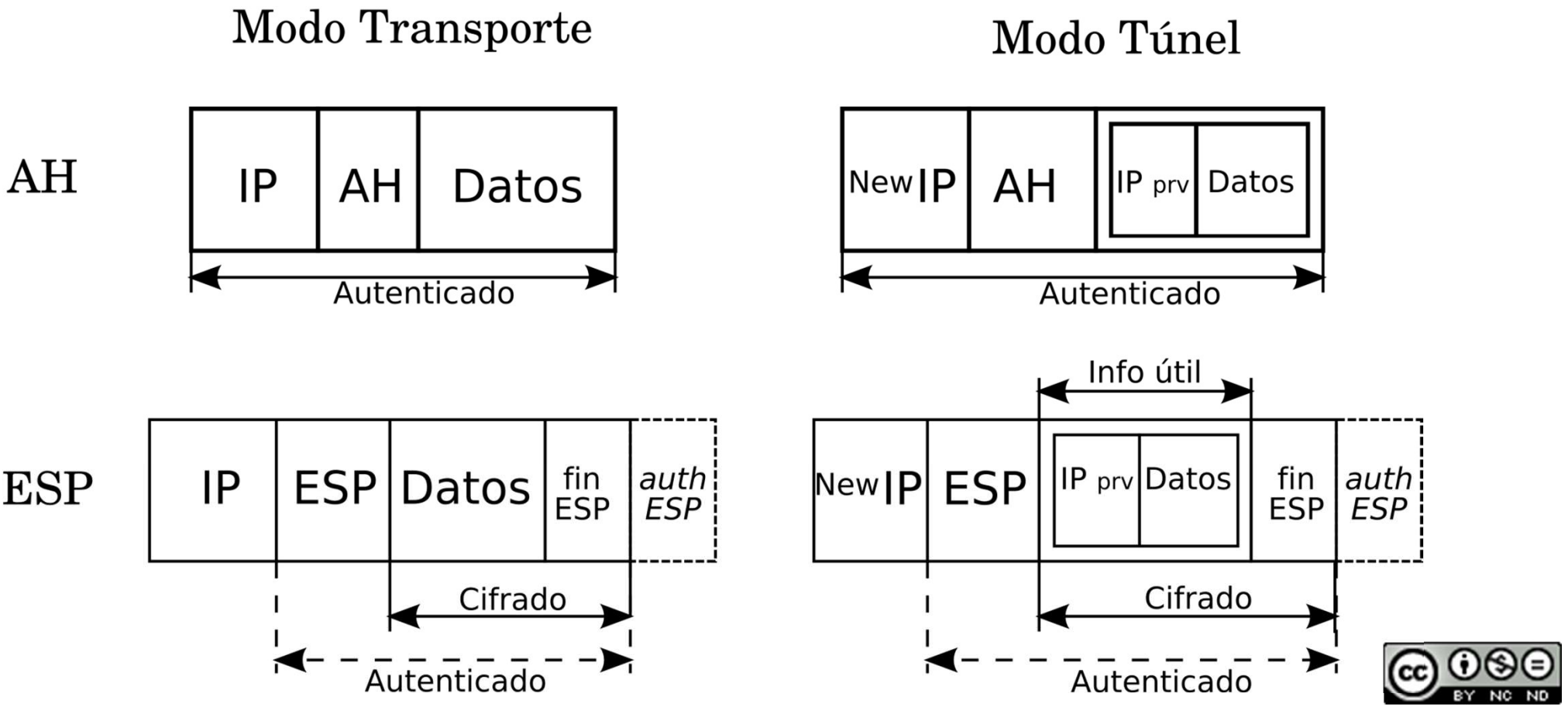



ESP

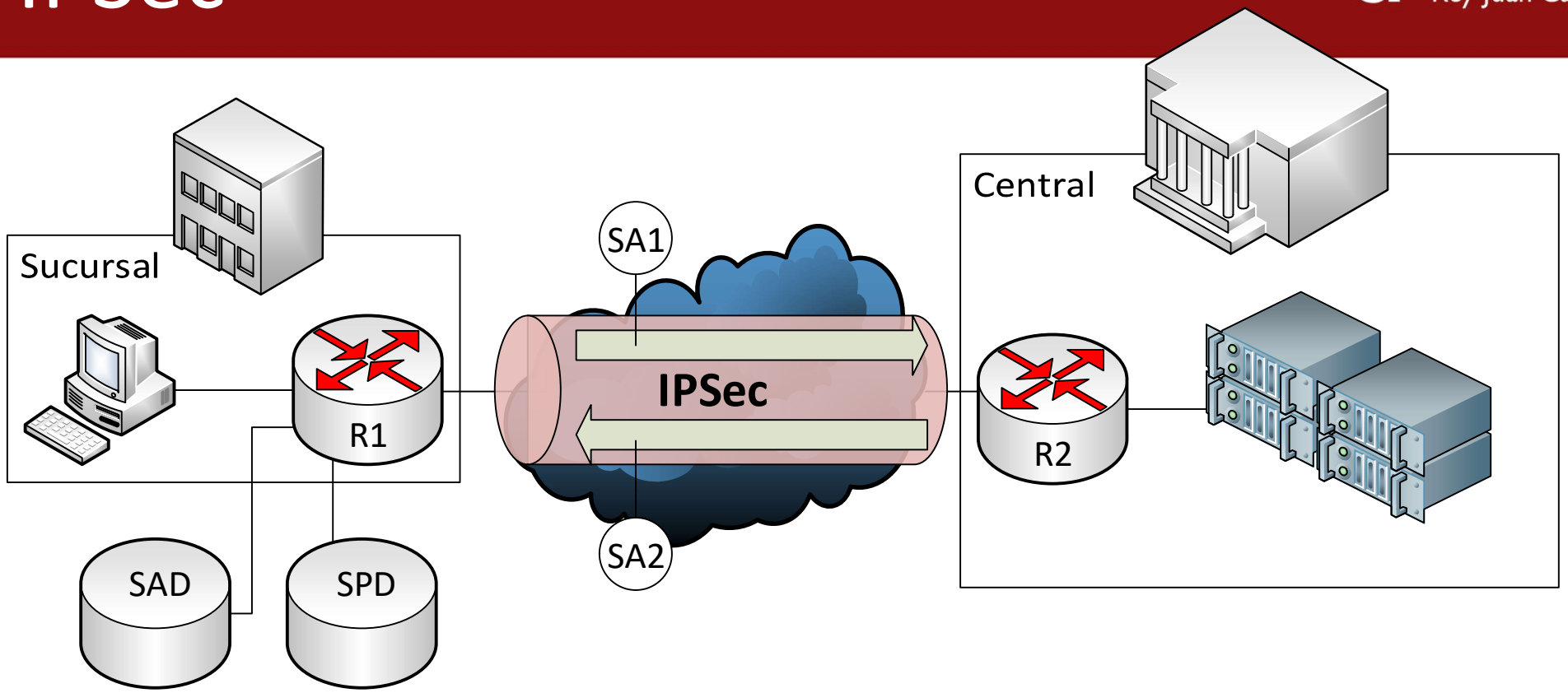


# IPSec

- IPSec utiliza formatos estándar de paquete IP, de manera que los dispositivos de red intermedios no distinguen entre paquetes IP y paquetes IPSec.



# IPSec



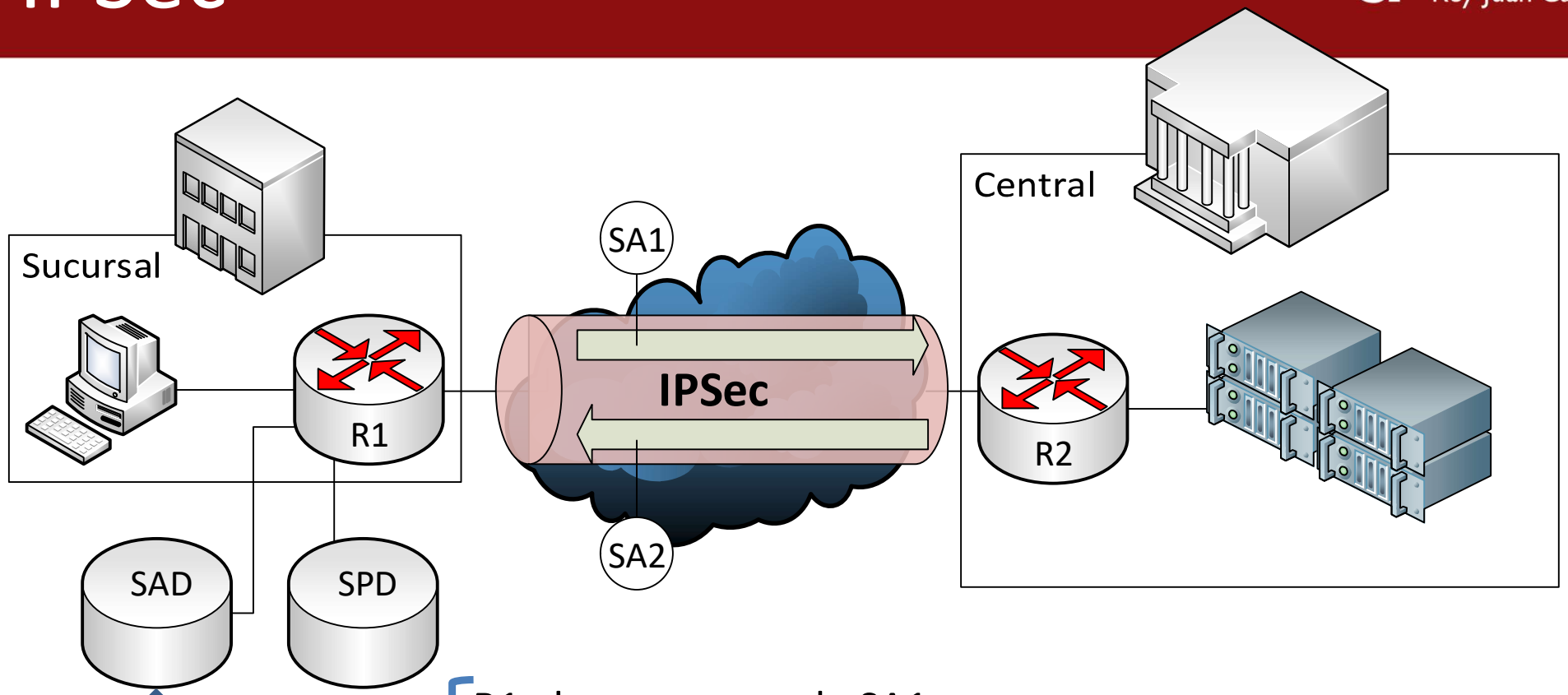

Queremos comunicar la red de la sucursal con la central usando un túnel IPSec y usando el protocolo ESP.

Se crean dos Asociaciones de Seguridad que definen los parámetros para que la comunicación sea segura.

Cada comunicación tiene un id (SPI, *Security Parameter Index*), su interfaz de origen y de destino.

Toda esta información se guarda en el SAD (*Security Association Database)*

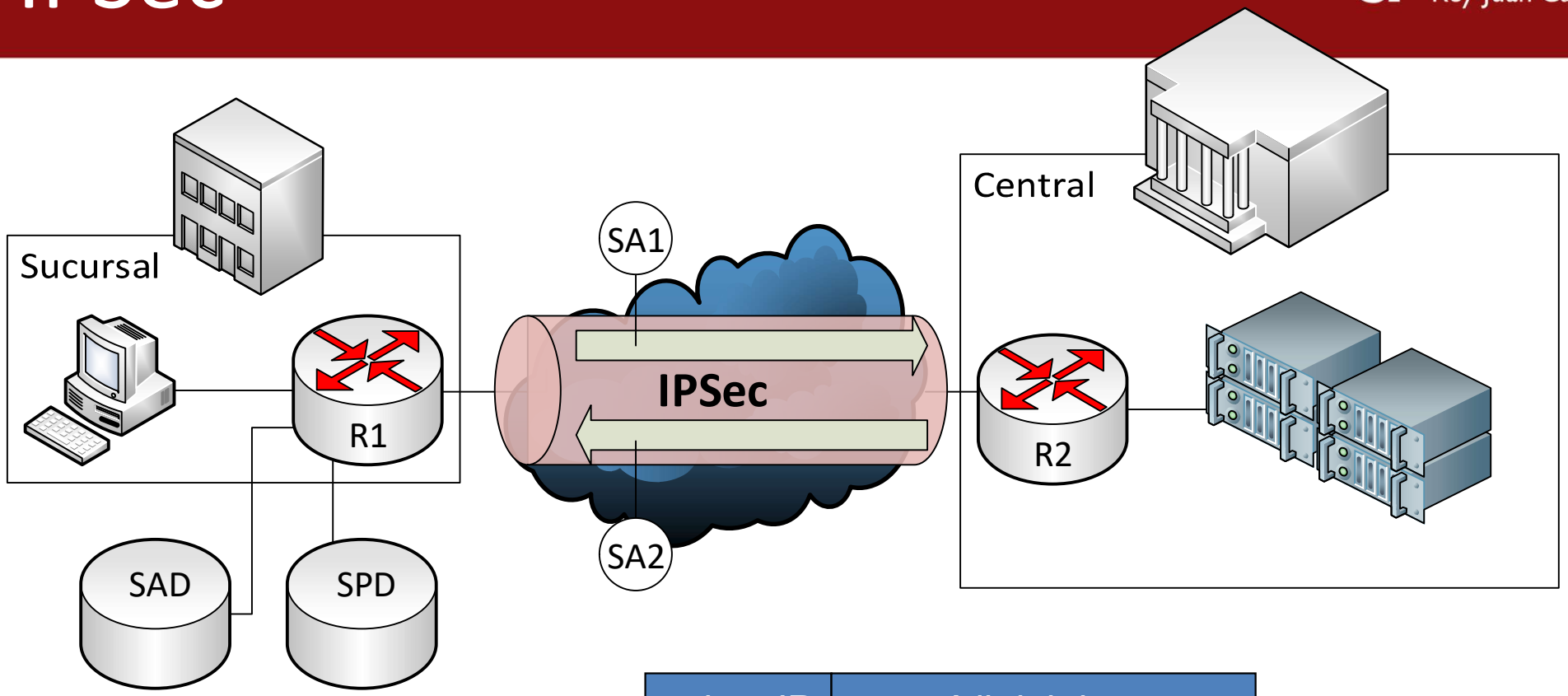
# IPSec




R1 almacena para la SA1:

- Security Parameter Index (SPI), identificador de SA (32bit)
- Interfaz origen de la SA (R1)
- Interfaz destino de la SA (R2)
- Protocolo: ESP
- Cifrado a usar (ej. AES)
- Clave de cifrado
- Algoritmo de integridad (ej. HMAC con SHA256)
- Clave de autenticación

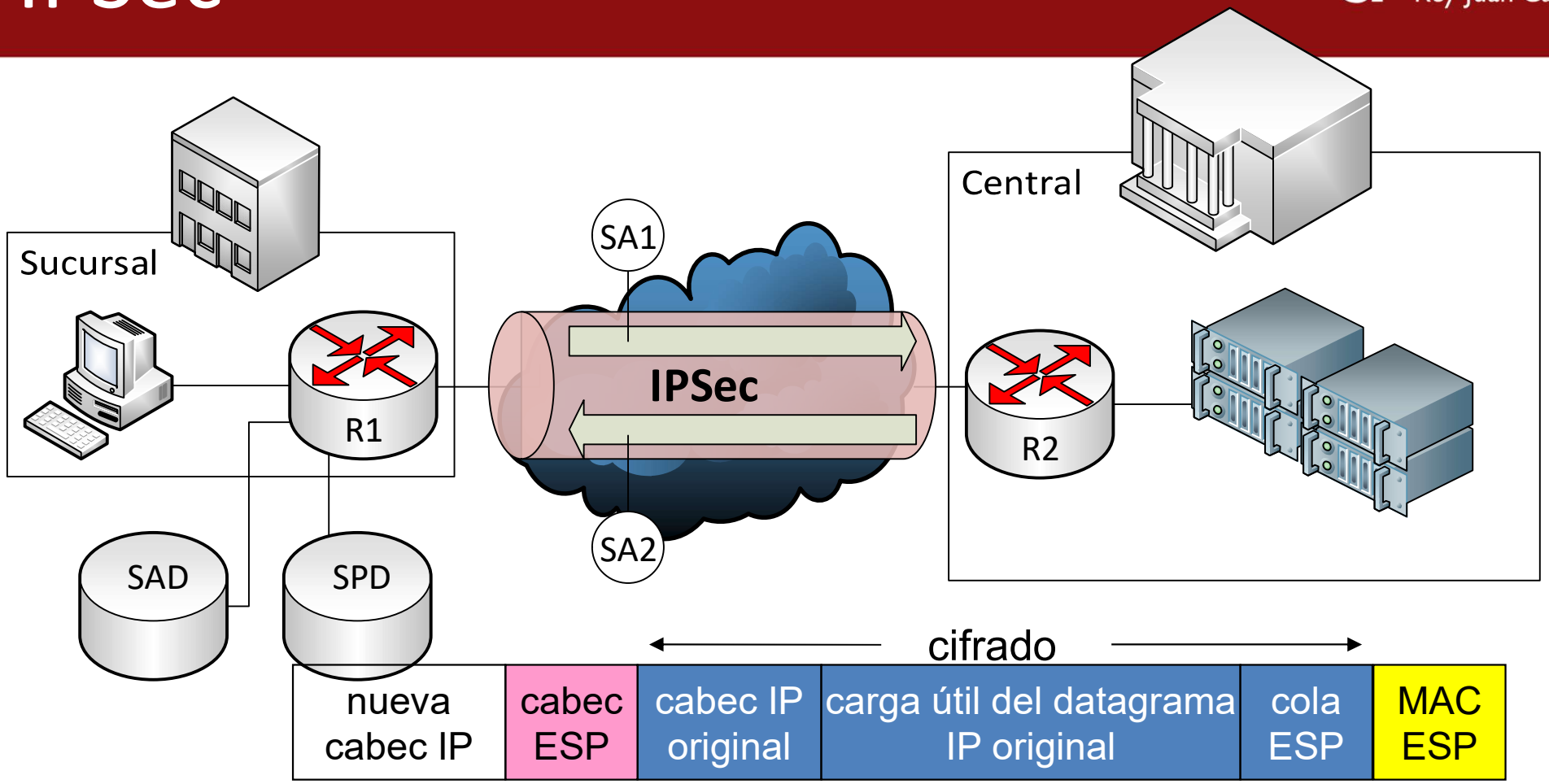
# IPSec




| cabec IP original | carga útil del datagrama IP original |
|---|---|

El equipo manda el mensaje a R1. Este accede al SAD y obtiene la información para configurar el paquete.

# IPSec




Se añade la cabecera ESP que incluye el identificador SPI de la SA, y un número incremental.

Genera un MAC que añade al final del paquete.

Crea una nueva cabecera IP.

# IPSec

Universidad Rey Juan Carlos

Resumen de servicios IPSec:

- Supongamos que un intruso intenta un ataque MitM entre R1 y R2 (sin conocer claves).
- ¿Será capaz de ver el contenido del datagrama original? ¿Y las direcciones IP de origen o destino, el protocolo de transporte o el puerto de aplicación?
- ¿Puede intercambiar bits sin ser detectado?
- ¿Y suplantar a R1 utilizando la dirección IP de R1?

# Índice

Universidad Rey Juan Carlos

- Introducción.
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- **SSL/TLS.**
- Resumen.

# SSL/TLS

Universidad Rey Juan Carlos

- SSL es un protocolo creado por Netscape en 1994.
- Funciona entre la capa de aplicación y la de transporte (generalmente TCP/IP).
- Proporciona seguridad a cada servicio o protocolo al nivel de aplicación:
  - HTTP (https)
  - FTP
  - Telnet
  - POP 3
  - SMTP

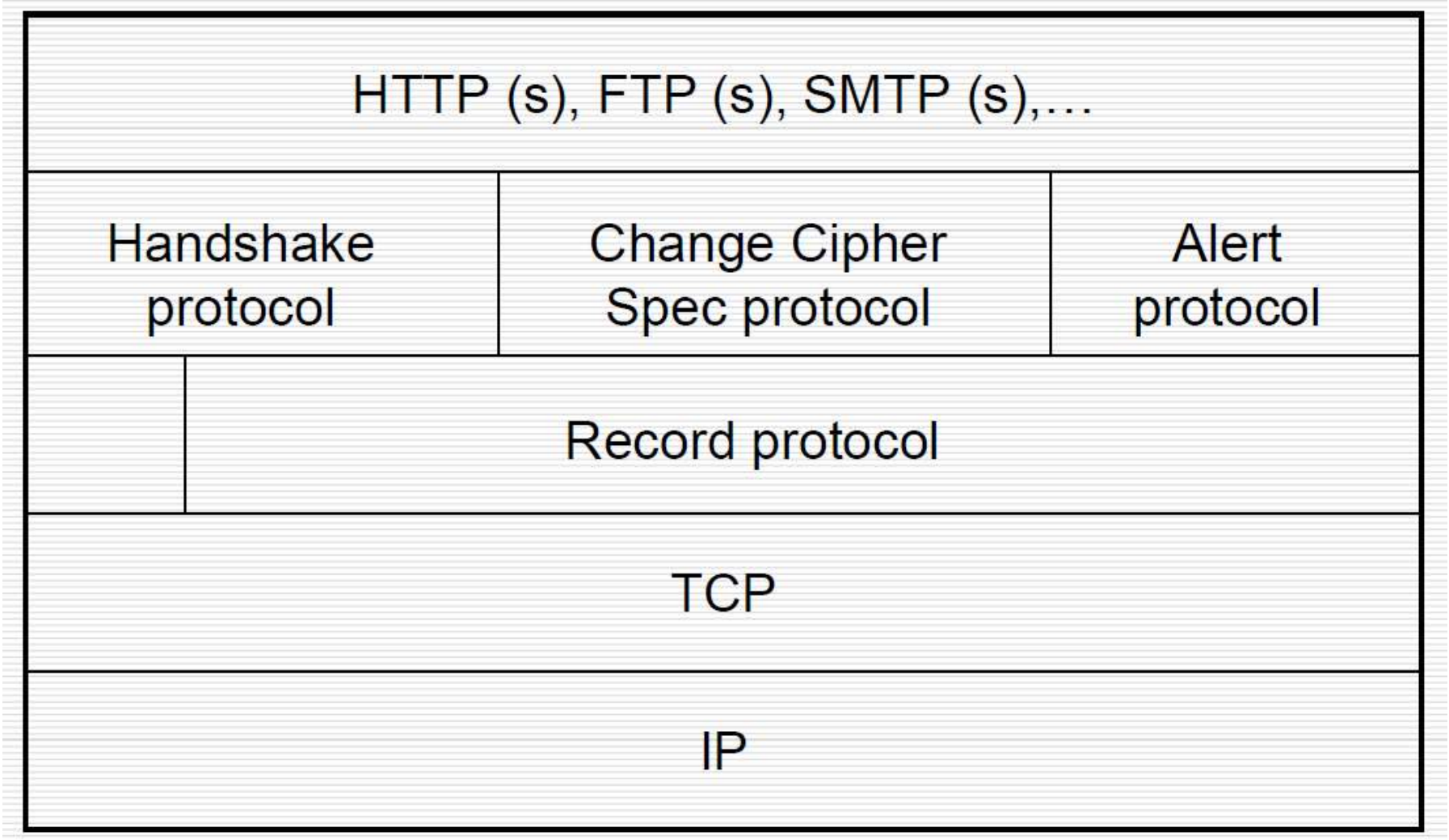
Universidad Rey Juan Carlos

**Características:**

- Establece un canal seguro en la capa de aplicación entre dos entidades.
- Permite compresión (aunque es opcional)
- Proporciona diferentes servicios de seguridad:
  - Autenticación del cliente.
  - Autenticación del servidor.
  - Integridad: con el uso de MACs.
  - Confidencialidad: cifrado simétrico.
  - No repudio.

# SSL/TLS





**Alert protocol:**

- Se utiliza para informar sobre ciertos eventos.
- Se manda una descripción y cómo de severo es el evento.

- Ejemplos de eventos:
  - Condiciones de error (errores en el MAC).
  - El certificado ha expirado.
  - Uso de algún parámetro ilegal.
  - Se termina la conexión planificada.

**Change Cipher Spec:**

- Se utiliza para notificar un cambio en el cifrado que se está usando (algoritmo, claves, etc.)
- Se manda un mensaje encriptado con las características del cifrado (lo mandan tanto el cliente como el servidor).
- Tiene lugar en la fase 4 del *Handshake protocol.*

**Handshake Protocol:**

- Es el protocolo más complejo de SSL.
- Permite la autenticación mutual de cliente y servidor.
- Se negocia el algoritmo, los parámetros y las claves que se usarán para cifrar los datos.
- Tiene lugar antes de la transmisión de los datos de aplicación.
- Consta de 4 fases:
  - Fase 1: establece el id de la sesión, el conjunto de cifrado…
  - Fase 2: se manda el certificado del servidor y se solicita el certificado del cliente.
  - Fase 3: se manda el certificado del cliente.
  - Fase 4: se acuerdan los algoritmos de cifrado.

Universidad Rey Juan Carlos

**Fase 1:**

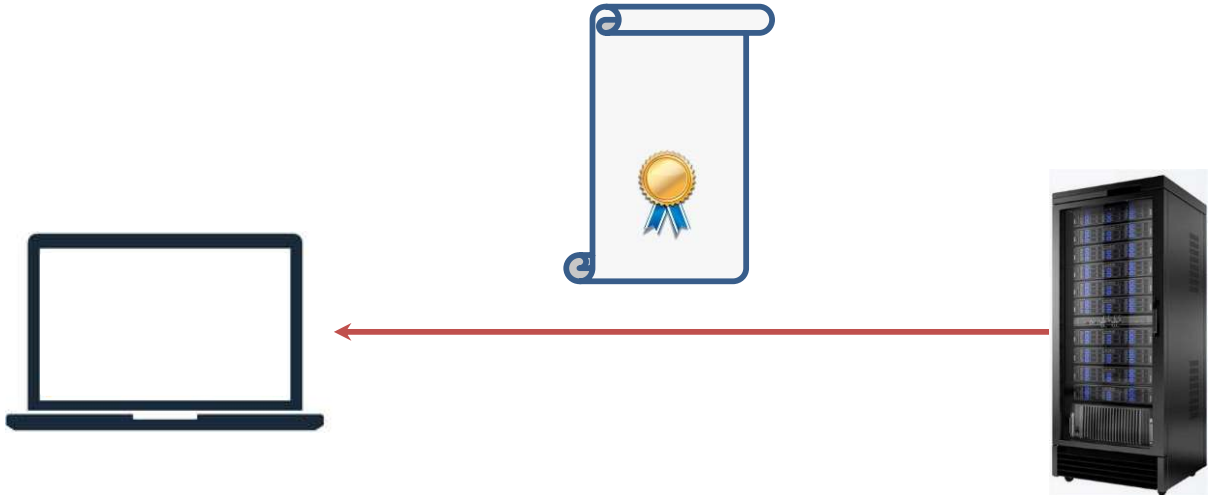

- Cliente:
  - Crea un número aleatorio con el timestamp (*client random*).
  - Manda los algoritmos de cifrado que soporta:
    - Método de intercambio de claves.
    - Algoritmo de cifrado para la transmisión de datos.
  - Envía también tipo de compresión.

**Fase 1:**


- Server:
  - Crea un número aleatorio (*server random*).
  - Envía el método de intercambio de claves y el algoritmo de cifrado seleccionado.
  - Envía también tipo de compresión.

Universidad Rey Juan Carlos

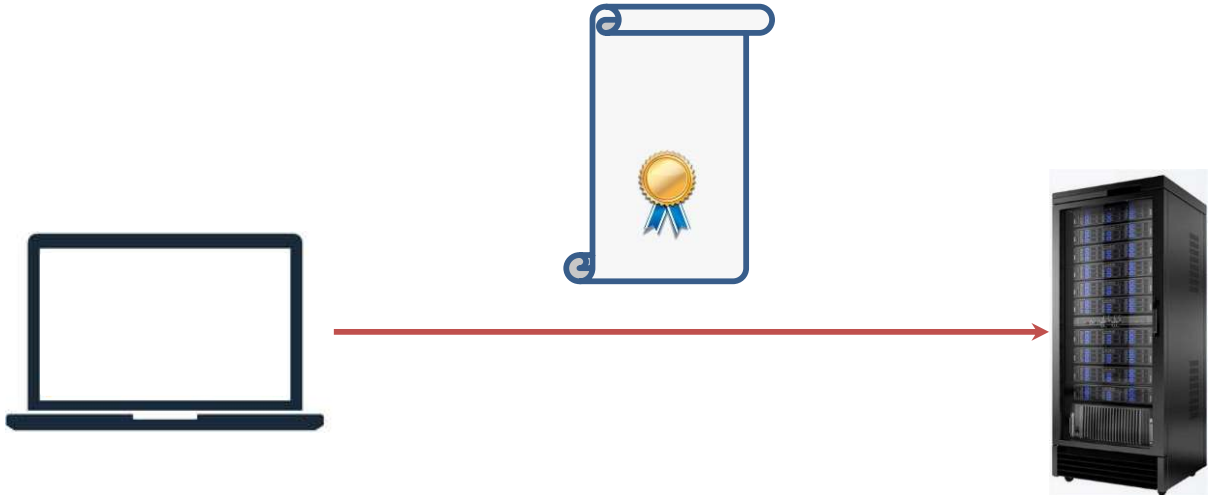
**Fase 2:**



- Server:
  - Envía su certificado
  - Solicita el certificado del cliente.
  - Manda el mensaje “`ServerHelloDone`”

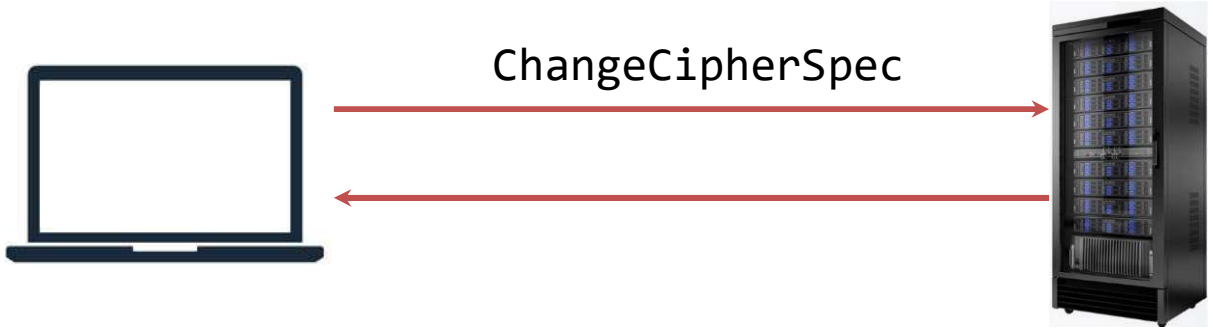
Universidad Rey Juan Carlos

**Fase 3:**



- Cliente:
  - Envía su certificado
  - Envía cifrada un *pre-master secret* para el intercambio de claves.

**Fase 4:**



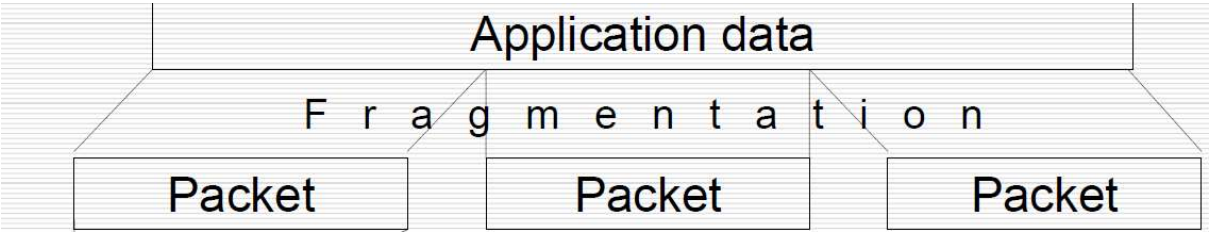

- Servidor:
  - Desencripta el *pre-master secret* y genera el *master secret.*
- Cliente:
  - Genera el *master secret.*
  - Envía el mensaje `ChangeCipherSpec`
- Servidor:
  - Confirma el `ChangeCipherSpec`

**Record Protocol:**

- Proporciona confidencialidad e integridad.

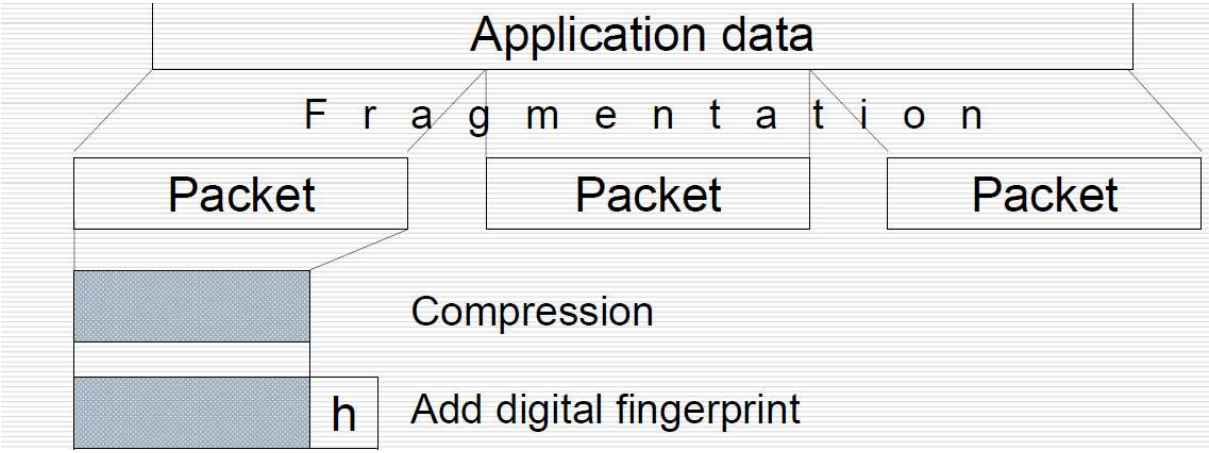
**Record Protocol:**

- Proporciona confidencialidad e integridad.
- Los datos de la aplicación se fraccionan.



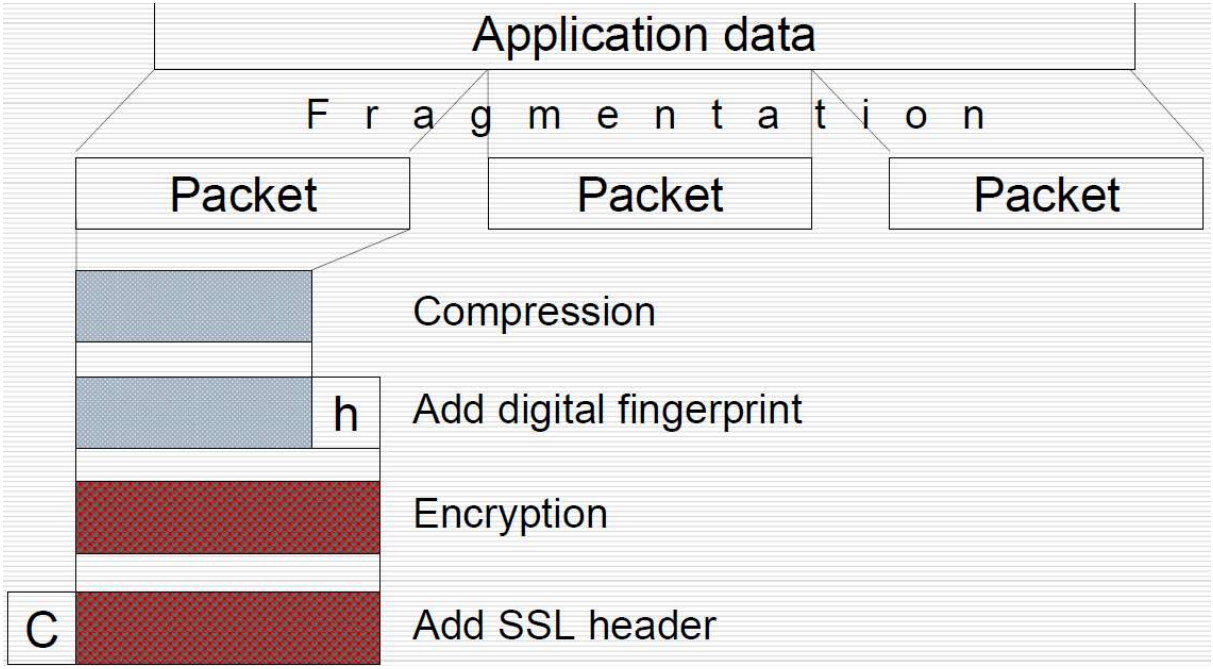
**Record Protocol:**

- Proporciona confidencialidad e integridad.
- Los datos de la aplicación se fraccionan.
- Cada fragmento se comprime y se calcula su MAC.



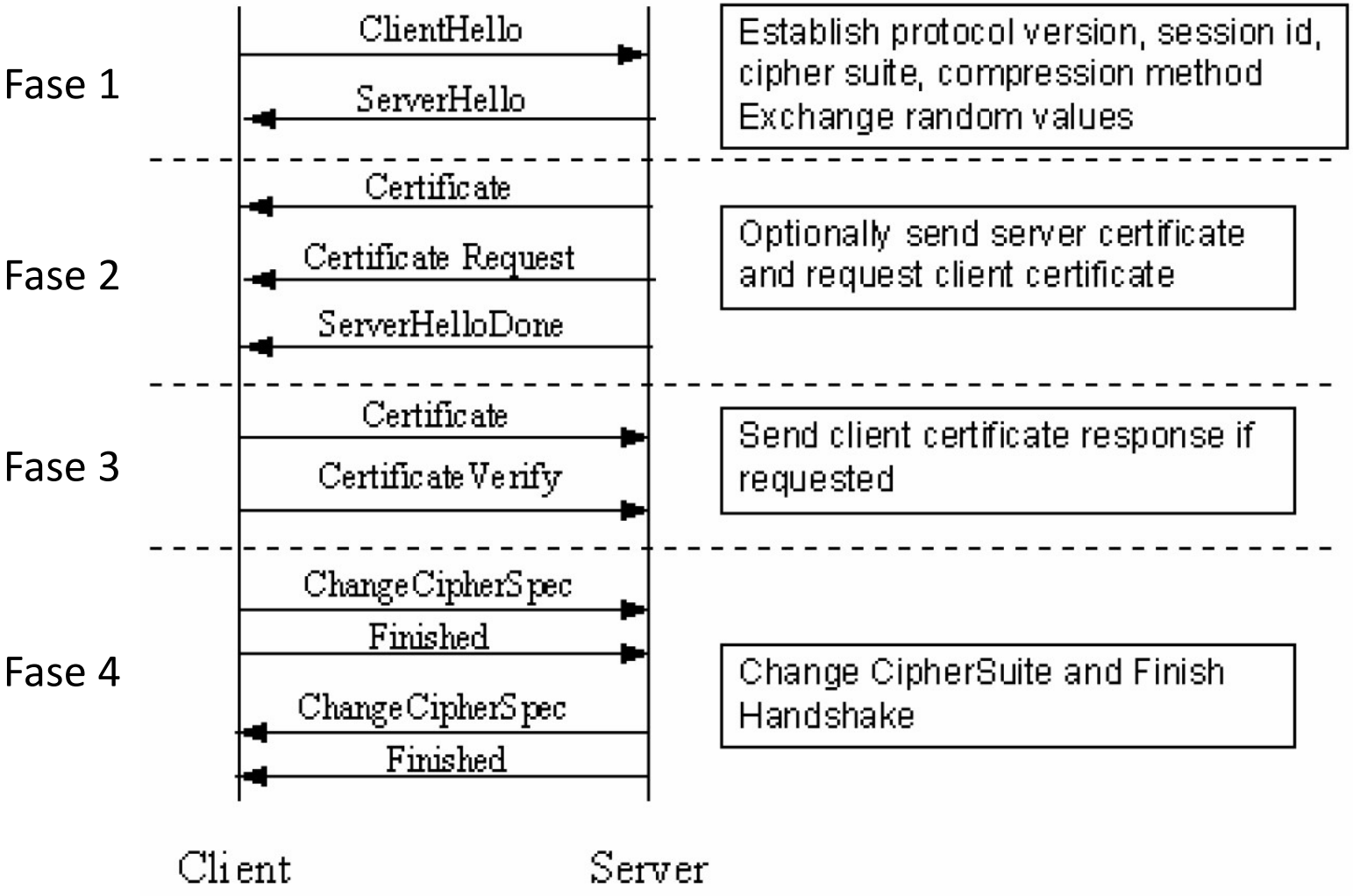
**Record Protocol:**

- Proporciona confidencialidad e integridad.
- Los datos de la aplicación se fraccionan.
- Cada fragmento se comprime y se calcula su MAC.
- El resultado se encripta y se añade la cabecera SSL



# SSL/TLS





# Índice

Universidad Rey Juan Carlos

- Introducción.
- Firewalls y DMZs.
- Honeypots.
- Redes Privadas Virtuales (VPN).
- IPSec.
- SSL/TLS.
- **Resumen.**

# Resumen

Universidad Rey Juan Carlos

- **IPSec VPN**:
  - Funciona en la capa de red.
  - Comunica de forma segura todos los datos entre los dos extremos, sin estar asociado a una aplicación en concreto.
  - Una vez lograda la conexión, el equipo remoto tendrá acceso total a la red corporativa.
  - La negociación de los parámetros de seguridad y la configuración de los extremos es compleja.
  - Los nodos intermedios deben permitir el paso de tráfico IPSec.

# Resumen

Universidad Rey Juan Carlos

- **SSL VPN**:
  - Funciona en la capa de aplicación.
  - Comunica de forma segura datos enviados vía web.
  - Emplea el navegador web como cliente, por lo que es más flexible y puede usarse desde más equipos (no requiere instalación de SW específico).
  - Control de acceso más detallado que con IPSec (especifica recursos a los que se tiene acceso).
  - Más simple que IPSec (su paso por nodos intermedios está generalmente aceptado, puerto 443).
- Tres modos de funcionamiento:
  - Clientless / Thin client / Tunnel mode

# Redes Privadas Virtuales

Universidad Rey Juan Carlos

- IPSec:
  - Tendremos una conexión permanente con control de acceso inicial.
  - Se emplea para dar acceso a entornos y equipos controlados.

- SSL:
  - Se usa para dar acceso a usuarios en movilidad, que se conectan desde cualquier equipo o sitio que no está controlado.
  - Debemos controlar a qué aplicaciones y datos se conecta.