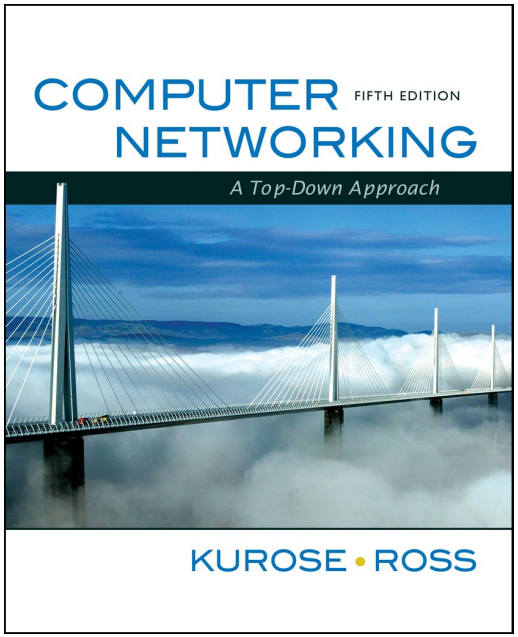
Capítulo 8
Seguridad en Redes
WEP, FW, IDS



Basado en:
Computer Networking: A Top Down Approach,
5th edition.
Jim Kurose, Keith Ross
Addison-Wesley, April 2009.

Capítulo 8 contenidos

8.1 ¿Qué es la seguridad en la red?

8.2 Principios de criptografía

8.3 Integridad de mensajes

8.4 Dando seguridad a e-mail

8.5 Conexiones TCP seguras: SSL

8.6 Seguridad en capa de Red: IPsec (lo saltamos)

8.7 Seguridad en redes locales inalámbricas

8.8 Cortafuegos y Sistemas de detección de intrusión (IDS)

Capítulo 8 contenidos

8.1 ¿Qué es la seguridad en la red?

8.2 Principios de criptografía

8.3 Integridad de mensajes

8.4 Dando seguridad a e-mail

8.5 Conexiones TCP seguras: SSL

8.6 Seguridad en capa de Red: IPsec (lo saltamos)

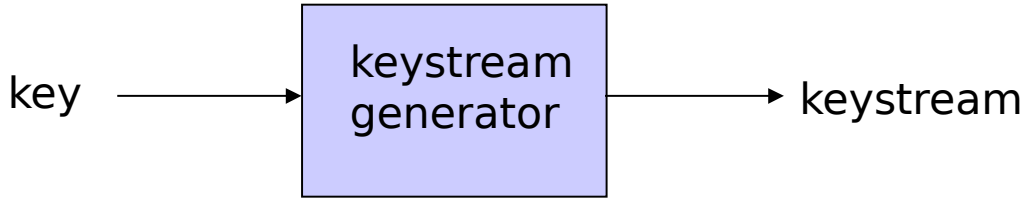
8.7 Seguridad en redes locales inalámbricas

8.8 Cortafuegos y Sistemas de detección de intrusión (IDS)

Wired Equivalent Privacy:WEP Objetivos de diseño

- Cifrado de clave simétrica
  - Confidencialidad
  - Autorización de acceso
  - Integridad de datos
- Auto sincronización: cada paquete es cifrado separadamente
  - Dado un paquete cifrado y una clave, podemos descifrarlo; podemos continuar descifrado aún cuando el paquete previo se ha perdido.
  - Distinto a Cifrado de bloques en cadena (Cipher Block Chaining, CBC)
- Eficiente
  - Puede ser implementado en software o hardware

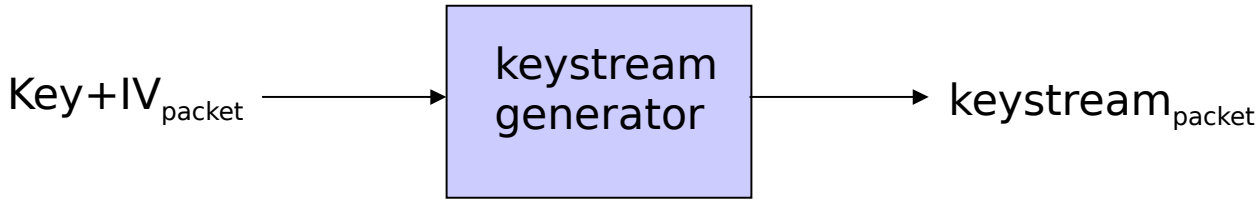
Recordemos: Cifrado simétrico de flujos



- Combina cada byte del keystream con byte de texto plano para obtener texto cifrado
- m(i) = i° unidad de mensaje
- ks(i) = i° unidad del keystream
- c(i) = i° unidad del texto cifrado
- $c(i) = ks(i) \oplus m(i)$ ($\oplus$ = or-exclusive)
- $m(i) = ks(i) \oplus c(i)$
- WEP usa RC4

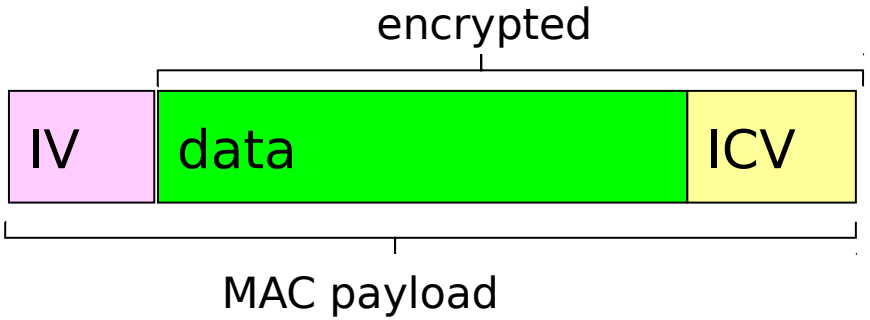
Cifrado de flujo e independencia de paquetes

- Recordemos el objetivo de diseño: cada paquete debe cifrarse separadamente
- Si para trama n+1, usamos keystream desde donde quedó en trama n, no se cumple cifrado independiente de tramas
  - Pues necesitamos saber dónde terminamos en paquete n
- Esquema WEP: se inicia el keystream con clave y vector de iniciación (Initialization Vector) por cada paquete:

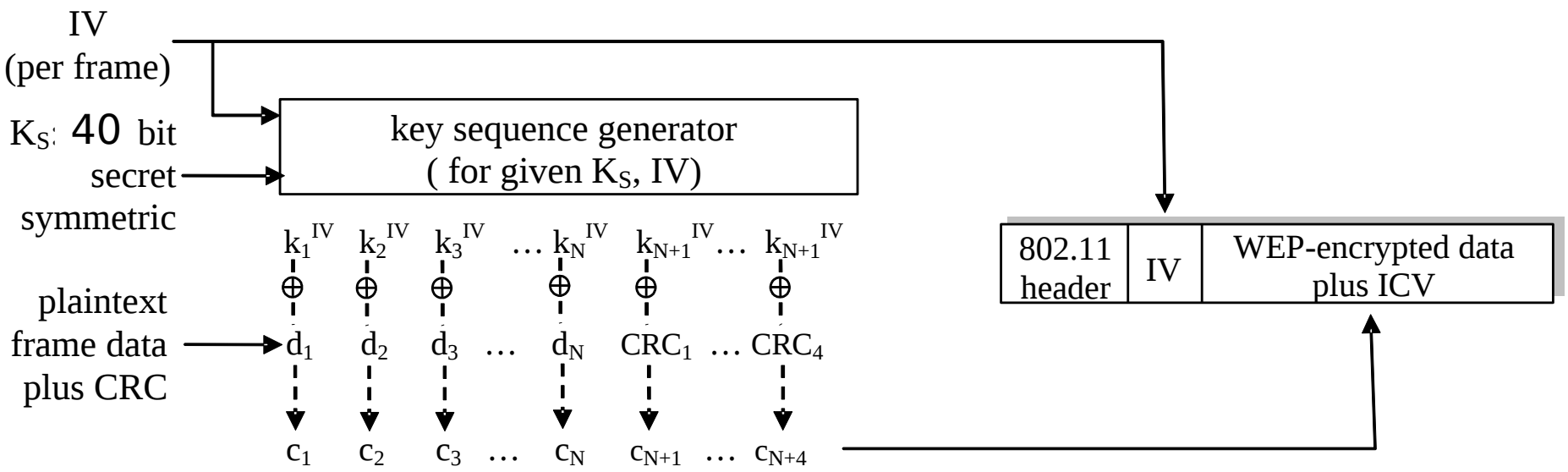


Encriptación WEP (1)

- Tx calcula un **V**alor de **C**hequeo de **I**ntegridad (ICV) de los datos
  - Es un hast/CRC de 4 bytes para integridad a los datos
- Cada extremo tiene una clave compartida de 40 bits.
- Tx crea un vector de iniciación (IV) de 24 bits y lo agrega a la clave: se tiene clave de 64 bits
- Clave de 64 bits ingresa al algoritmo pseudo aleatorio para generar keystream
- La trama + ICV es encriptado con RC4:
  - Or-ex de bytes de keystream con bytes de datos e ICV
  - IV e ID de clave son agregadas a los datos cifrados
  - El resultado es insertado en trama 802.11

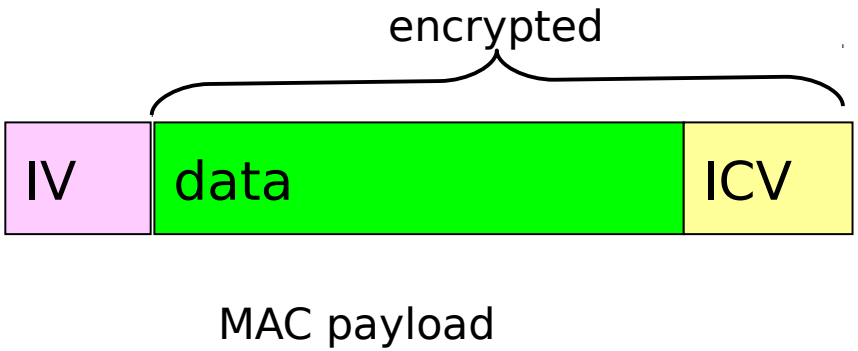


Encriptación WEP (2)



IV nuevo por cada frame

Descifrando WEP



- Rx extrae IV
- Ingresa IV y secreto compartido en generador pseudo aleatorio, obtiene keystream
- Hace OR-EX de keystream con datos encriptados, así obtiene datos e ICV
- Verifica integridad de los datos con ICV

Autenticación WEP

No todos los APs lo hacen, Aún si usan WEP. AP indica en beacon si autenticación Es requerida. Es hecha Antes de la asociación.

AP

Requerimiento de autenticación

Número único (128 bytes)

Número único cifrado con clave compartida

Éxito si número único corresponde

Vulnerando cifrado WEP 802.11

Hoyo de seguridad:

- IV de 24-bit y uno por trama -> IV es reusado en algún momento
- IV no es cifrado -> reuso de IV es detectado
- Ataque:
  - Intruso causa que Alicia cifre texto conocido d_1 d_2 d_3 ...
  - Intruso ve: $c_i = d_i$ XOR k_i^{IV}
  - Intruso conoce c_i d_i, puede calcular k_i^{IV}
  - Así intruso llega a saber la secuencia de claves k_1^{IV} k_2^{IV} k_3^{IV} ...
  - La próxima vez que IV es usado, el intruso puede descifrar mensaje!
- Hoy existen mejores opciones, por ejemplo EAP: extensible authentication protocol

Capítulo 8 contenidos

8.1 ¿Qué es la seguridad en la red?

8.2 Principios de criptografía

8.3 Integridad de mensajes

8.4 Dando seguridad a e-mail

8.5 Conexiones TCP seguras: SSL

8.6 Seguridad en capa de Red: IPsec (lo saltamos)

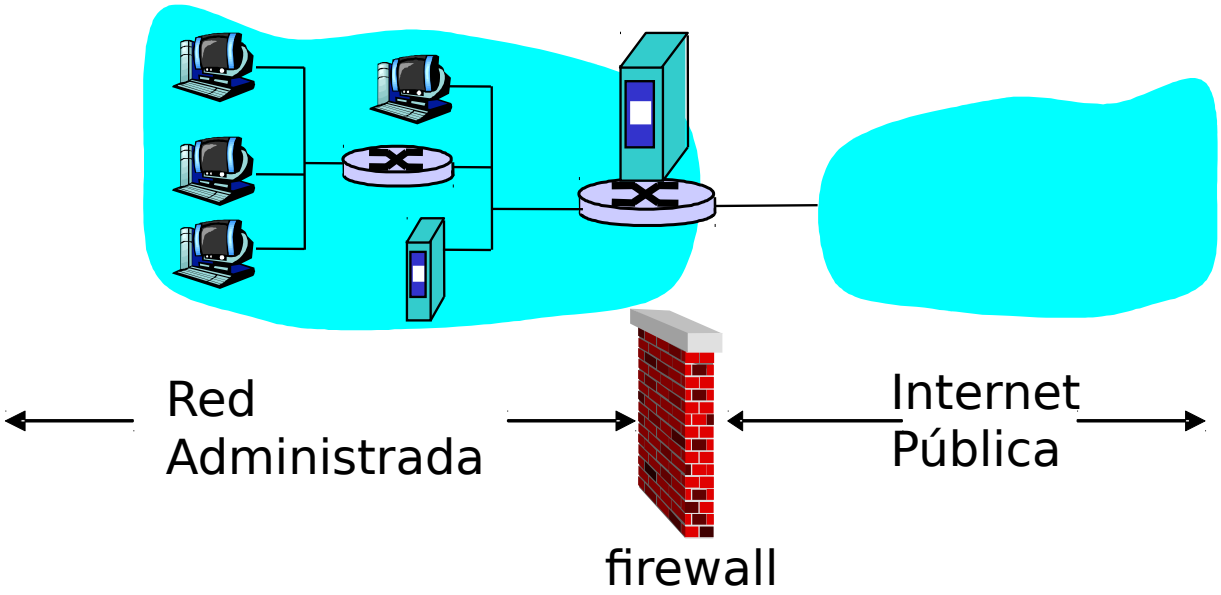
8.7 Seguridad en redes locales inalámbricas

8.8 Cortafuegos y Sistemas de detección de intrusión (IDS)

Cortafuegos

Cortafuegos

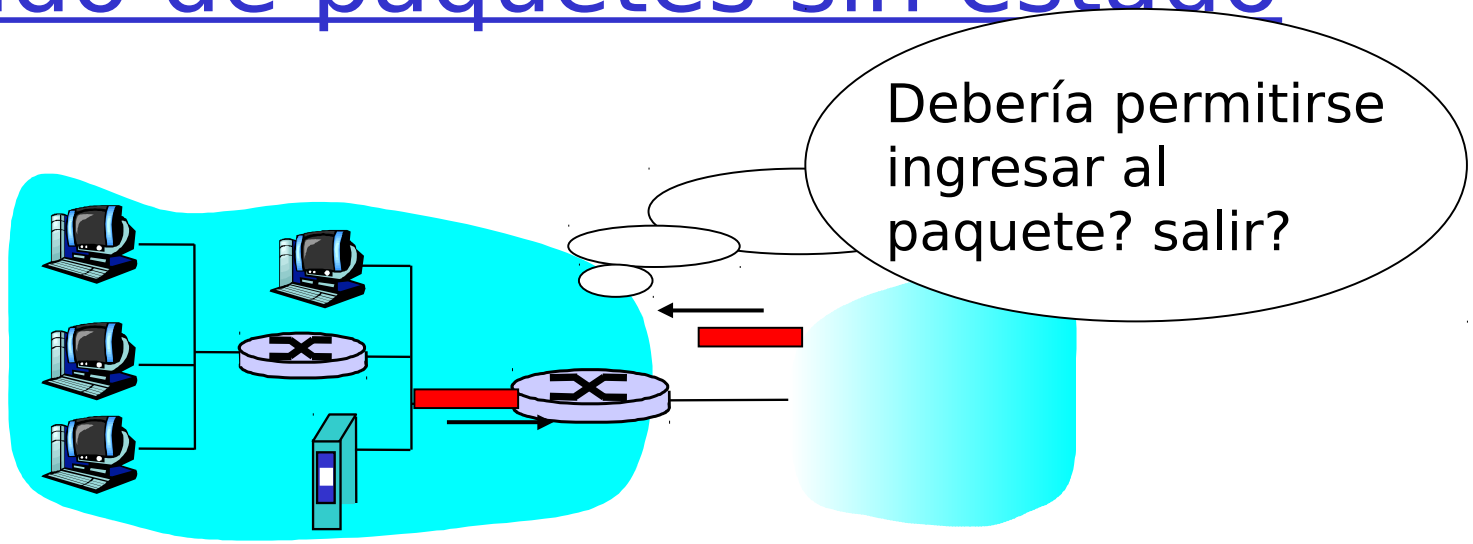
Aísla la red interna de la organización de Internet, permite pasar a algunos paquetes y bloquea otros.



Cortafuegos: ¿Por qué?

- Previene ataques de denegación de servicio:
  - Inundación de SYN: atacante establece muchas conexiones TCP inconclusas, no deja recursos para las reales.
- Previene modificación/acceso ilegal a datos internos.
  - e.g., atacante cambia la página web del Depto.
- Permite sólo accesos autorizados al interior de la red.
- Hay tres tipos de cortafuegos:
  - Filtros de paquete sin estado
  - Filtro de paquetes con estado
  - Gateways de aplicación

Filtrado de paquetes sin estado



- Red interna conectada a Internet vía router cortafuego
- router filtra paquete por paquete, decisión es basada en:
  - IP fuente, IP destino
  - Número de puertos fuente y destino TCP/UDP
  - Tipo de mensaje ICMP
  - Bits SYN y ACK de TCP

Ejemplo de filtrado sin estado

- Ejemplo 1: bloquear datagramas de entrada y salida campo protocolo IP = 17 o con puerto fuente o destino = 23.
  - Bloquea todo flujo UDP de entrada y salida, y bloquea conexiones telnet
- Ejemplo 2: Bloquee segmentos TCP entrantes con ACK=0.
  - Impide a clientes externos hacer conexiones TCP con clientes internos, pero en el otro sentido sí se permite.

Más ejemplos de filtrado sin estado

Política	Configuración de Firewall
No permitir acceso a Web externo.	Descarte todo paquete saliente a puerto 80, cualquier IP
No conexiones TCP entrantes, excepto a servidor web de la institución.	Descarte todo SYN TCP a cualquier IP excepto a 130.207.244.203, puerto 80
Impedir que radios Web consumanbandwidth.	Descartar todo paquete UDP entrante excepto DNS y broadcasts de routers.
Impedir que hagan traceroute sobre la red	Descartar todo paquete ICMP de salida señalando TTL expirado

Listas de control de acceso (ACL)

- *ACL:* Tabla de reglas, aplicada de arriba a abajo a paquetes de paso: pares (acción, condición)

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Filtrado de paquetes con estado

- Filtrado sin estado
  - Admite paquetes que “no hacen sentido”; ej. puerto destino = 80, ACK bit fijado, aún cuando no existe conexión TCP establecida:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *Filtrado con estado:* sigue estado de cada conexión TCP
  - Sigue los SYN, FIN: Puede determinar si los paquetes “hacen sentido”
  - Puede hacer timeout de conexiones inactivas: no acepta más paquetes

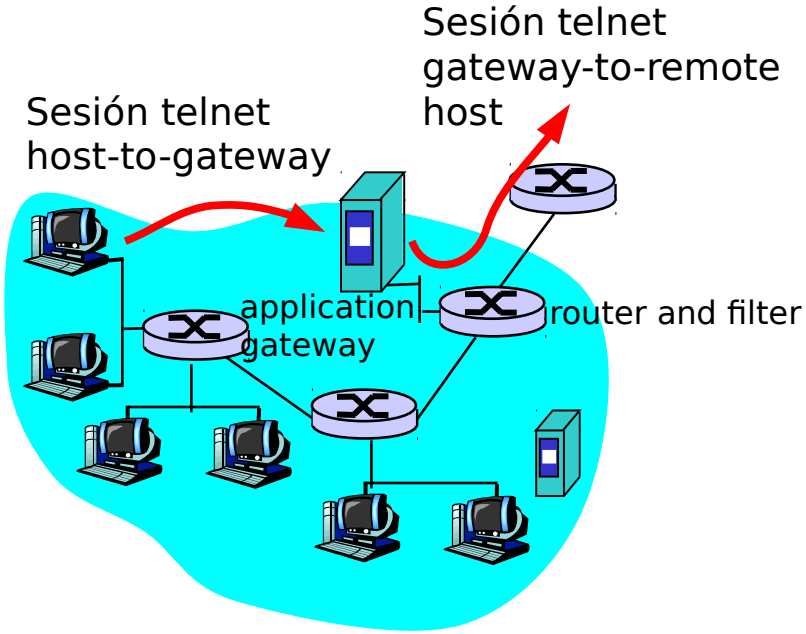
Filtrado con estado

- ACL aumentada para indicar la necesidad de verificar el estado de la conexión antes de admitir paquete

action	source address	dest address	proto	source port	dest port	flag bit	check connection
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Gateway de Aplicación

- Filtra paquetes según datos de aplicación y también campos IP/TCP/UDP.
- Ejemplo: permite hacer telnet sólo a usuarios seleccionados.



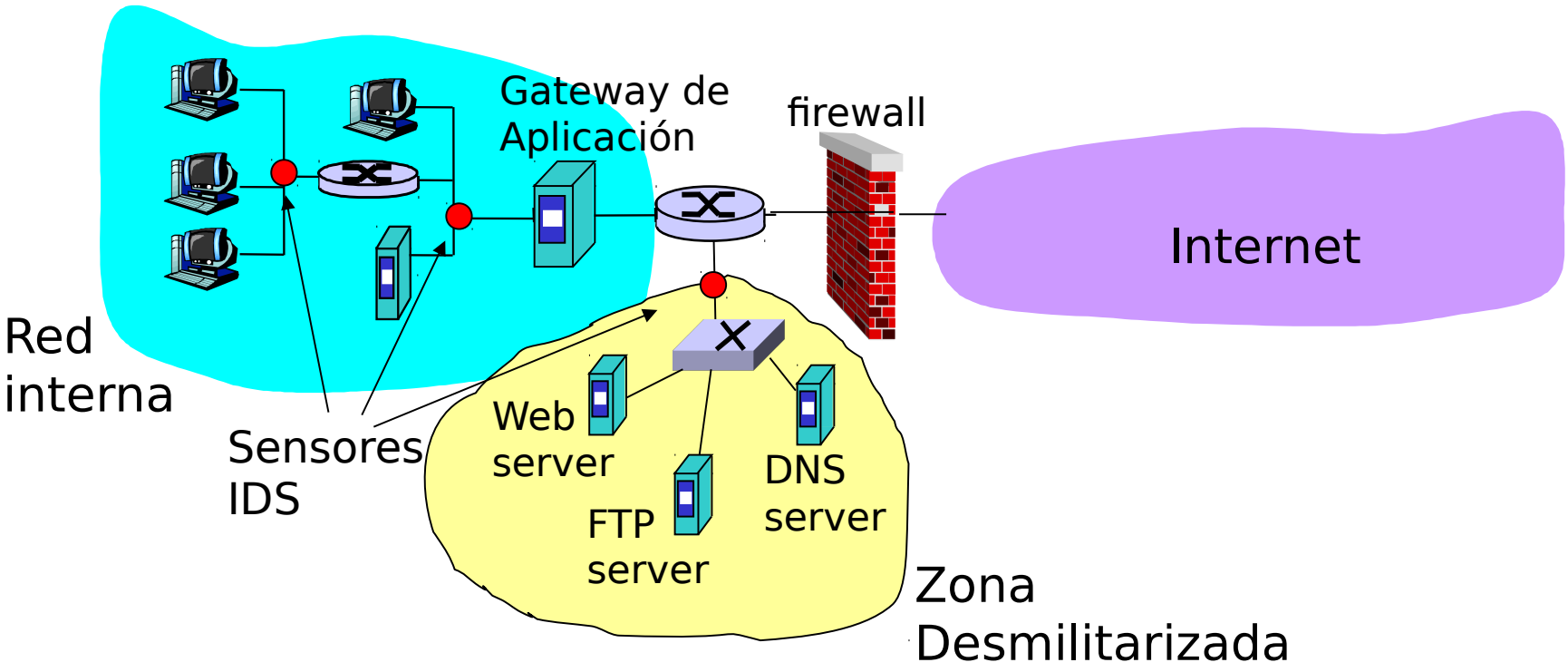
1. Requiere que todo telnet sea hecho a través del gateway.
2. Para los autorizados, el gateway hace la conexión al host destino. Gateway hace reenvío entre las dos conexiones.
3. El router filtra todo telnet que no venga desde el gateway.

IDS Intrusion detection systems (sistemas de detección de intrusión)

- Filtrado de paquetes:
  - Operan sólo sobre encabezados TCP/IP
  - No hay correlación entre sesiones
- *IDS: intrusion detection system*
  - *Hacen inspección profunda del paquete:* Se fija en contenido (ej. revisa contenido en base de datos buscando virus, ataques etc.)
  - examina correlación entre múltiples paquetes
    - Scaneo de puertos
    - Mapeo de la red
    - Ataques de DoS

Intrusion detection systems

- múltiple IDSs: diferentes tipos de chequeo en diferentes puntos



Seguridad en Redes (resumen)

Técnicas básicas……

- Criptografía (simétrica y pública)
- Integridad de mensajes
- Autenticación entremo a extremo

…. son usadas en muchos escenarios de seguridad

- email
- Capa transporte (SSL)
- Capa de red IP sec (lo saltamos)
- 802.11 (Wifi)

Seguridad Operacional: Cortafuegos e IDS