11

SEGURIDAD OPERACIONAL EN REDES LAN

Objetivo

- Describir cómo utilizar firewalls y dispositivos IDS para proteger la infraestructura de la red frente a potenciales ataques maliciosos.

Manual de clases

Última modificación:
4 de noviembre de 2022

Tema 11 de:
SEGURIDAD EN REDES

Edison Coimbra G.

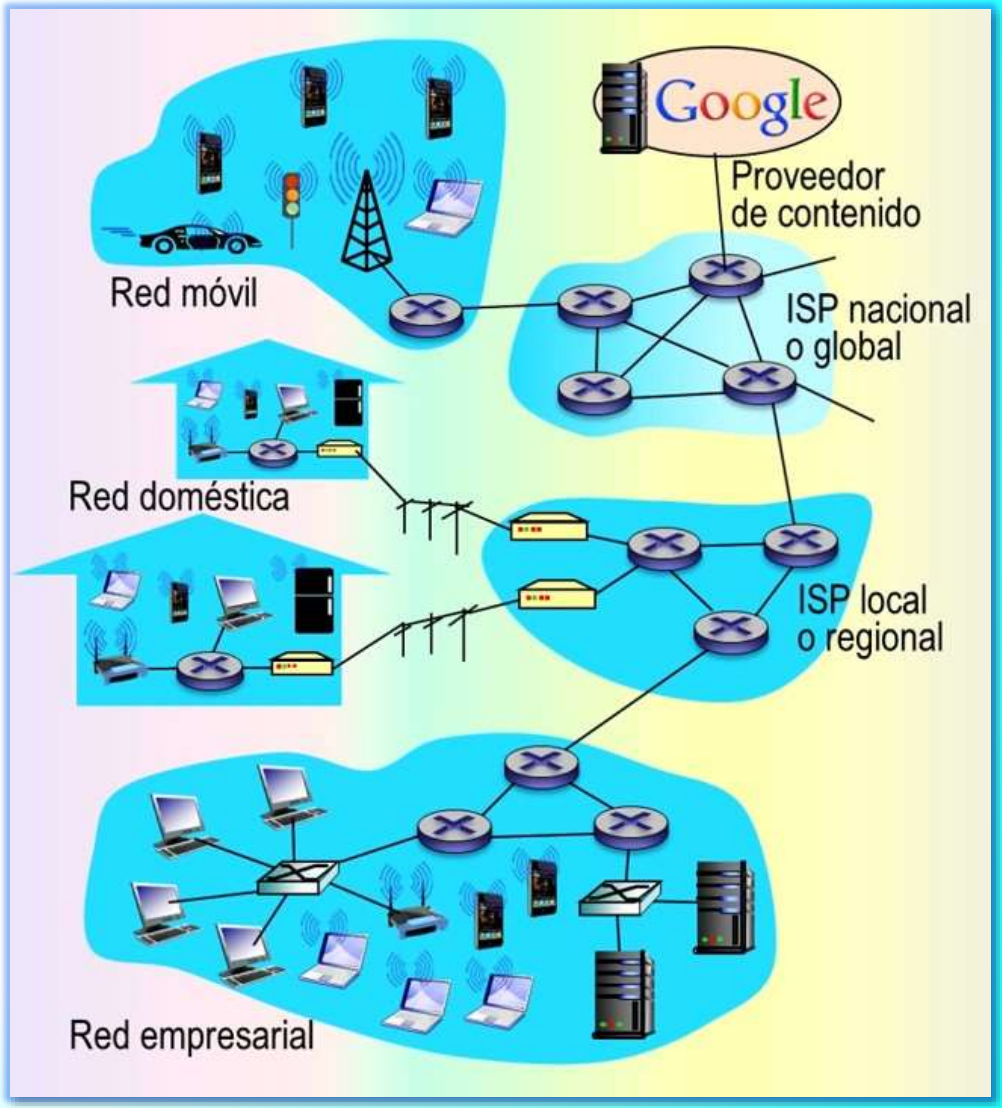
1. LA SEGURIDAD EN REDES

SEGURIDAD OPERACIONAL EN REDES LAN

(Kurose, 2017)

¿A qué hace referencia la seguridad en las redes?

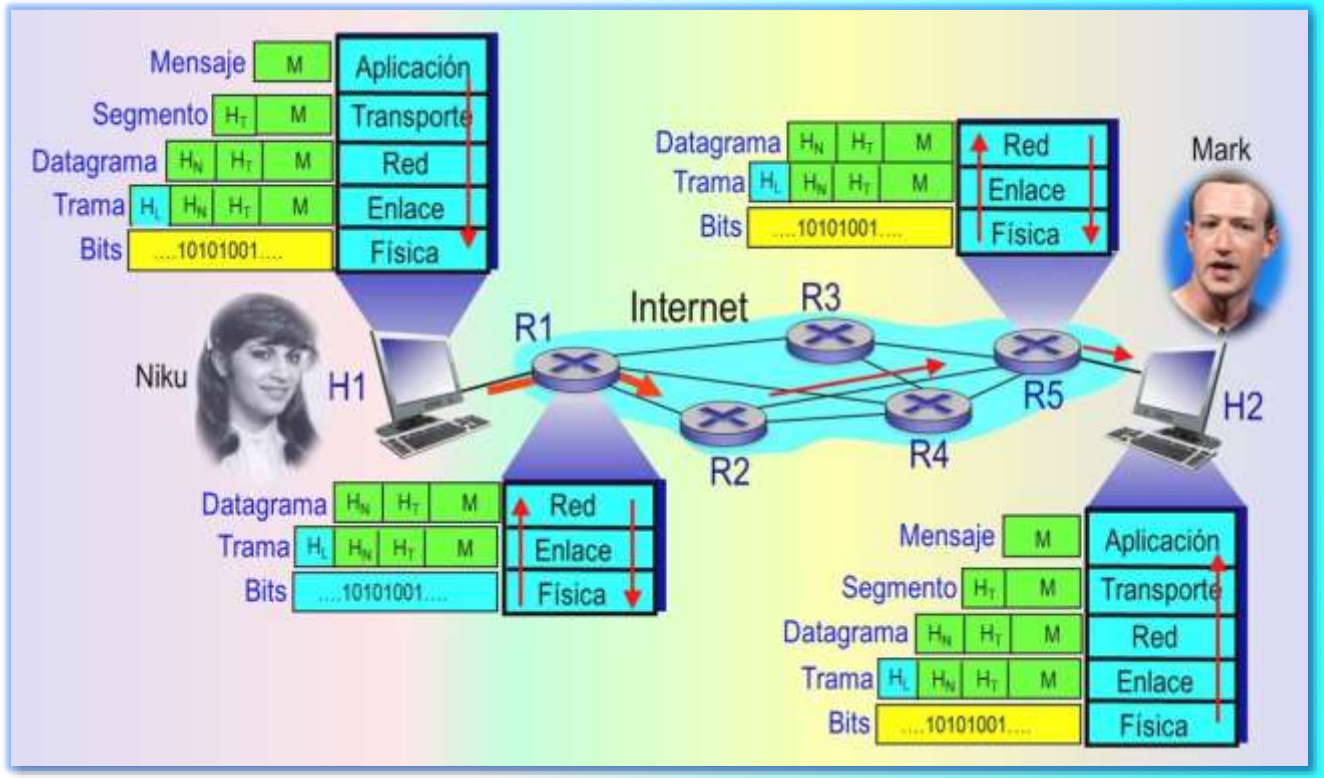
- **Internet** se ha convertido en una herramienta crítica para muchas instituciones, incluyendo empresas pequeñas y medianas, universidades y organismos gubernamentales.
- **Muchas personas** confían en Internet para llevar a cabo sus actividades profesionales, sociales y personales. Miles de millones de "cosas" (incluyendo dispositivos corporales y electrodomésticos) se conectan hoy en día a Internet.
- **Detrás** de todas estas utilidades y toda esta excitación, hay un lado oscuro: desde el punto de vista de un administrador de red, el mundo se divide de forma bastante nítida en dos bandos:
  - ▶Los buenos, aquellos que pertenecen a la red de la organización y que deben poder acceder a los recursos internos de la misma de una forma relativamente poco restringida y….
  - ▶Los malos, todos los demás, aquellos que deben ser cuidadosamente escrutados a la hora de acceder a los recursos de la red.
- **El campo de la seguridad de red** se ocupa de ver cómo "los malos" pueden atacar a las redes de computadoras y cómo se las puede defender de esos ataques, o mejor todavía, de cómo diseñar nuevas arquitecturas que sean inmunes a tales ataques.



SEGURIDAD OPERACIONAL EN REDES LAN

¿Por qué Internet se ha convertido en un lugar inseguro? (Kurose, 2017)

- **Básicamente**, la respuesta es que Internet fue diseñada originalmente de esa manera, ya que se basaba en el modelo de un “grupo de usuarios que confiaban entre sí, conectados a una red transparente”, un modelo en el que, por definición, no había necesidad de pensar en la seguridad.
- **Muchos aspectos** de la arquitectura de Internet original reflejan profundamente esta idea de confianza mutua.
  - ✉Por ejemplo, la posibilidad de que un usuario envíe un paquete a cualquier otro usuario es la opción predeterminada, al igual que lo normal es creer que la identidad del usuario es la que declara, en lugar de autenticarle por defecto.
- **Pero actualmente Internet** no implica realmente "usuarios de confianza mutua”.

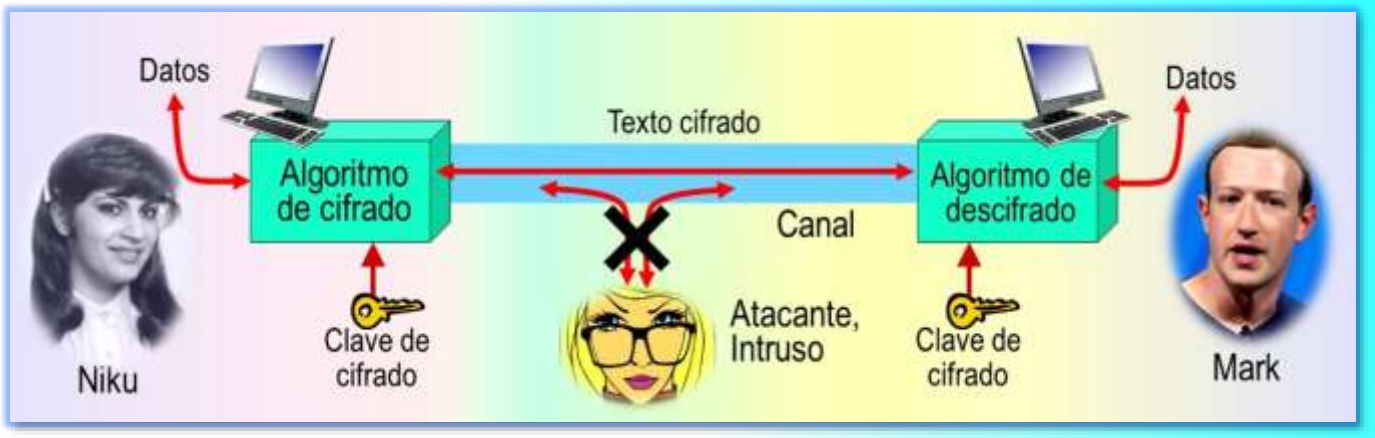


- **Sin embargo**, los usuarios de hoy día necesitan comunicarse aunque no necesariamente confíen entre sí. Pueden desconfiar del hardware, del software e incluso del aire a través del que se comunican.
- **Se tiene que tener presente** que la comunicación entre usuarios de mutua confianza es la excepción, mas que la regla. Este es el mundo de las redes modernas de comunicaciones.

SEGURIDAD OPERACIONAL EN REDES LAN

¿Qué es la seguridad de red?

(Kurose, 2017)



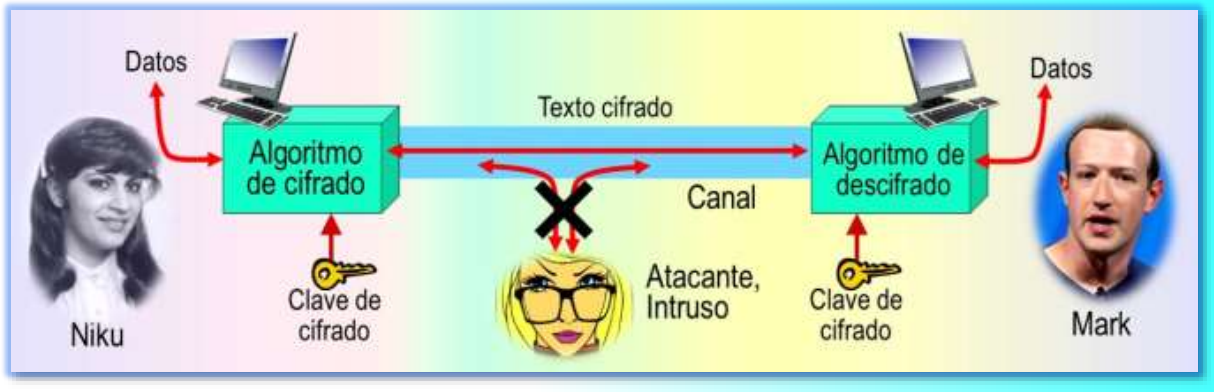
- **Para tener un visión panorámica** del escenario de la seguridad, se presenta a Niku y a Mark que desean comunicarse y desean hacerlo "de manera segura", resaltando que estas dos personas podrían ser:
  - ▶Dos routers que desean intercambiar sus tablas de routing en forma segura.
  - ▶Un cliente y un servidor que desean establecer una conexión de transporte segura.
  - ▶Dos aplicaciones de correo electrónico que quieren intercambiar mensajes de correo seguros.
- **Los asuntos** amorosos, las comunicaciones en tiempo de guerra y las transacciones de negocios son las necesidades humanas de comunicaciones seguras habituales.
- **Niku y Mark** desean comunicarse de "forma segura". En realidad, Niku quiere que solo Mark sea capaz de comprender los mensajes que ella envía, incluso aunque estén comunicándose a través de un medio no seguro en el que un **intruso** pueda interceptar lo que Niku transmite.
- **Mark también** quiere estar seguro de que el mensaje que él recibe de Niku fue realmente enviado por Niku, y Niku quiere estar segura de que la persona que se está comunicando con ella es realmente Mark. Ambos también quieren estar seguros que el contenido de sus mensajes no ha sido alterado en el camino.
- **Además**, quieren estar seguros de que siempre podrán comunicarse (es decir, que nadie les puede denegar el acceso a los recursos necesarios para comunicarse).

SEGURIDAD OPERACIONAL EN REDES LAN

Las cuatro propiedades de una comunicación segura

(Kurose, 2017)

- ▶**1. Confidencialidad**. Solo Niku y Mark deberán comprender el contenido de los mensajes transmitidos. Puesto que los atacantes o intrusos pueden interceptar los mensajes, es absolutamente necesario que los mensajes sean cifrados de alguna manera, de modo que un mensaje interceptado no pueda ser comprendido por el que lo ha interceptado.
  - ⌧Este aspecto de la confidencialidad es probablemente el concepto más comúnmente percibido del término comunicación segura.
- ▶**2. Integridad de los mensajes**. Niku y Mark cuando se comunican quieren estar seguros de que el contenido de sus comunicaciones no se vea alterado durante la transmisión ni maliciosamente ni por accidente.
  - ⌧Se pueden emplear extensiones a las técnicas de suma de comprobación en los protocolos de enlace y de transporte para proporcionar integridad a los mensajes.



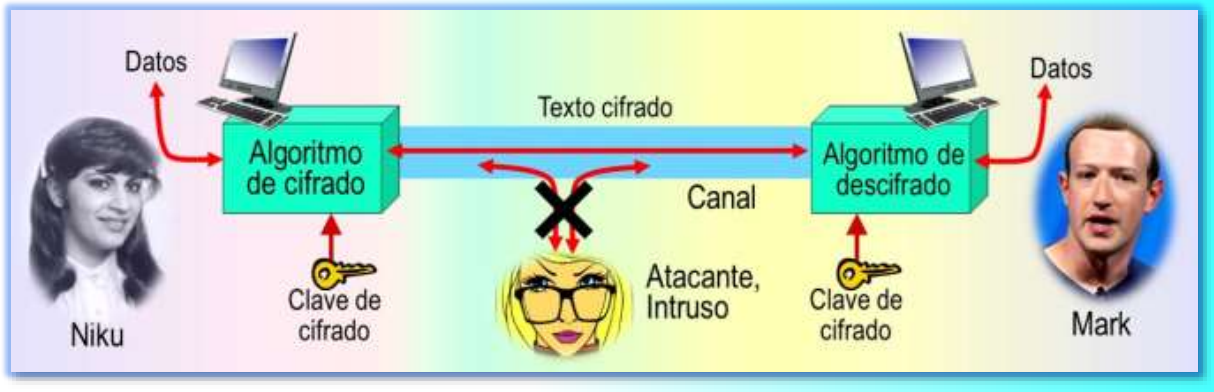
Propiedades de una comunicación segura			
1. Confidencialidad	**2. Integridad de los mensajes**	**3. Autenticación del punto terminal**	**4. Seguridad operacional**
Cifrado PGP para correo	Cifrado PGP para correo	Cifrado PGP para correo	Firewalls (Filtros de paquetes. Filtros con memoria del estado. Gateways de aplicación)
Protocolo TCP-SSL	Protocolo TCP-SSL	Protocolos de autenticación (Contraseñas y números distintivos)	Sistemas de Detección y de Prevención de Intrusiones
Protocolo IPsec (ESP)	Protocolo IPsec (AH, ESP)	Protocolo TCP-SSL Protocolo IPsec (AH, ESP)	Zonas de seguridad y zonas desmilitarizadas

SEGURIDAD OPERACIONAL EN REDES LAN

Las cuatro propiedades de una comunicación segura (cont.)

(Kurose, 2017)

- ▶**3. Autenticación del punto terminal**. Tanto Niku como Mark deberán poder confirmar la identidad del otro en el proceso de comunicación (confirmar que el otro es de hecho quien dice ser). La comunicación humana frente a frente resuelve este problema fácilmente gracias al reconocimiento visual.
  - ✉Cuando Niku y Mark se comunican a través de un medio en el que no es posible ver al otro, la autenticación no es tan sencilla. Por ejemplo, cuando un usuario accede a su bandeja de entrada ¿cómo verifica el servidor de correo que el usuario es la persona que dice ser?
- ▶**4. Seguridad operacional**. Casi todas las organizaciones (empresas, universidades, etc.) disponen de redes que están conectadas a Internet. Estas redes pueden, potencialmente, verse comprometidas. Los atacantes pueden intentar depositar gusanos en los hosts de la red, conseguir secretos corporativos, realizar un mapa de las configuraciones internas de la red y ejecutar ataques DoS.
  - ✉Para responder a estos ataques, se emplean dispositivos de seguridad operacional como los **firewalls** y los **sistemas de detección de intrusiones**, que protegen la infraestructura de la red

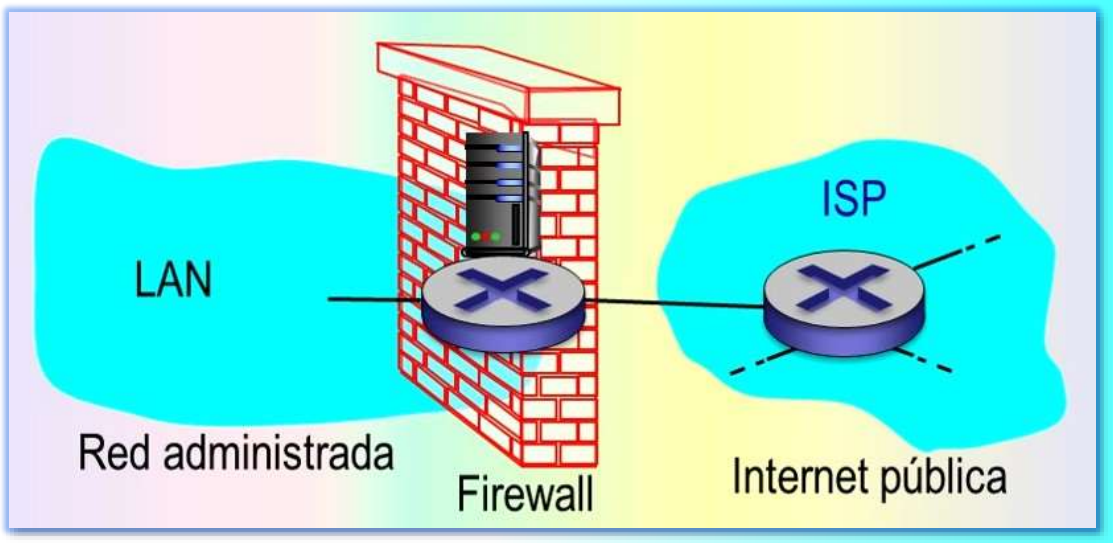


Propiedades de una comunicación segura			
1. Confidencialidad	**2. Integridad de los mensajes**	**3. Autenticación del punto terminal**	**4. Seguridad operacional**
Cifrado PGP para correo	Cifrado PGP para correo	Cifrado PGP para correo	Firewalls (Filtros de paquetes. Filtros con memoria del estado. Gateways de aplicación)
Protocolo TCP-SSL	Protocolo TCP-SSL	Protocolos de autenticación (Contraseñas y números distintivos)	Sistemas de Detección y de Prevención de Intrusiones
Protocolo IPsec (ESP)	Protocolo IPsec (AH, ESP)	Protocolo TCP-SSL Protocolo IPsec (AH, ESP)	Zonas de seguridad y zonas desmilitarizadas

SEGURIDAD OPERACIONAL EN REDES LAN

¿Cómo proteger la infraestructura de la red?

- **En muchas organizaciones**, desde los castillos medievales a los modernos edificios de oficinas, existe un único punto de entrada/salida donde se hace una comprobación de seguridad tanto de los buenos como de los malos que entran y salen de la organización.
  - ✉En un castillo esto se hacía en la puerta situada en el extremo de un puente levadizo.
  - ✉En un edificio de oficinas esto se hace en el control de seguridad de entrada.

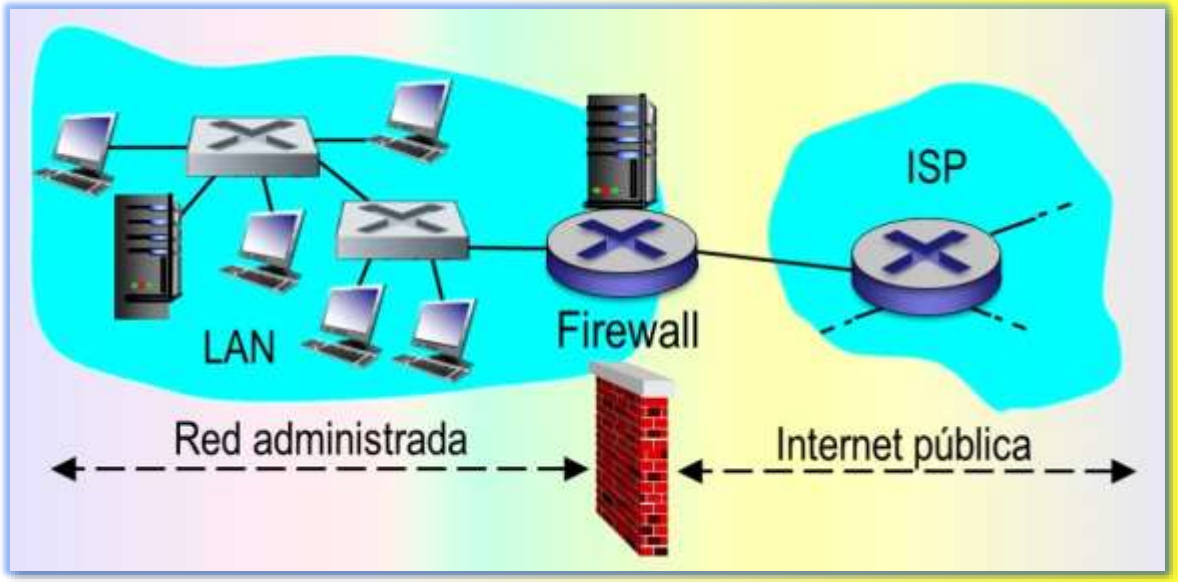


- **En una red de comunicación de datos**, cuando se tiene que comprobar si el tráfico que entra/sale de red es seguro, cuando se tiene que registrar ese tráfico y cuando se tiene que eliminar o reenviar, quienes se encargan de esas tareas son una serie de dispositivos operacionales conocidos como:
  - ▶**Firewalls** o cortafuegos.
  - ▶**IDS**, sistemas de detección de intrusiones.
  - ▶**IPS**, sistemas de prevención de intrusiones.

¿Qué es un firewall?

(Kurose, 2017)

- **Un firewall** es una combinación de hardware y software que aísla la red interna de la organización de Internet, permitiendo pasar a algunos paquetes y bloqueando a otros. Permite a un administrador de red controlar el acceso desde el mundo exterior a los recursos de la red administrada, gestionando el flujo de tráfico hacia y desde esos recursos. Un firewall tiene tres objetivos:
  - ▶**1.** Todo el tráfico que va desde el exterior hacia el interior de la red, y viceversa, pasa a través del firewall. El firewall se sitúa en el límite entre la red administrada y la Internet pública. Aunque las organizaciones grandes pueden utilizar varios niveles de firewalls o firewalls distribuidos, el colocar uno en un único punto de acceso a la red, facilita la gestión y el imponer una política de control de acceso.
  - ▶**2.** Solo permite el paso del tráfico autorizado de acuerdo con la política de seguridad local. Si todo el tráfico de entrada y de salida de la red institucional pasa a través del firewall, este puede restringir el acceso al tráfico autorizado.



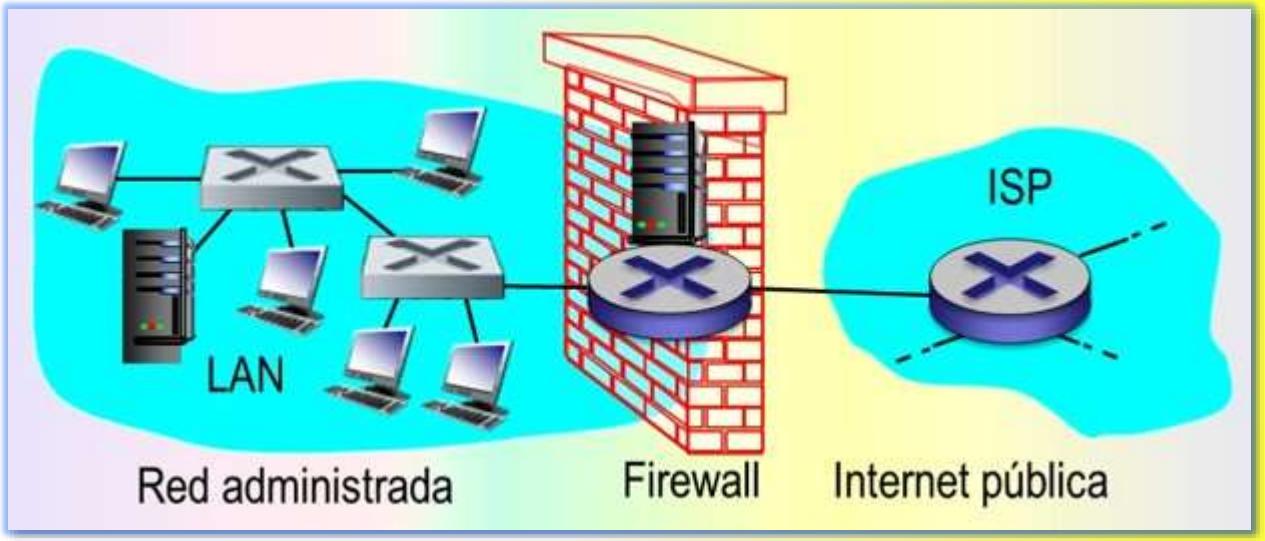
  - ▶**3.** El propio firewall es vulnerable a la penetración, pues es un dispositivo conectado a la red. Si no está diseñado o instalado apropiadamente puede verse comprometido, en cuyo caso solo proporciona una falsa sensación de seguridad (lo que es peor que no disponer de firewall).

SEGURIDAD OPERACIONAL EN REDES LAN

Clasificación de los firewalls

(Kurose, 2017)

- **Cisco y Ckeck Point** son dos de las empresas líderes actuales de distribución de firewalls.
- **Un firewall** también puede crearse fácilmente a partir de una máquina Linux utilizando *iptables* (software de dominio público, que se suministra habitualmente con Linux).
- **Además**, ahora los firewalls se implementan frecuentemente en los router y se controlan de forma remota mediante SDN, redes definidas por software.



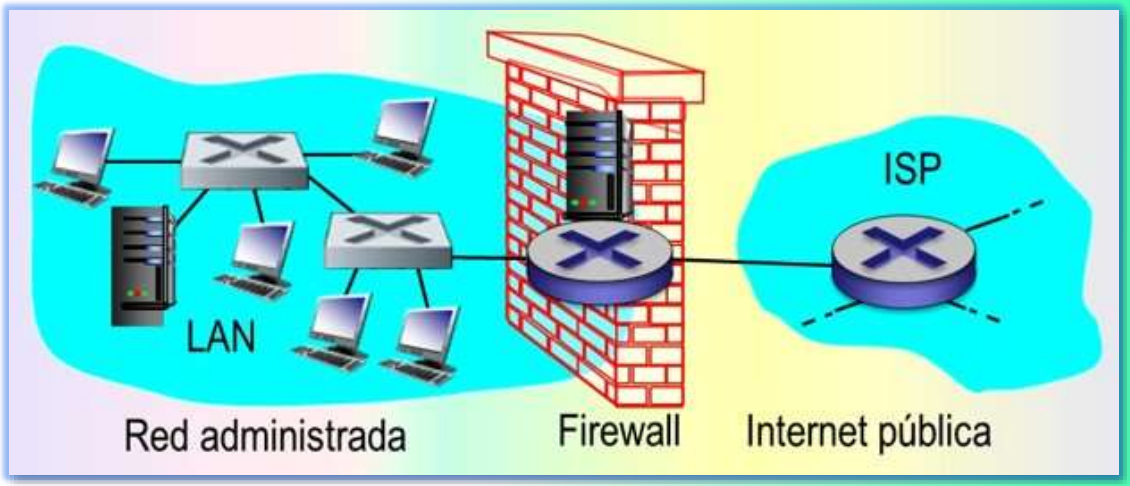
- **Los firewalls** se pueden clasificar en **tres categorías:**
  - Filtros de paquetes tradicionales.
  - Filtros con memoria del estado.
  - Gateways de aplicación.

SEGURIDAD OPERACIONAL EN REDES LAN

¿En qué se basan las decisiones de filtrado?

(Kurose, 2017)

- **Una organización** dispone normalmente de un router gateway que conecta su red LAN con su ISP (y por tanto con la internet publica). Todo el tráfico que sale y entra de la red LAN pasa a través de este router y es en este router donde tiene lugar el filtrado de paquetes.



- **Un filtro de paquetes** examina cada datagrama aisladamente, determinando si debe pasar o debe ser eliminado basándose en las reglas especificadas por el administrador. Las decisiones de filtrado normalmente se basan en:
  - Las direcciones IP de origen o de destino.
  - El tipo de protocolo especificado en el campo de datagrama IP: TCP, UDP, ICMP, OSPF, etc.
  - El puerto de destino y de origen TCP o UDP.
  - Los bits indicadores de TCP: SYN, ACK, etc.
  - El tipo de mensaje ICMP.
  - Diferentes reglas para los datagramas que salen y entran en la LAN.
  - Diferentes reglas para las distintas interfaces del router.
- **Un administrador de red** configura el firewall con base en la política de la organización. La política puede tener en cuenta la productividad del usuario y el uso de ancho de banda, así como los problemas de seguridad de una organización.

SEGURIDAD OPERACIONAL EN REDES LAN

Políticas y reglas de filtrado

(Kurose, 2017)

- **La tabla enumera** algunas de las posibles políticas que una organización puede tener y como podrían controlarse mediante un sistema de filtrado de paquetes.
  - ▶Por ejemplo, la política 2., si la organización no desea permitir ninguna conexión TCP entrante excepto aquellas destinadas a su servidor web público, entonces puede bloquear todos los segmentos TCP SYN entrantes, salvo aquellos cuyo puerto de destino sea el puerto 80 y cuya dirección IP de destino sea la correspondiente al servidor web.

Políticas y reglas de filtrado correspondientes de la red 130.207.0.0/16 de una organización con un servidor web en 130.207.244.203

Política	Configuración del firewall
1.Sin acceso web externo.	Eliminar todos los paquetes salientes hacia cualquier dirección IP, puerto 80.
2.Sin conexiones TCP entrantes, excepto las destinadas al servidor web público de la organización.	Eliminar todos los paquetes TCP SYN entrantes hacia cualquier IP, excepto 130.207.244.203, puerto 80.
3.Impedir que las aplicaciones de radio web consuman el ancho de banda disponible.	Eliminar todos los paquetes UDP entrantes, excepto los paquetes DNS.
4.Impedir que la red sea utilizada para llevar a cabo un ataque DoS distribuido.	Eliminar todos los paquetes ping ICMP hacia una dirección de "difusión" (por ejemplo, 130.207.255.255)
5.Impedir que la red sea examinada con Traceroute.	Eliminar todo el tráfico ICMP TTL saliente caducado.

- ▶La política 3, si la organización no desea que sus usuarios monopolicen el ancho de banda de acceso con aplicaciones de radio por Internet, puede bloquear todo el tráfico UDP no critico (ya que la radio por Internet a menudo se transmite sobre UDP).
- ▶La política 5, si la organización no desea que su red interna sea analizada (con Traceroute) por alguien externo, puede bloquear todos los mensajes ICMP TTL caducados que salen de la red de la organización.

SEGURIDAD OPERACIONAL EN REDES LAN

Lista de control de acceso

(Kurose, 2017)

- **Las reglas de firewalls** se implementan en los router mediante listas de control de acceso, teniendo cada interfaz del router su propia lista. En la tabla se muestra un ejemplo de una lista de control de acceso para una organización 222.22.0.0/16.

- ▶**Política 1**. Los usuario de la red de la organización tienen permitido navegar por la Web.
  - ✉ La Acción 1 permite salir de la red a cualquier paquete TCP con el puerto de destino 80.
  - ✉ La Acción 2 permite entrar a la red a cualquier paquete TCP que tenga el puerto de origen 80 y el bit ACK activado.

Lista de control de acceso para una interfaz de router de la organización 222.22/16

Acción	Dirección de origen	Dirección de destino	Protocolo	Puerto de origen	Puerto de destino	Bit indicador
1.Permitir	222.22/16	Fuera de 222.22/16	TCP	>1023	80	Cualquiera
2. Permitir	Fuera de 222.22/16	222.22/16	TCP	80	>1023	ACK
3 Permitir	222.22/16	Fuera de 222.22/16	UDP	>1023	53	—
4. Permitir	Fuera de 222.22/16	222.22/16	UDP	53	>1023	—
5. Denegar	Todos	Todos	Todos	Todos	Todos	Todos

- ✉Observe que si un origen externo intenta establecer una conexión TCP con un host interno la conexión será bloqueada, incluso aunque el puerto de origen o el de destino sea el puerto 80.

SEGURIDAD OPERACIONAL EN REDES LAN

Lista de control de acceso (cont.)

(Kurose, 2017)

- ▶**Política 2**. Los usuarios pueden hacer sus consultas al servidor DNS que se encuentra en la red del ISP.
  - ✉ La Acción 3 permite salir de la red a los paquetes DNS (puerto de destino 53).
  - ✉ La Acción 4 permite entrar a la red a los paquetes DNS (puerto de origen 53).
- ▶**Política 3**. Bloquear todo lo demás.
  - ✉ La Acción 5 deniega todas las acciones, excepto las contempladas en la Políticas 1 y 2.

Lista de control de acceso para una interfaz de router de la organización 222.22/16						
Acción	**Dirección de origen**	**Dirección de destino**	**Protocolo**	**Puerto de origen**	**Puerto de destino**	**Bit indicador**
1.Permitir	222.22/16	Fuera de 222.22/16	TCP	>1023	80	Cualquiera
2. Permitir	Fuera de 222.22/16	222.22/16	TCP	80	>1023	ACK
3 Permitir	222.22/16	Fuera de 222.22/16	UDP	>1023	53	—
4. Permitir	Fuera de 222.22/16	222.22/16	UDP	53	>1023	—
5. Denegar	Todos	Todos	Todos	Todos	Todos	Todos

- **En resumen,** esta Lista de control de acceso bastante restrictiva bloquea todo el tráfico excepto el tráfico web iniciado dentro de la organización y trafico DNS. La certificación CERT Filtering 2012 proporciona una lista de filtros de paquetes basados en puertos/protocolos recomendados para evitar una serie de agujeros de seguridad bien conocidos en las aplicaciones de red existentes.

SEGURIDAD OPERACIONAL EN REDES LAN

Lista de control de acceso (cont.)

(Kurose, 2017)

SEGURIDAD OPERACIONAL EN REDES LAN

¿Cómo funcionan los filtros con memoria del estado?

(Kurose, 2017)

- **En un filtro de paquetes** tradicional las decisiones de filtrado se toman para cada paquete de forma aislada.
- **Un filtro con memoria del estado** controla las conexiones TCP y utiliza dicha información para tomar decisiones de filtrado.
  - ✉ Para entender este filtro, observe que la Lista de control de acceso de la tabla, aunque bastante restrictiva, permite (Acción 2) que cualquier paquete procedente del exterior con ACK = 1 y puerto de origen 80 atraviese el filtro.

Lista de control de acceso para una interfaz de router de la organización 222.22/16

Acción	Dirección de origen	Dirección de destino	Protocolo	Puerto de origen	Puerto de destino	Bit indicador
1.Permitir	222.22/16	Fuera de 222.22/16	TCP	>1023	80	Cualquiera
2. Permitir	Fuera de 222.22/16	222.22/16	TCP	80	>1023	ACK
3 Permitir	222.22/16	Fuera de 222.22/16	UDP	>1023	53	—
4. Permitir	Fuera de 222.22/16	222.22/16	UDP	53	>1023	—
5. Denegar	Todos	Todos	Todos	Todos	Todos	Todos

- **Tales paquetes** podrían ser utilizados por posibles atacantes para intentar hacer fallar a los sistemas internos o paquetes mal formados, llevar a cabo ataques de denegación de servicio o realizar un mapa de la red interna. La solución más sencilla consiste en bloquear también los paquetes TCP ACK, pero este método impediría a los usuarios internos de la organización navegar por la Web.
- **Los filtros con memoria del estado** resuelven este problema almacenando la información de todas las conexiones TCP activas en una tabla de conexiones. Esto es posible porque el firewall puede observar el inicio de una nueva conexión observando un acuerdo en tres fases (SYN, SYNACK y ACK) y puede observar el fin de una conexión cuando ve un paquete FIN para la conexión. El firewall también puede suponer que la conexión ha terminado cuando no ha observado ninguna actividad en la misma durante, por ejemplo, 60 segundos.

Firewalls - Filtros de paquetes con memoria del estado

Tabla de conexiones y Lista de control de acceso

(Kurose, 2017)

- **En la tabla se muestra** un ejemplo de una tabla de conexiones para un firewall.
- **Esta tabla de conexiones** indica que actualmente hay tres conexiones TCP activas, habiéndose iniciado todas ellas dentro de la organización.

Tabla de conexiones de un filtro con memoria del estado

Dirección de origen	Dirección de destino	Puerto de origen	Puerto de destino
1.222.22.1.7	37.96.87.123	12699	80
2.222.22.93.2	199.1.205.23	37654	80
3.222.22.65.143	203.77.240.43	48712	80

- **Adicionalmente**, el filtro con memoria del estado incluye una nueva columna "Comprobar conexión", en su lista de control de acceso, es decir, ahora la lista de control de acceso indica que la conexión debería ser comprobada para las Acciones 2 y 4.

Lista de control de acceso para un filtro con memoria de estado

Acción	Dirección de origen	Dirección de destino	Protocolo	Puerto de origen	Puerto de destino	Bit indicador	Comprobar conexión
1.Permitir	222.22/16	Fuera de 222.22/16	TCP	>1023	80	Cualquiera	
2.Permitir	Fuera de 222.22/16	222.22/16	TCP	80	>1023	ACK	X
3.Permitir	222.22/16	Fuera de 222.22/16	UDP	>1023	53	—	
4.Permitir	Fuera de 222.22/16	222.22/16	UDP	53	>1023	—	X
5.Denegar	Todos	Todos	Todos	Todos	Todos	Todos	

- **Ejemplo 1**. Suponga que un atacante intenta introducir un paquete mal formado a la red de la organización enviando un datagrama con el puerto de origen TCP número 80 y con el bit indicador ACK activado. Suponga además que este paquete tiene el número de puerto de origen 12543 y la dirección IP de origen 150.23.23.155.
  - ✉ Cuando este paquete llega al firewall, este comprueba la lista de control de acceso, la cual indica que la tabla de conexión también tiene que ser comprobada antes de permitir la entrada del paquete a la red de la organización (según la Acción 2).
  - ✉ El firewall comprueba debidamente la tabla de conexiones, ve que ese paquete no es parte de una conexión TCP activa y lo rechaza.

SEGURIDAD OPERACIONAL EN REDES LAN

Tabla de conexiones y lista de control de acceso (cont.)

- **Ejemplo 2**. Suponga que un usuario interno desea navegar por un sitio web externo. Puesto que este usuario en primer lugar envía un segmento TCP SYN, la conexión TCP del usuario se registra en la tabla de conexiones, por ejemplo la Dirección de origen 3..
  - ✉ Cuando el servidor web devuelve los paquetes con el bit ACK necesariamente activado (según la Acción 2), el firewall comprueba la tabla y ve que la correspondiente conexión está en curso, según la Dirección de origen 3.
  - ✉ Por tanto , el firewall deja pasar a estos paquetes, no interviniendo entonces en la actividad de navegación por la Web del usuario interno.

Tabla de conexiones de un filtro con memoria del estado

Dirección de origen	Dirección de destino	Puerto de origen	Puerto de destino
1.222.22.1.7	37.96.87.123	12699	80
2.222.22.93.2	199.1.205.23	37654	80
3.222.22.65.143	203.77.240.43	48712	80

Lista de control de acceso para un filtro con memoria de estado

Acción	Dirección de origen	Dirección de destino	Protocolo	Puerto de origen	Puerto de destino	Bit indicador	Comprobar conexión
1.Permitir	222.22/16	Fuera de 222.22/16	TCP	>1023	80	Cualquiera	
2.Permitir	Fuera de 222.22/16	222.22/16	TCP	80	>1023	ACK	X
3.Permitir	222.22/16	Fuera de 222.22/16	UDP	>1023	53	—	
4.Permitir	Fuera de 222.22/16	222.22/16	UDP	53	>1023	—	X
5.Denegar	Todos	Todos	Todos	Todos	Todos	Todos	

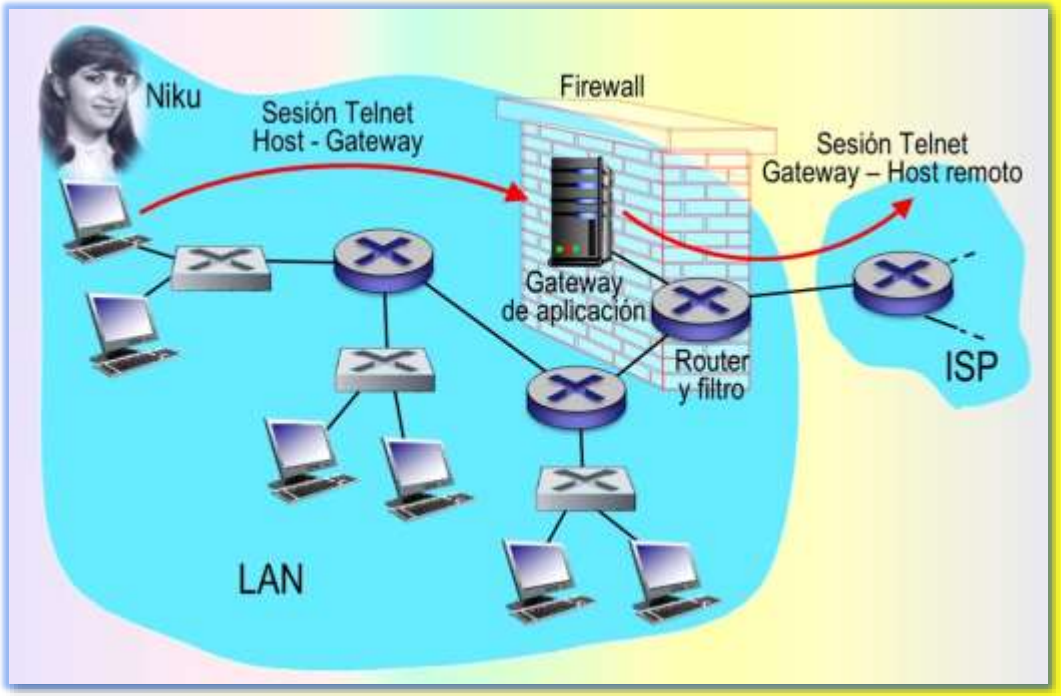
5. GATEWAYS DE APLICACIÓN

SEGURIDAD OPERACIONAL EN REDES LAN

¿Cómo conseguir un mayor nivel de seguridad?

(Kurose, 2017)

- **El filtrado,** en el nivel de paquetes, permite a una organización realizar un filtrado basto, con base al contenido de las cabeceras IP y TCP/UDP, las direcciones IP, los números de puerto y los bit de reconocimiento (ACK).
- **Pero**, ¿qué ocurre si una organización desea proporcionar, por ejemplo, el servicio Telnet a un conjunto restringido de usuarios internos?
- **¿Y qué ocurre** si la organización desea que tales usuarios privilegiados se autentiquen así mismos antes de permitirles establecer conexiones Telnet con el mundo exterior?
- **Tales tareas** quedan fuera de las capacidades de los filtros tradicionales y con memoria del estado. De hecho, la información acerca de la identidad de los usuarios internos está en los datos de la capa de aplicación y no está incluida en las cabeceras IP/TCP/UDP.
- **Para conseguir** un mayor nivel de seguridad, los firewall deben combinar los filtros de paquetes con gateways de aplicación, los cuales miran más allá de las cabeceras IP/TCP/UDP y toman sus decisiones basándose en los datos de la aplicación.



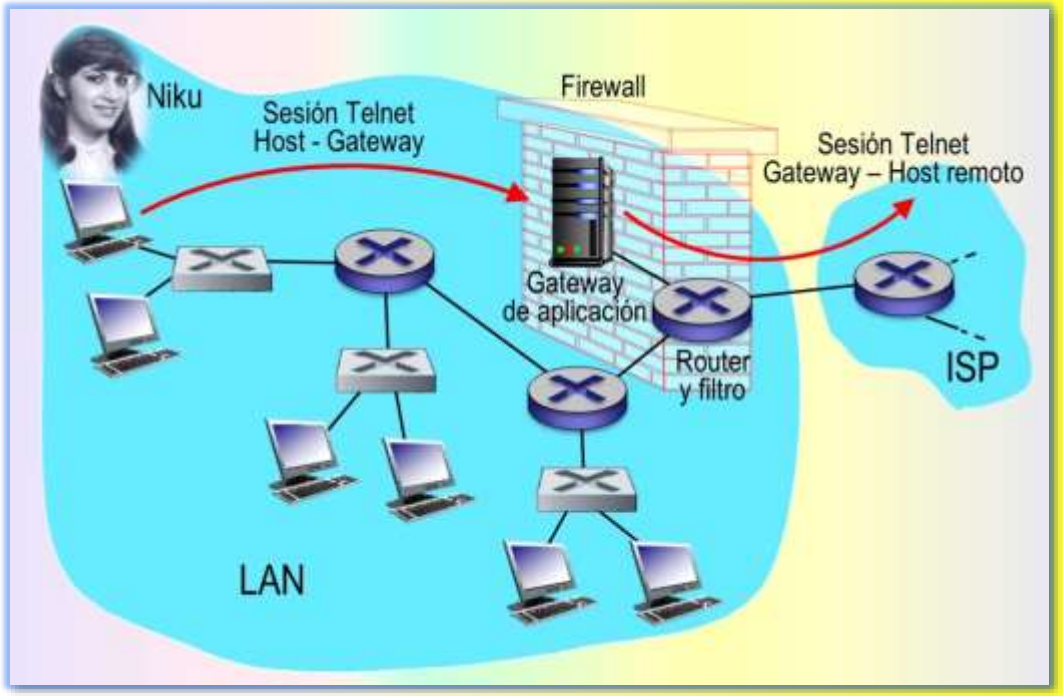
- **Un gateways de aplicación** es un servidor especifico de aplicación a través del cual deben pasar todos los datos de aplicación (entrantes y salientes). Pueden ejecutarse varias aplicaciones de gateways sobre el mismo host, pero cada gateway es un servidor separado con sus propios procesos.

Gateways de aplicación

SEGURIDAD OPERACIONAL EN REDES LAN

¿Cuál es el propósito del gateway de aplicación?

- **Para comprenderlo**, se va a diseñar un firewall que permita solo a un grupo restringido de usuarios internos establecer una conexión Telnet con el exterior y que impida a todos los clientes externos establecer una conexión Telnet con la red interna.
  - ▶**1.** Tal política se puede conseguir implementando una combinación de un filtro de paquetes (en un router) y un gateway de aplicación Telnet.
  - ▶**2.** El filtro del router se configura para bloquear todas las conexiones Telnet excepto aquellas que tienen su origen en la dirección IP del gateway de aplicación. Una configuración de filtro como esta, fuerza a todas las conexiones Telnet salientes a pasar a través del gateway de aplicación.



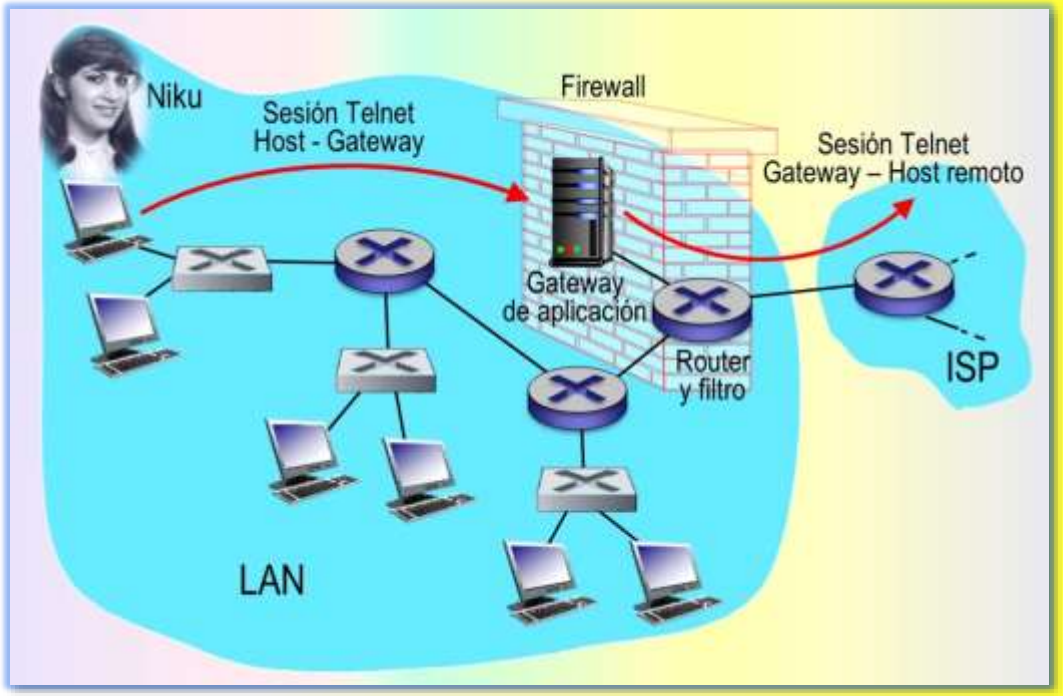
  - ▶**3.** Considere ahora un usuario interno que quiera conectarse mediante Telnet con el mundo exterior. El usuario tiene que establecer en primer lugar una sesión Telnet con el gateway de aplicación. Una aplicación que se ejecute en el gateway y que está a la espera de sesiones Telnet entrantes pedirá al usuario que introduzca un ID de usuario y una contraseña.
  - ▶**4.** Cuando el usuario proporcione esta información, el gateway de aplicación la comprobará para ver si el usuario tiene permiso para establecer una conexión Telnet con el mundo exterior. Si no es así, el gateway termina la conexón Telnet que tiene con el usuario interno.

Gateways de aplicación

¿Cómo funciona el gateway de aplicación?

(Kurose, 2017)

- ▶**5.** Si el usuario tiene permiso, entonces:
  - ✉ (1) El gateway pide al usuario el nombre del host externo con el que desea conectarse.
  - ✉ (2) El gateway establece una sesión Telnet entre él y el host externo.
  - ✉ (3) El gateway reenvía al host externo todos los datos que le lleguen del usuario, de la misma manera que reenvía al usuario todos los datos que le lleguen desde el host externo.
- ▶**6.** De este modo, el gateway de aplicación Telnet no solo se encarga de realizar la autorización del usuario, sino que actúa como servidor y cliente Telnet, retransmitiendo la información entre el usuario y el servidor Telnet remoto.



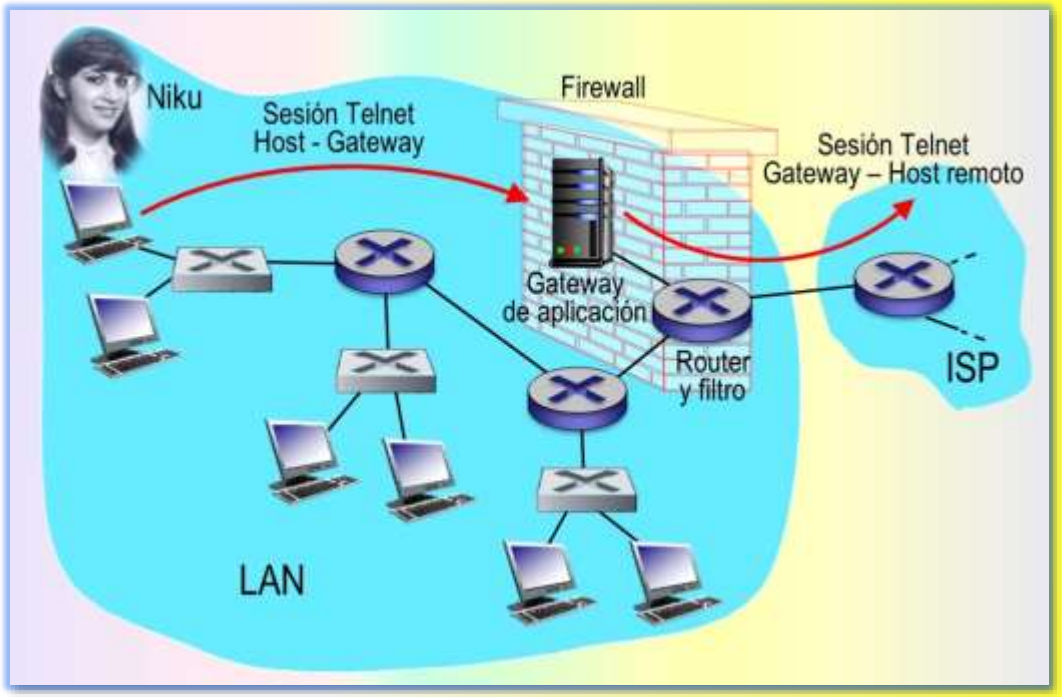
- ▶**7.** Observe que el filtro permitirá que se lleve a cabo el paso 2, dado que es el gateway quien inicia la conexión Telnet con el mundo exterior.

Gateways de aplicación

Gateways en las redes LAN

(Kurose, 2017)

- **Las redes internas** a menudo disponen de múltiples gateways de aplicación, por ejemplo, Gateways para Telnet, HTTP, FTP y correo electrónico. De hecho, el servidor de correo de una organización y la caché web son gateways de aplicación.
- **Pero los gateways de aplicación** también tienen sus desventajas:
  - ▶**1.** Hace falta un gateway de aplicación diferente para cada aplicación.
  - ▶**2.** El rendimiento se verá afectado, dado que todos los datos tendrán que ser reenviados a través del gateway. Esto se convierte en un problema en aquellos casos en los que hay varios usuarios o aplicaciones utilizando la misma máquina gateway.
  - ▶**3.** El software de cliente debe saber cómo contactar con el gateway cuando el usuario realiza una solicitud, y debe saber también cómo decir al gateway de aplicación con qué servidor externo hay que conectarse.



La necesidad de una inspección profunda de paquetes

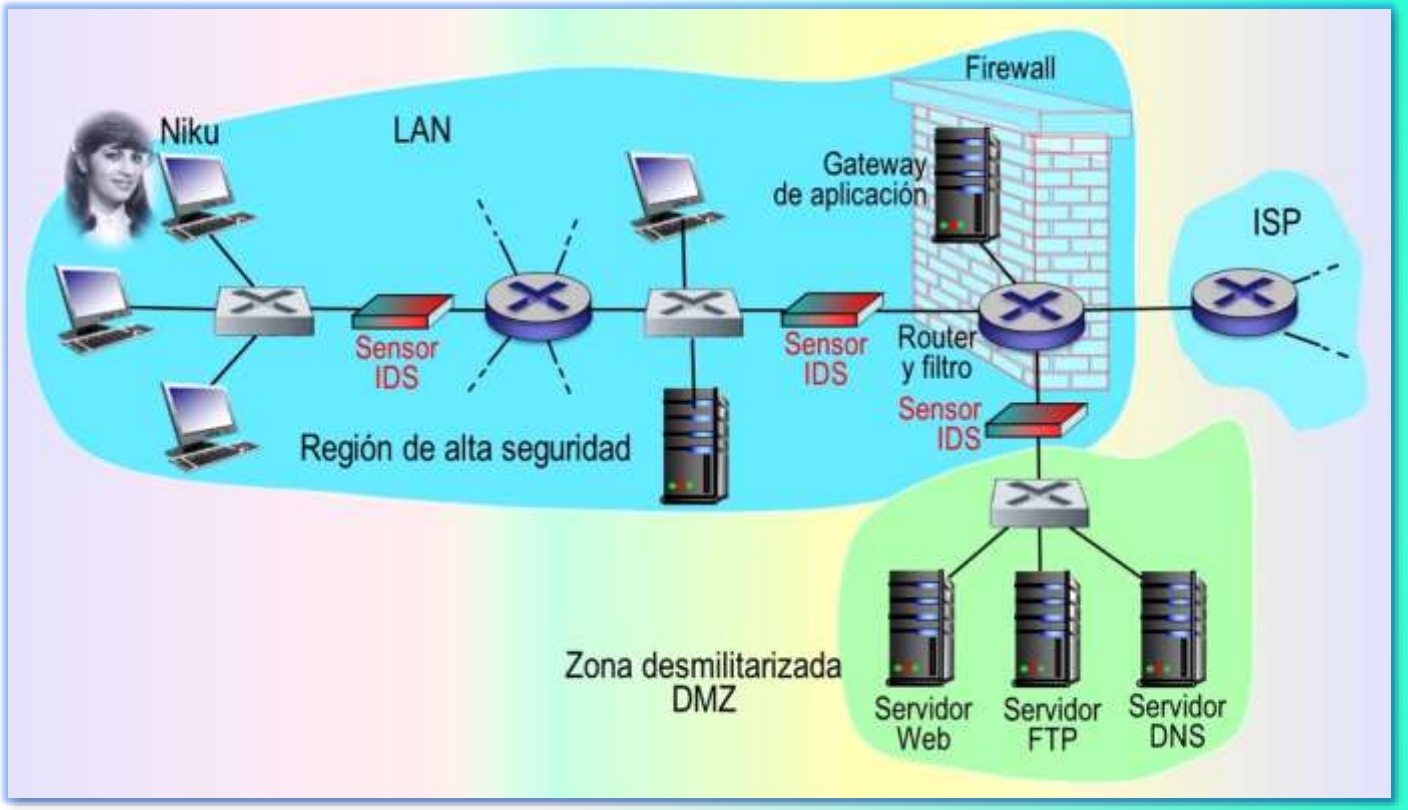
(Kurose, 2017)

- **Para detectar** muchos tipos de ataques se necesita llevar a cabo una inspección profunda de paquetes, es decir, mirar más allá de los campos de cabecera, examinando los propios datos de aplicación transportados por los paquetes.
  - ✉ Los gateways de aplicación realizan a menudo una inspección profunda de los paquetes. Pero cada gateway de aplicación solo lleva a cabo esa tarea para una aplicación específica.
- **Existen otros dispositivos** que no solo examinan las cabeceras de todos los paquetes que le atraviesen, sino que también llevan a cabo una inspección profunda de los paquetes (a diferencia de lo que sucede con los filtros de paquetes).
  - ✉ Si estos dispositivos detectan un paquete sospechoso o una serie sospechosa de paquetes, impiden que esos paquetes entren a la red de la organización. A estos dispositivos que filtran el tráfico sospechoso se les denomina sistema de prevención de intrusiones (IPS).
  - ✉ Pero si la actividad detectada solo se considera sospechosa, los dispositivos dejan pasar los paquetes pero envían alertas a un administrador de red, que puede de ese modo echar un vistazo mas detallado a dicho tráfico y tomar las medidas oportunas. A estos dispositivos que generan alertas cuando observan la presencia de tráfico potencialmente malicioso se les denomina sistema de detección de intrusiones (IDS).
- **Se describirán** ambos tipos de sistemas (IPS e IDS) conjuntamente, dado que el aspecto técnico más interesante de dichos sistema es cómo detectar el tráfico sospechoso (y no si eliminan paquetes o envían alertas). Por tanto, se utilizará el término sistemas IDS para referirse tanto a los sistemas IPS como a los IDS.

SEGURIDAD OPERACIONAL EN REDES LAN

Ataques que detectan los sistemas IDS

(Kurose, 2017)



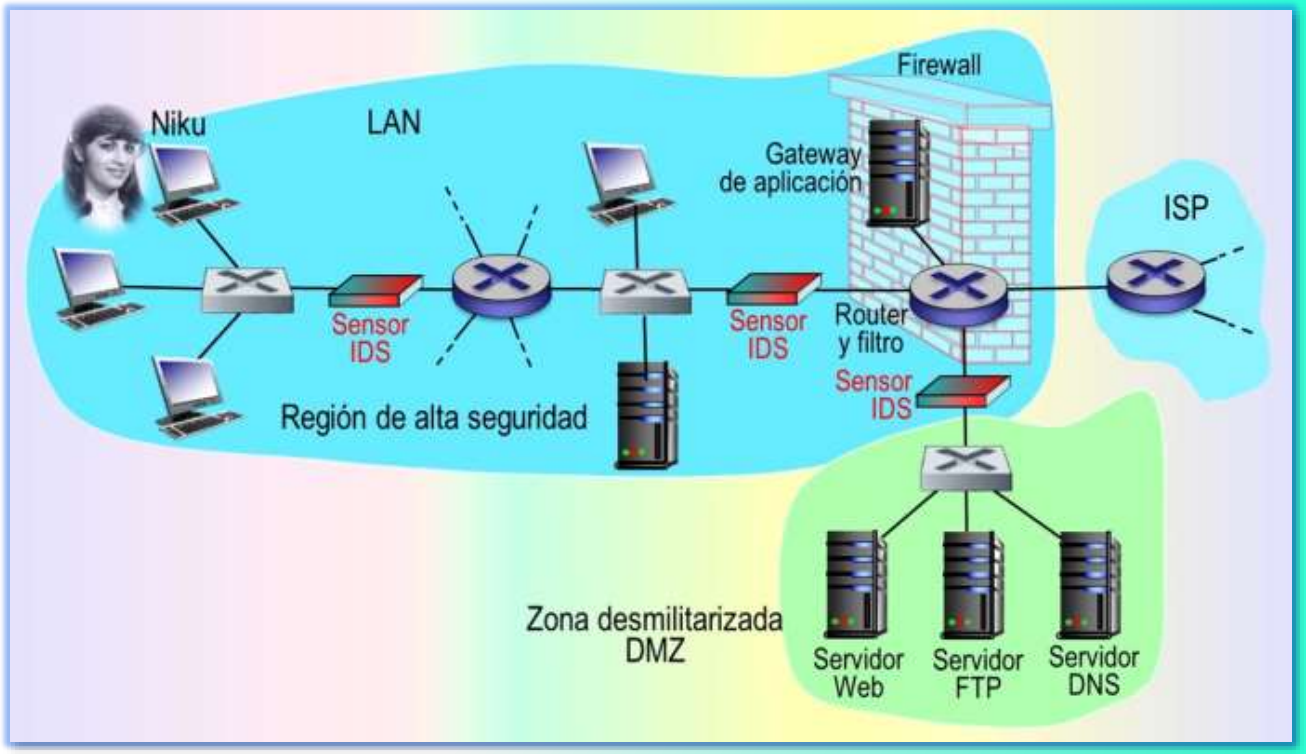
- **Un sistema IDS** se emplea para detectar una amplia gama de ataques, incluyendo:.
  - Mapeado de red, generado por ejemplo, por *nmap.*
  - Escaneo de puertos.
  - Escaneo de la pila de protocolos TCP
  - Ataques DoS de inundación del ancho de banda,
  - Gusanos y virus,
  - Ataques de vulnerabilidades del sistema operativo.
  - Ataques de vulnerabilidades de aplicación.
- **Una organización** puede implementar uno o más sensores IDS en su red. La figura muestra una organización con tres sensores IDS.
- **Actualmente**, miles de organizaciones utilizan sistemas IDS. Muchos de estos sistemas son propietarios, comercializados por Cisco, Check Point y otros fabricantes de equipos de seguridad.
- **Pero muchos** otros sistemas IDS son sistemas de dominio público, como el popular sistemas de IDS Snort.

SEGURIDAD OPERACIONAL EN REDES LAN

Sistemas de seguridad con múltiples sensores IDS

(Kurose, 2017)

- **Cuando** se implantan múltiples sensores, normalmente funcionan de manera concertada, enviando información acerca de las actividades de tráfico sospechoso a un procesador IDS central que recopila e integra la información y envía alarmas a los administradores de la red, cuando lo considera apropiado.
- **Las organizaciones**, por lo general, dividen su red en dos regiones, vea el ejemplo de la figura.
  - ▶Una región de alta seguridad, protegida por un filtro de paquetes y un gateway de aplicación y monitoreada por sensores IDS.
  - ▶Una región de menor seguridad denominada zona desmilitarizada (DMZ) que está protegida solo por el filtro de paquetes, aunque también está monitoreada mediante sensores IDS.
    - ✉La DMZ incluye los servidores de la organización que necesitan comunicarse con el mundo exterior, como su servidor web público y su servidor DNS.

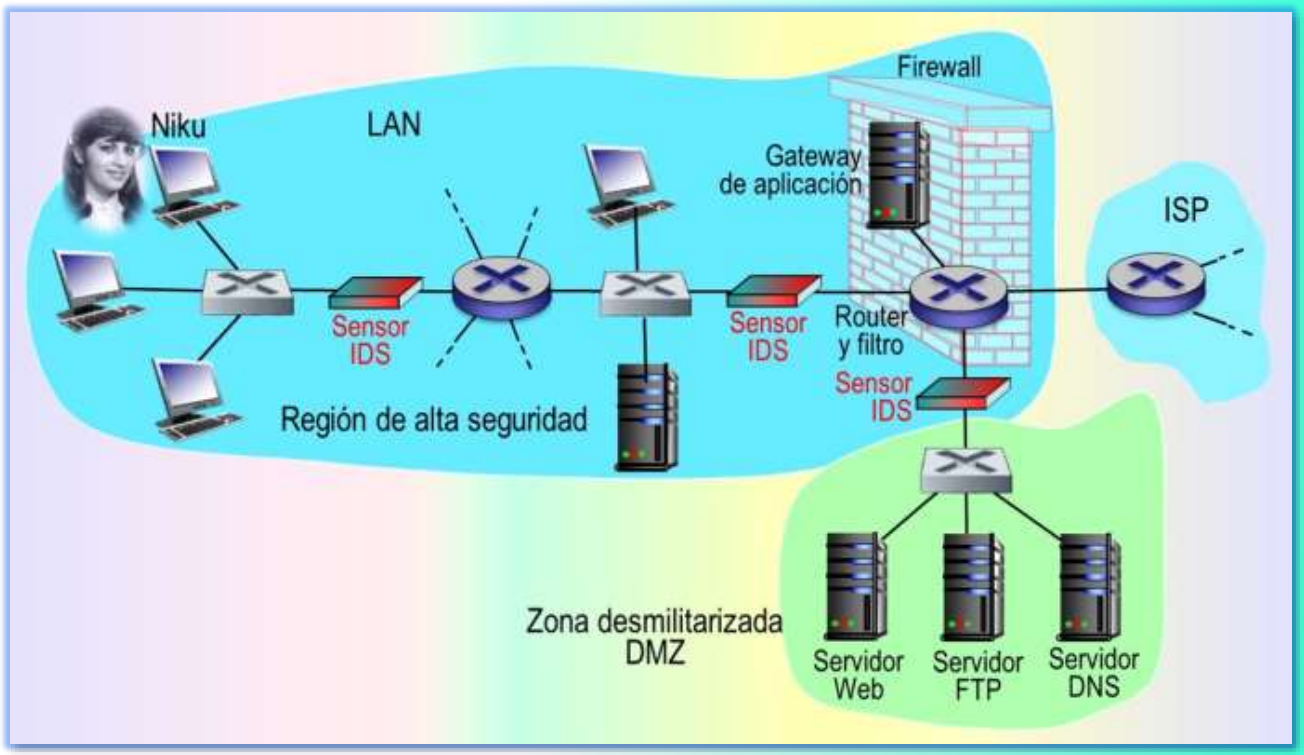


SEGURIDAD OPERACIONAL EN REDES LAN

¿Por qué se emplean múltiples sensores?

(Kurose, 2017)

- **Surgen las preguntas**: ¿por qué se emplean múltiples sensores IDS? ¿Por qué no colocar simplemente un sensor IDS justo detrás del filtro de paquetes, o incluso integrado con el filtro de paquetes?
- **Un IDS** no solo tiene que llevar a cabo una inspección profunda de los paquetes, sino que también debe comparar cada paquete que pasa con decenas de miles de "firmas", esto puede requerir una cantidad significativa de procesamiento, en particular si la organización recibe tráfico de Internet del orden de Gbps.
- **Colocando los sensores IDS** un poco más aguas abajo, cada uno de ellos solo ve una fracción del tráfico de la organización y puede cumplir mas fácilmente con su tarea.



- **De todos modos**, hoy día hay disponibles sistemas IDS e IPS de altas prestaciones y muchas organizaciones suelen conformarse con un único sensor localizado cerca de su router de acceso.

Sistemas IDS basados en firmas

(Kurose, 2017)

- **Los sistemas IDS** se clasifica. en términos generales, en sistemas basados en firmas y sistemas basados en anomalías.
- ▶**1.** Sistemas IDS basados en firmas
  - **Un IDS basado en firmas** mantiene una amplia base de datos de firmas de ataques.
  - **Cada firma** es un conjunto de reglas concernientes a una actividad de intrusión. Una firma puede ser simplemente una lista de características acerca de un determinado paquete (por ejemplo, números de puerto de origen y de destino, tipo de protocolo y una cadena específica de bits en la carga útil del paquete) o puede estar relacionada con una serie de paquetes.
  - **Las firmas** normalmente son creadas por ingenieros de seguridad de red experimentados que se dedican a investigar los ataques conocidos. El administrador de red de una organización puede personalizar las firmas y añadir otras de su creación a la base de datos.
  - **Operacionalmente**, un sistema IDS basado en firmas analiza cada paquete que pasa a través de él, comparando cada paquete husmeado con las firmas de su base de datos. Si un paquete (o una serie de paquetes) concuerda con una firma de la base de datos, el IDS genera una alerta.
  - **La alerta** podría enviarse al administrador de red en un mensaje de correo electrónico, o mandarse al sistema de gestión de la red o simplemente almacenarse en un registro para su futura inspección.

Sistemas IDS basados en firmas - Limitaciones

(Kurose, 2017)

- **Los sistemas IDS** basados en firmas, aunque están ampliamente implantados, presentan una serie de limitaciones:
  - ▶La más importante es que se requiere un conocimiento previo del ataque para generar una firma precisa. En otras palabras, un IDS basado en firmas es completamente inútil frente a nuevos ataques que todavía no hayan sido investigados.
  - ▶Otra desventaja es que incluso si se produce una concordancia con una firma, puede que dicha concordancia no sea el resultado de un ataque, con lo que se generaría una falsa alarma.
  - ▶Finalmente, puesto que es necesario comparar cada paquete con una amplia colección de firmas, el IDS puede verse desbordado por las necesidades de procesamiento y debido a ello fracasar a la hora de detectar muchos paquetes maliciosos.

Sistemas IDS basados en anomalías

(Kurose, 2017)

- ▶**2.** Sistemas IDS basados en anomalías
  - **Un IDS basado en anomalías** crea un perfil de tráfico observando el tráfico durante la operación normal, después busca flujos de paquetes que sean estadísticamente inusuales, como por ejemplo un porcentaje inusual de paquetes ICMP o un crecimiento exponencial súbito en el escaneo de puertos y barridos mediante ping.
  - **Lo mejor de los sistemas IDS** basados en anomalías es que no dependen del conocimiento previo acerca de los ataques existentes; es decir, pueden detectar potencialmente nuevos ataques no documentados. Por otro lado, el problema de distinguir entre el tráfico normal y el tráfico estadísticamente inusual es extremadamente complejo.
- **A la fecha**, la mayoría de los sistemas IDS implantados son basados en firmas, aunque alguno de ellos incluyen alguna características de los sistemas basados en anomalías.

Clasificación de los sistemas IDS

El IDS Snort

(Kurose, 2017)

- **Snort es un IDS** de dominio público y código abierto, con centenares de miles de implantaciones conocidas. Puede ejecutarse sobre plataformas Linux, UNIX y Windows. Utiliza la interfaz genérica de análisis *libpcap*, que también es utilizada por Wireshark y otros muchos husmeadores de paquetes. Puede gestionar fácilmente 100 Mbps de tráfico: Para instalaciones con velocidades de tráfico del orden de Gbps puede ser necesario emplear múltiples sensores de Snort.

- **Para entender** un poco cómo funciona Snort, examine el siguiente ejemplo de firma utilizada por Snort:

```
alert icmp  $EXTERNAL_NET  any -> $HOME_NET any
(msg : "ICMP PING NMAP "; dsize: 0 ;  itype: 8;)
```

  - ✉ Esta firma concordará con cualquier paquete ICMP que entre en la red de la organización ($HOME_NET) desde el exterior ($EXTERNAL _NET), que sea de tipo 8 (ping ICMP) y que carezca de carga útil (dsize: 0). Puesto que *nmap* genera paquetes ping con estas características específicas, esta firma está diseñada para detectar los barridos ping realizados con *nmap*. Cuando un paquete concuerda con esta firma, Snort genera una alerta que incluye el mensaje "ICMP PING NMAP".

- **Lo más impresionante** acerca de Snort quizás sea **la enorme comunidad de usuarios** y expertos de seguridad que mantienen su base de datos de firmas. Normalmente, al cabo de pocas horas de detectarse un nuevo ataque, la comunidad Snort escribe y publica una firma del ataque que después es descargada por los centenares de miles de implantaciones Snort distribuidas por todo el mundo.

- **Además**, utilizando la sintaxis de firmas de Snort, los administradores de red pueden adaptar las firmas a las necesidades de su propia organización modificando las firmas existentes o creando otras completamente nuevas.

Referencias bibliográficas

SEGURIDAD OPERACIONAL EN REDES LAN

Referencias bibliográficas

- CISCO (2015). *CCNA Routing and Switching. Introduction to Networks*. CISCO.
- CISCO (2016). *Introducción a las redes.* Madrid: Pearson Education, S.A.
- Forouzan, B. A. (2020). *Transmisión de datos y redes de comunicaciones.* Madrid: McGraw-Hill.
- Huawei Technologies (2020). *Basics of data communication networks*. Huawei.
- Kurose, J. Keith, R. (2017). *Redes de computadoras: un enfoque descendente*. Madrid: Pearson Education, S.A.

FIN

Tema 11 de:

SEGURIDAD EN REDES

Edison Coimbra G.