CONCEPTOS DE SEGURIDAD DE REDES

Módulo 10

Temas a tratar

1. Requisitos de seguridad y tipos de ataque
2. Criptografía
   a) Cifrado Simétrico
   b) Cifrado Asimétrico
   c) Función Hash
3. Proxy
4. Firewall
5. Firewall de uso libro: *"iptables"*

Objetivos del módulo

Al finalizar el presente módulo el alumno debe ser capaz de:

1. Conocer cuales son los posibles ataques que puede sufrir un sistema informático desplegado en una red
2. Entender cuales son las medidas para mitigar el éxito de los ataques
3. Conocer el funcionamiento de un sistema criptográfico
4. Entender que es un Proxy y un Firewall
5. Adquirir habilidades en la implementación de un Firewall de uso libre

Seguridad en la red
Introducción

- ✓ Seguridad en la Red:
  - ✓ Es un conjunto de políticas y prácticas recomendadas, para ser aplicadas en toda una red, con el objeto de prevenir: accesos y modificaciones de datos no autorizadas, denegaciones de servicios y reemplazos de identidades.
- ✓ Proteger los recursos físicos y lógicos
- ✓ Extensible a los cables, routers y todo ítem que constituya la infraestructura de la red
- ✓ La protección del recurso lógico se traduce en:
  - ✓ Integridad de los datos
  - ✓ Disponibilidad de los datos
  - ✓ Confidencialidad de los datos
  - ✓ Autenticidad de los datos (Autenticación)

Seguridad en la red
Introducción

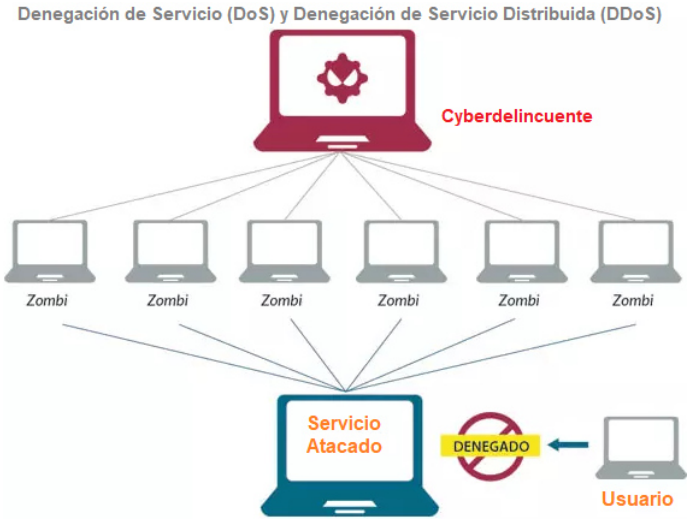
- Seguridad física: acceso físico, infraestructura del edificio, centro de Datos.
- Seguridad de la red corporativa: configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, disciplina operativa, gestión de cambios, desarrollo de aplicaciones.
- Seguridad de usuarios: composición de claves, seguridad en estaciones de trabajo, formación y creación de conciencia
- Seguridad de datos: criptografía, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.
- Auditoria de seguridad: análisis de riesgo, revisiones periódicas, visitas técnicas, monitoreo y auditoria.
- Aspectos legales: prácticas personales, contratos y acuerdos comerciales, leyes y reglamentación gubernamental.

Seguridad en la red
Tipos de ataque: Ataque Pasivo

- Consiste en escuchas o monitorizaciones de las transmisiones
- Difíciles de detectar, no alteran los datos
- Se pueden evitar cifrando el contenido a transmitir
- Footprinting, Herramientas OSINT

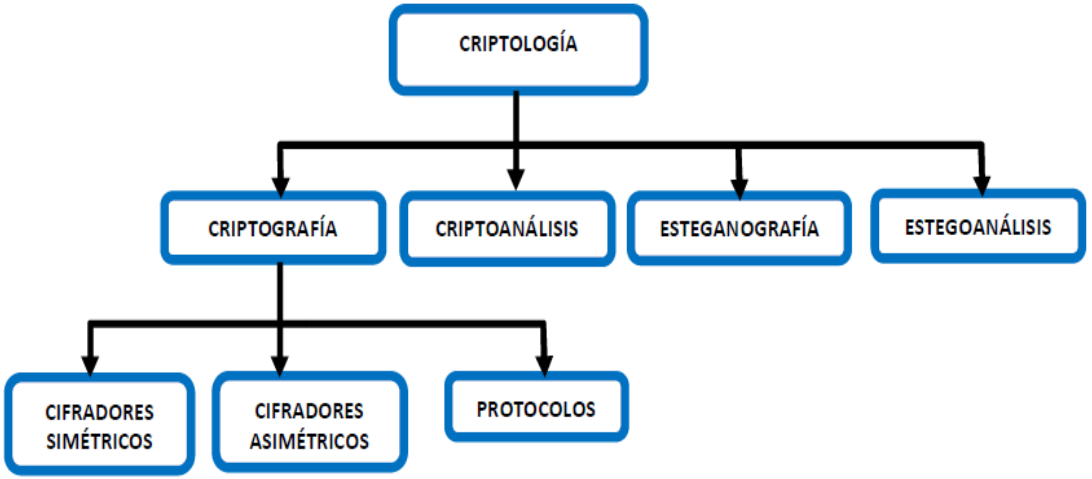
Seguridad en la red
Tipos de ataque: Ataque Activo

- Interrupción
- Enmascaramiento o suplantación
- Modificación de mensajes
- Fingerprint
- Denegación de servicio (DoS) y Denegación de servicios distribuida (DDoS)



Seguridad en la red
Criptografía

- ✓ Criptografía: arte de ocultar los mensajes, los cuales pueden ser revelados por quién posee la clave de encriptación
- ✓ Criptoanálisis: se ocupa de encontrar el significado de mensajes encriptados a través del análisis de las debilidades de los algoritmos de encriptación



Seguridad en la red
Sistema Criptográfico

- ✓ Es una tupla {P, C, K, E y D}
  - ✓ P es el conjunto de todos los mensajes a transmitir. Es el espacio de textos planos.
  - ✓ C es el conjunto de todos los mensajes cifrados. Es el espacio de textos cifrados.
  - ✓ K es el conjunto de claves a utilizar. Es el espacio de claves.
  - ✓ E es la familia de todas las funciones de cifrado. $E = \{E_k : k \in K\}$ y $E_k : P \rightarrow C$
  - ✓ D es la familia de todas las funciones de descifrado. $D = \{D_k : k \in K\}$ y $D_k : C \rightarrow P$.
- ✓ Para cada $e \in K$, hay un $d \in K$ tal que $D_d(E_e(p)) = p$ para todo $p \in P$. (e puede ser igual a d)
- ✓ Cualidades de un sistema criptográfico
  - ✓ Seguridad
  - ✓ Autenticidad e integridad
  - ✓ No repudio

Seguridad en la red
Sistema Criptográfico

- ✓ Algoritmos Simétricos (o de clave privada): Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar los mensajes
- ✓ Algoritmos Asimétricos (o de clave pública): La criptografía asimétrica, es aquella que utiliza dos claves diferentes para cada usuario, una para cifrar (clave pública) y otra para descifrar (clave privada).
- ✓ Esquemas híbridos:
  - ✓ Un sistema de encapsulación de clave, que es un sistema de cifrado de clave pública.
  - ✓ Un sistema de encapsulación de datos, que es un sistema de cifrado de clave simétrica.
- ✓ Función Hash: Una función hash H acepta un bloque de datos de longitud variable M como entrada y produce un valor hash de tamaño fijo h = H(M).

Seguridad en la red
Técnicas de encriptación

1. Transposición:

- ✓ Cambia el orden de los caracteres o bits según un patrón:

  Ejemplo: dividir el texto en bloques de 4 letras:

  REDES DE DATOS =⇒REDE SDED ATOS

- ✓ Tomar como patrón 4213

  EERD DDSE STAO =⇒EERDDDSESTAO

Seguridad en la red
Técnicas de encriptación

2.Sustitución:

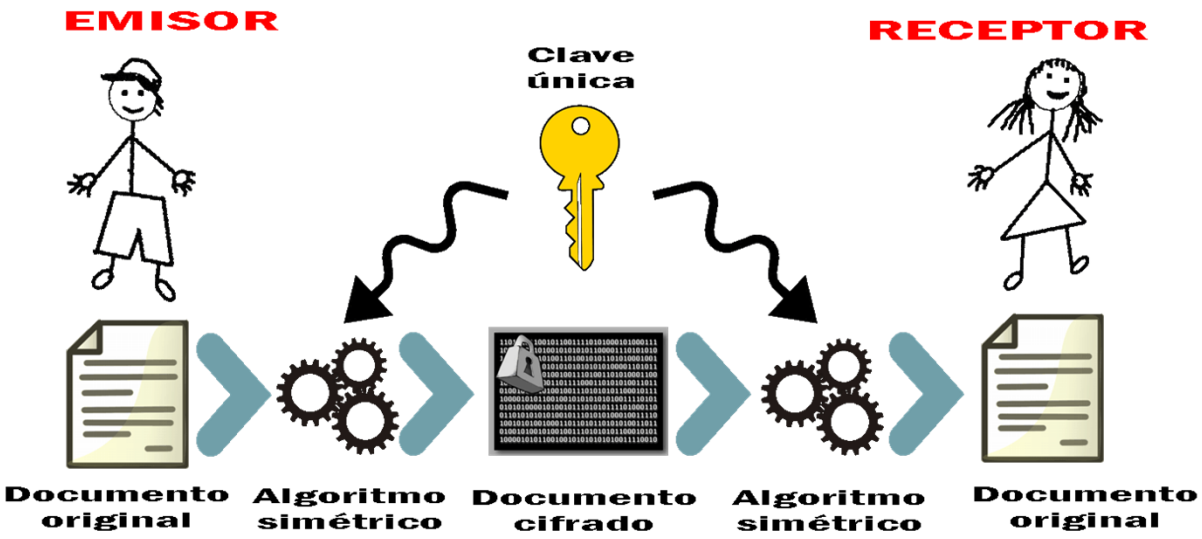
- ✓ Cada letra se sustituye por otra según una tabla y según su posición en el texto
- ✓ Si no depende de la posición es monoalfabética
- ✓ Si depende de la posición es polialfabética
  - ✓ Monoalfabética: Julio César
  - ✓ Ejemplo: X ⇒ X +3
  - ✓ ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - ✓ DEFGHIJKLMNOPQRSTUVWXYZABC
  - ✓ BUENOS DIAS ⇒EXHQRV GLDV

Seguridad en la red
Técnicas de encriptación

2.Sustitución:

- ✓ Polialfabética: Vignere
- ✓ n coordenadas enteras en el intervalo $0 \leq x \leq 25$, $k = (k0, k1, \cdots, kn-1)$ en Zn 26
- ✓ Se numeran las letras del texto t0,t1,t2,⋯ ,tm
- ✓ Se sustituye ti por ci según: $ci = (ti + ki \bmod n) \bmod 26$
- ✓ Si n = 1, Julio César

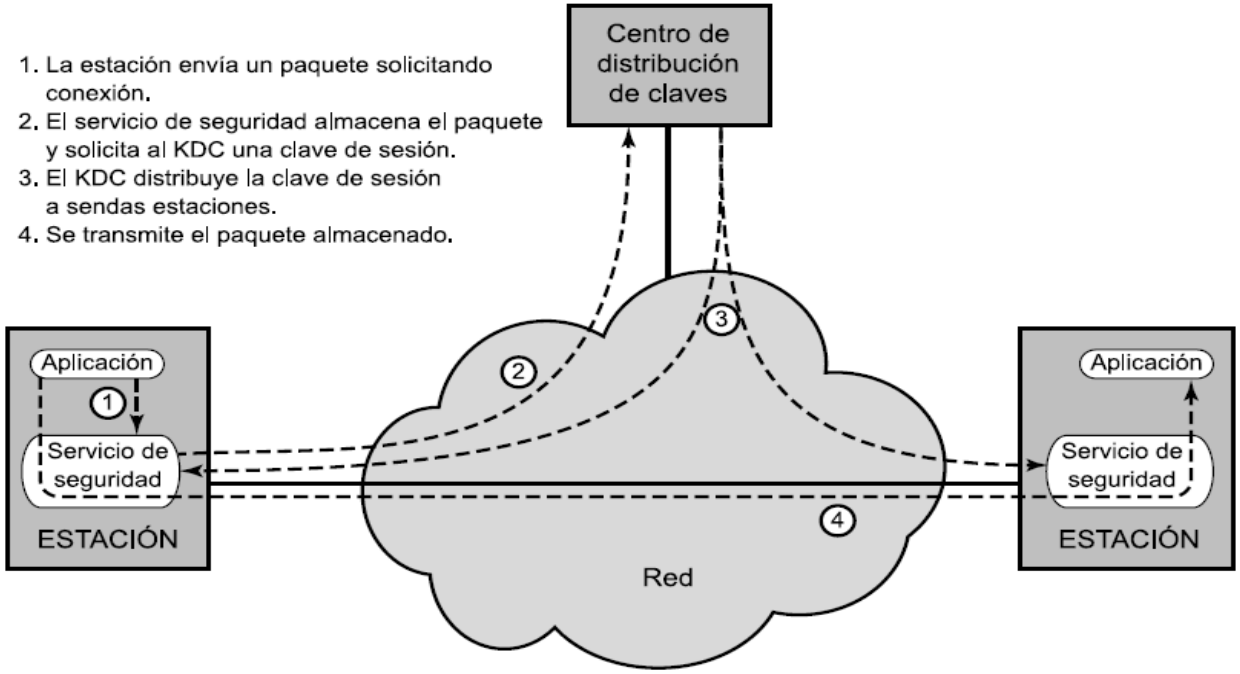
Seguridad en la red
Algoritmos Simétricos



Seguridad en la red
Algoritmos Simétricos

- ✓ Son los algoritmos más clásicos de encriptación
- ✓ Utilizados en redes comerciales desde el principio de los 70
- ✓ Se emplea la misma clave en las transformaciones de cifrado y descifrado
- ✓ Distribución de claves: las dos entidades que deseen comunicarse van a tener que compartir una misma clave. Ésta se debe distribuir a cada uno de ellos. Más significativos:
- ✓ Técnicas de cifrado:
  - ✓ Cifrado en "Stream" (no muy seguro según los expertos)
  - ✓ Cifrado en bloque
- ✓ Los algoritmos simétricos más importantes: DES, 3DES y AES

Seguridad en la red
Algoritmos Simétricos: Distribución de Claves



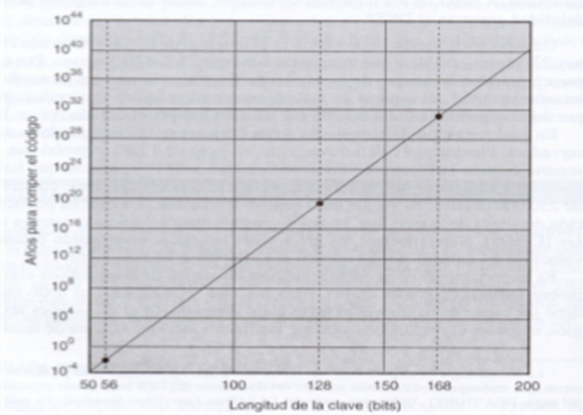
Distribución de claves extremo a extremo en un protocolo orientado a conexión

Seguridad en la red
Algoritmos Simétricos: Técnica de cifrado en bloque

- ✓ Utilizado en e-mail(PGP), seguridad en sesiones TCP(SSL), a nivel de red(IPSec)
- ✓ El texto plano se divide en bloques de k bits
- ✓ Cada bloque se encripta independientemente
- ✓ El cifrado consiste en "mapear" los k bits del texto plano con los k bits del texto cifrado
- ✓ Con k = 3 tenemos 8 posibles entradas que se permutan en 8! = 40.320 posibilidades
- ✓ Con k = 3 es rápidamente criptoanalizado
- ✓ Usualmente se parte de k = 64, generando 264! permutaciones

plano	cifrado	plano	cifrado
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

Seguridad en la red
Tabla y gráfico promedio para descifrar una clave



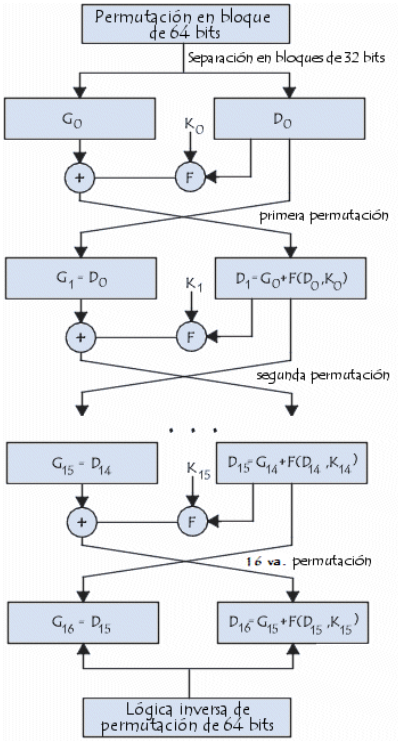
Tiempo empleado en romper un código
(Suponiendo 10^6 *descifrados*/μs)

Tamaño de la clave (bits)	Número de claves alternativas	Tiempo necesario a 1 cifrado/μs	Tiempo necesario a 10^6 cifrados/μs
32	$2^{32} = 4{,}3 \times 10^9$	2^{31} μs = 35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1.142 años	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	2^{127} μs = $5{,}4 \times 10^{24}$ años	$5{,}4 \times 10^{18}$ años
168	$2^{168} = 3{,}7 \times 10^{50}$	2^{167} μs = $5{,}9 \times 10^{36}$ años	$5{,}9 \times 10^{30}$ años

Seguridad en la red
Algoritmos Simétricos: DES (Data Encryption Standard)

- ✓ Nació como petición del gobierno de los EEUU al "National Bureau of Standards" en 1973 para poder mantener comunicaciones seguras
- ✓ Se eligió uno presentado por IBM y tras una serie de revisiones públicas, fue adoptado como estándar en 1977
- ✓ El algoritmo se basa en permutaciones, substituciones y sumas módulo 2
- ✓ Emplea una clave de 56 bits y opera con bloques de datos de 64 bits
- ✓ Utiliza funciones que simulan la permutación aleatoria de tabla completa
- ✓ Con la tecnología de esa época hubieran tardado 2200 años en probar todas las posibles claves. Hoy sólo se tarda 1 segundo!

Seguridad en la red
Algoritmos Simétricos: DES (Data Encryption Standard)

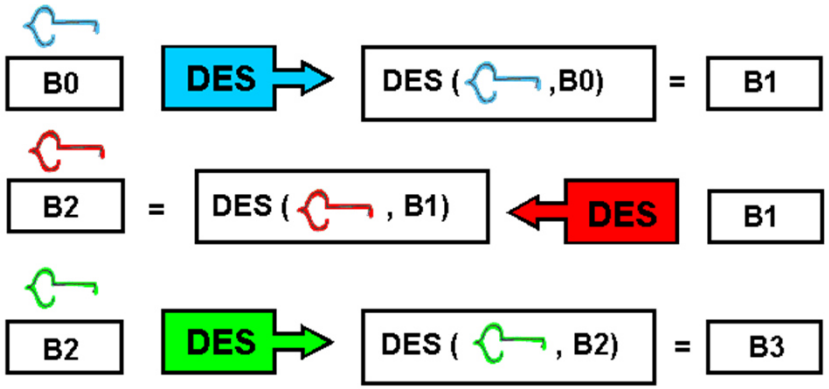


- ✓ Fraccionamiento del texto en bloques de 64 bits (8 bytes),
- ✓ Permutación inicial de los bloques,
- ✓ Partición de los bloques en dos partes: izquierda y derecha, denominadas *I* y *D* respectivamente
- ✓ Transformación con clave de "x" bits, preserva la mitad derecha
- ✓ fases de permutación y de sustitución repetidas 16 veces (denominadas **rondas**),
- ✓ Reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.

Seguridad en la red

Algoritmos Simétricos: 3DES (Triple Data Encryption Standard)

- ✓ Se estandarizó inicialmente para aplicaciones financieras en el estándar ANSI X9.17 en 1985.
- ✓ Se incorporó como parte del DES en 1999, con la publicación de FIPS PUB 463
- ✓ Usa tres claves y tres ejecuciones del algoritmo DES.
- ✓ La función sigue la secuencia cifrar-descifrar-cifrar(EDE: encrypt-decrypt-encrypt)



$$C = EK_3[DK_2[EK_1[P]]]$$

Donde

C = texto cifrado

P = texto plano

$E_K[X]$ =

cifrado de X usando la clave K

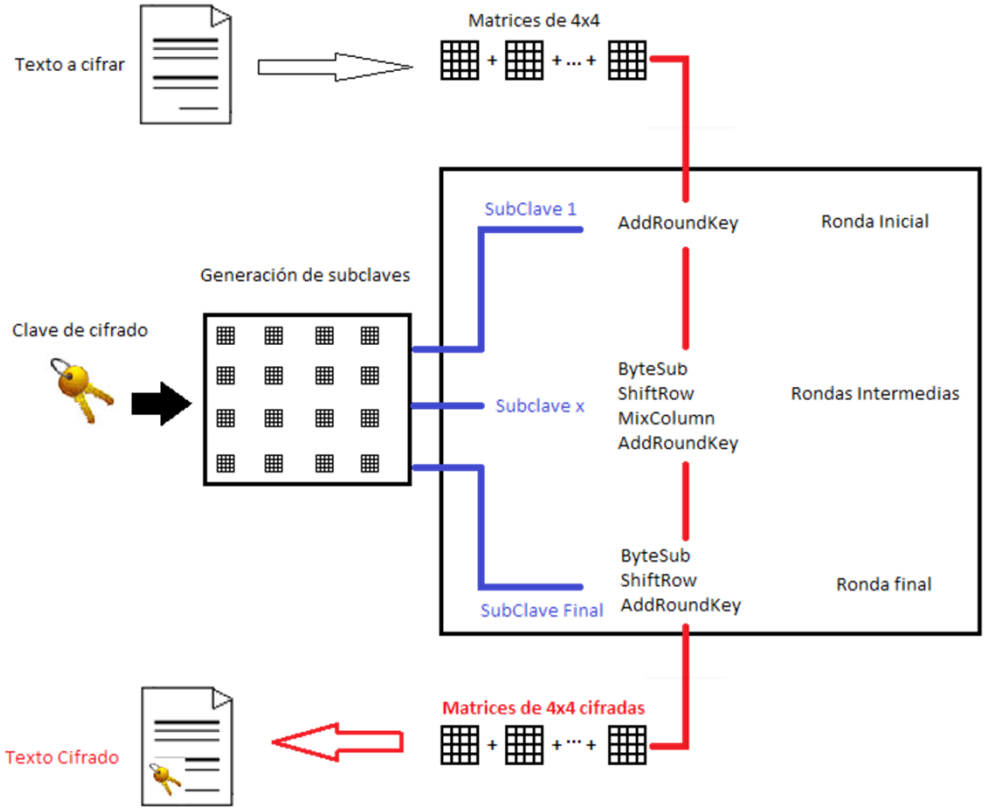
$D_K[Y]$ =

descifrado de Y usando la clave K

Seguridad en la red
Algoritmos Simétricos: AES (Advanced Encryption Standard)

- ✓ Publicado el 2 de Octubre de 2000 por el NIST como ganador de la convocatoria AES (estándar de cifrado avanzado)
- ✓ Fue desarrollado por: Joan Daemen y Vincent Rijmen, ambos de origen belga.
- ✓ Se desarrollo bajo el nombre de: Rijndael (pronunciado "Rain Doll" en inglés).
- ✓ Se transformó en un estándar efectivo el 26de mayo de 2002.
- ✓ Sustituye al D.E.S.
- ✓ El tamaño de clave debe ser de, al menos, 128, 192 y 256 bits (debe admitir los tres), y el tamaño de bloque de cifrado debe ser de 128 bits
- ✓ Buena combinación de seguridad, velocidad, eficiencia (en memoria y puertas lógicas), sencillez y flexibilidad

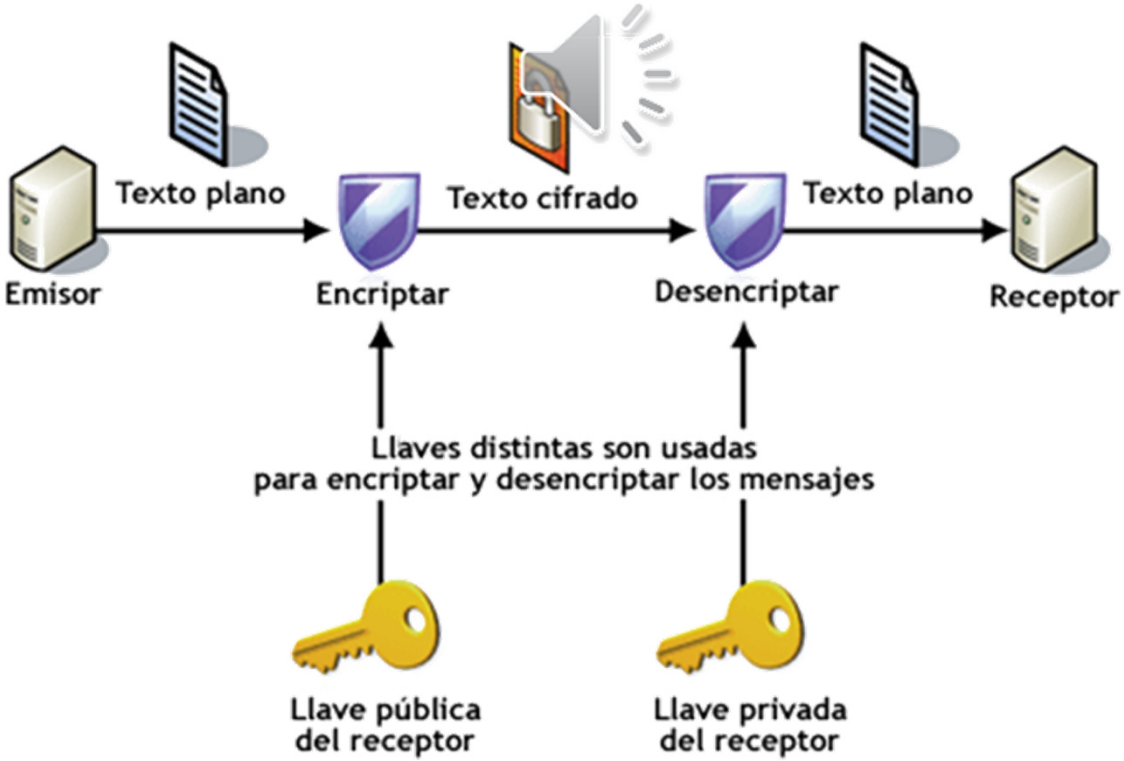
Seguridad en la red
Algoritmos Simétricos: AES (Advanced Encryption Standard)



Seguridad en la red
Algoritmos Asimétricos

- ✓ Son aquellos que emplean dos claves, una pública y otra privada La clave privada sólo la posee el receptor y la utiliza para desencriptar
- ✓ La clave pública la posee el receptor, pero se la pasa al emisor para que la utilice a la hora de encriptar su mensaje
- ✓ Son más seguros, ya que aunque un intruso consiga la clave pública, no será capaz de encontrar la clave privada a través de la clave pública para poder desencriptar el mensaje
- ✓ El principal inconveniente es que resulta computacionalmente costosa su implementación
- ✓ Son más lentos que los algoritmos simétricos

Seguridad en la red
Algoritmos Asimétricos



Seguridad en la red
Algoritmos Asimétricos: RSA (Rivest, Shamir y Adleman)

- ✓ Es el algoritmo asimétrico más sencillo de comprender e implementar
- ✓ Su nombre proviene de sus tres inventores: Rivest, Shamir y Adleman
- ✓ Se basa en la dificultad para factorizar números grandes, así pues, las claves se calculan a partir de un número que se obtiene como producto de dos números primos grandes
- ✓ Algoritmo utilizado en el SSH (Secure Shell Client)
- ✓ Un tamaño de clave de 1024 bits (300 dígitos decimales aproximadamente) se considera lo suficientemente robusto para casi todas las aplicaciones

Seguridad en la red
Algoritmos Asimétricos: RSA (Rivest, Shamir y Adleman)

Paso 1: Generación del par de claves

- ✓ Se eligen aleatoriamente dos números primos grandes, p y q (de unas 200 cifras cada uno, por ejemplo). Después se calcula el producto n = p X q
- ✓ Se calcula un número e coprimo con el producto de (p-1) X (q-1) al que le llamamos $\phi(n)$. El par de números (e , n) pueden ser conocidos por cualquiera, y constituyen la llamada clave pública
- ✓ Se calcula d como el inverso del número e mod $\phi(n)$. La clave privada será el par (d , n). Este número d debe mantenerse secreto y sólo será conocido por el propietario del par de claves.

Seguridad en la red
Algoritmos Asimétricos: RSA (Rivest, Shamir y Adleman)

Paso 2: Cifrar del mensaje con la clave pública

Hay que hacer notar que con este algoritmo los mensajes que se cifran y descifran son números enteros de tamaño menor que n, no letras sueltas como en el caso de los cifrados César o Vignere.

Para obtener el mensaje cifrado C a partir del mensaje en claro M, se realiza la siguiente operación: $C = M^e \bmod n$

Paso 3: Descifrado del mensaje con la clave privada

Para recuperar el mensaje original a partir del cifrado se realiza la siguiente operación: $M = C^d \bmod n$

Seguridad en la red
Algoritmos Asimétricos: RSA (Rivest, Shamir y Adleman)

1. Silvia envía un mensaje encriptado a Mafalda
2. Mafalda adopta p = 5 ;q = 7 (para facilitarle las cuentas a Silvia), por lo tanto: n = 35 y z = 24,
3. Mafalda elige:

   e = 5; 5 y 24 son primos entre sí (e clave pública de Mafalda)

   d = 29 ; (5×29) mod 24 = 1, d clave privada de Mafalda

   El mensaje de Silvia consta de 4 palabras "JELP"
4. El mensaje llega a Mafalda y lo desencripta.

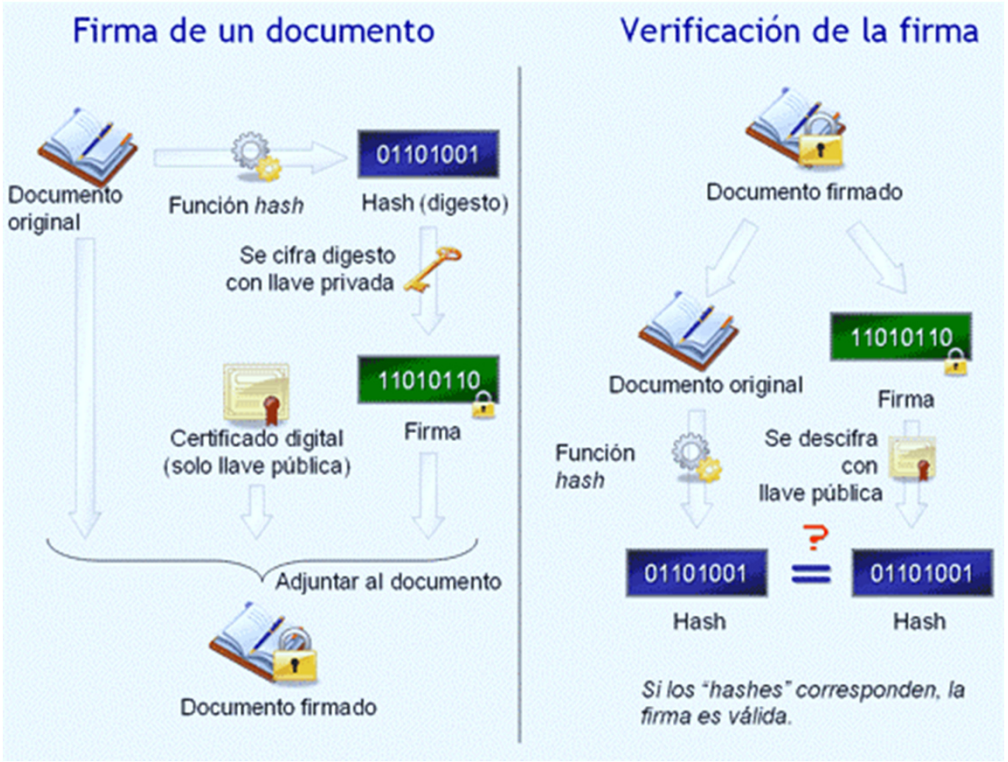
texto plano	Codif	m^e	texto cifrado $c = m^e \bmod n$
J	12	248832	17
E	15	759375	15
L	22	5153632	22
P	5	3125	10

texto cifrado	c^d	$m = c^d \bmod n$	texto plano
17	481968572106750915091509141182522307169 7	12	J
15	127834039403948858939111232757568359375	15	E
22	851643319086537701956194499721106030592	22	L
10	10000000000000000000000000000	5	P

Seguridad en la red
Función Hash

- ✓ Usadas para preservar la integridad de los datos (autenticación de mensajes), firma digital (autenticación de emisor o fuente), archivos de contraseñas (se almacena el hash de la contraseña) y para detectar intrusos o virus que puedan cambiar el contenido de archivos almacenados
- ✓ No tienen inversa
- ✓ Dado H(T) es imposible encontrar T
- ✓ Dado T no se puede encontrar T' tal que H(T) = H(T'); computacionalmente inviable
- ✓ MD5 (RFC 1321) 128 bits de hashing
- ✓ SHA-1(FIPS 1995)160 bits de hashing

Seguridad en la red
Función Hash: Ejemplo de Firma Digital



Seguridad en la red
Función Hash: SHA Secure Hash Algorithm

- ✓ En 1993, NIST publica *Secure Hash Standard* [FIPS 180]. Basado en el algoritmo MD4 de Ron Rivest
- ✓ En 1995, publica SHA-1 [FIPS 180-1] con un ligero cambio debido a un fallo significativo no revelado La versión original pasa a conocerse como SHA-0. En 2001, publica SHA-2 [FIPS 180-2] Revisado en 2008 [FIPS 180-3] y 2010 [FIPS 180-4]
- ✓ En 2005, se identifican fallos de seguridad en SHA-1, que comenzó a reemplazarse por SHA-2
- ✓ En 2012, una competición del NIST selecciona una nueva función SHA-3 [FIPS 202]

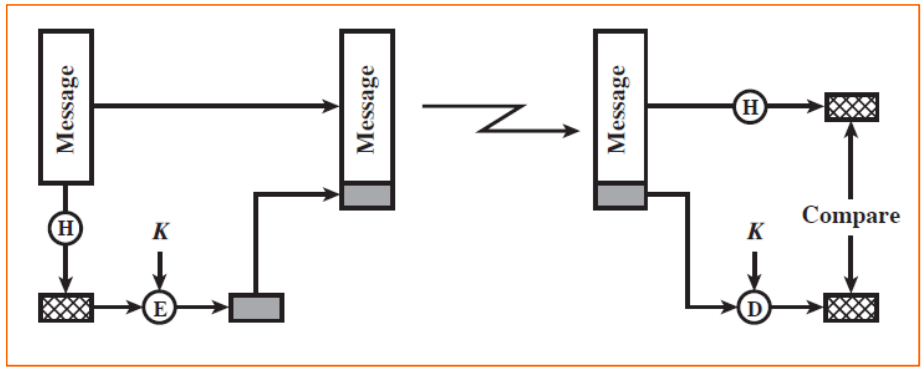
  No se basa en SHA-2 y no pretende reemplazarlo, sino que NIST percibe la necesidad de una alternativa diferente

Seguridad en la red
Función Hash: SHA Secure Hash Algorithm

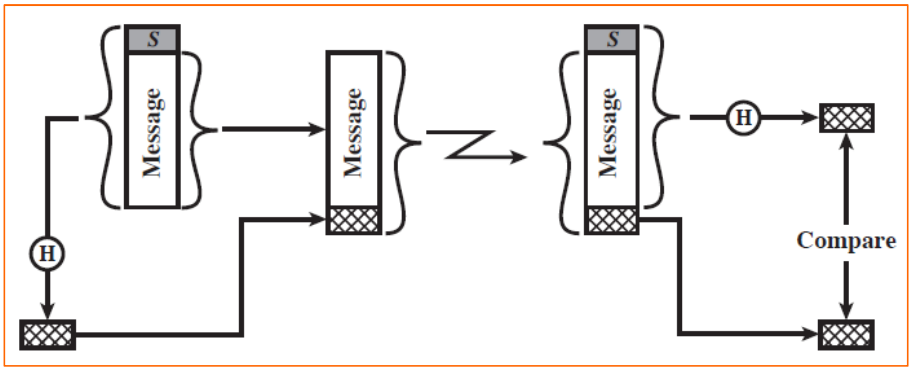
SHA-2 ⟷

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Seguridad en la red
Función Hash: Implementaciones



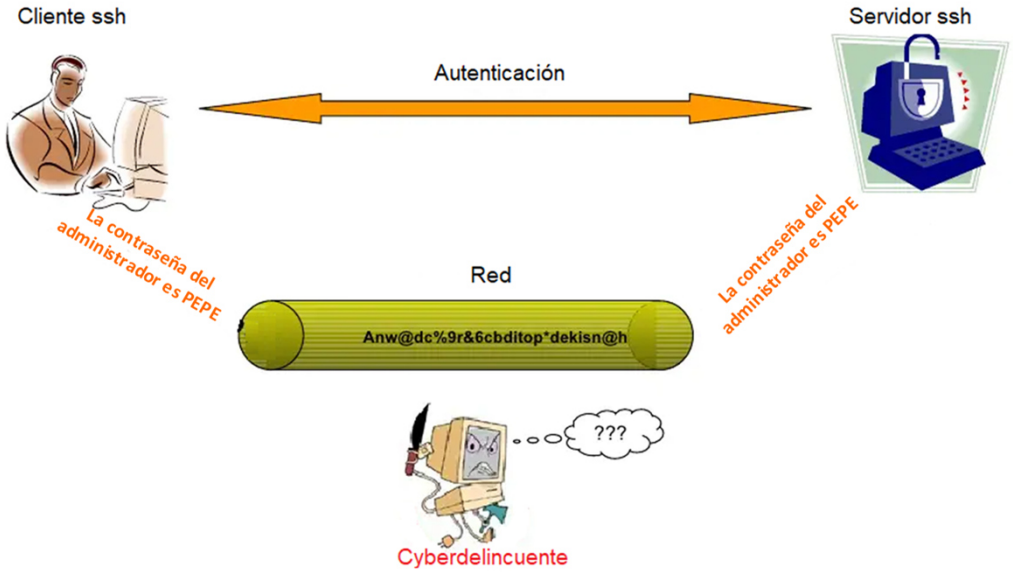
Autenticación de Mensajes con una función Hash y cifrado simétrico



Autenticación de Mensajes con una función Hash sin cifrado

Seguridad en la red
Protocolos Criptográfico: SSH (Secure Socket Shell)

- ✓ **SSH (Secure Shell)** Es un protocolo de capa de aplicación que hace posible que un cliente (un usuario o incluso un equipo) abra una sesión interactiva en una máquina remota (servidor) para enviar comandos o archivos a través de un canal seguro



Seguridad en la red
SSH (Secure Socket Shell): características

¿Qué es SSH?

- ✓ Es un Shell seguro
- ✓ Es un protocolo, no un producto
- ✓ Encripta datos enviados entre computadoras
- ✓ Tiene una arquitectura cliente/servidor
- ✓ Viene con todas las distribuciones de Linux, MAC OS, AIX, Sun Solaris, Open BSD, entre otros
- ✓ Se puede ejecutar en plataformas Windows
- ✓ Es el reemplazo de telnet, rlogin, rsh, rcp, ftp, etc.

¿Qué no es SSH?

- ✓ No es un verdadero Shell como sh, ksh y csh
- ✓ No es un intérprete de comandos
- ✓ No protege contra virus

Seguridad en la red

SSH (Secure Socket Shell): características

- ✓ Cifrado: SSH cifra todas las comunicaciones con variedad de algoritmos para elegir.
- ✓ Autenticación de dos factores: SSH puede requerir un nombre de usuario/contraseña o clave pública para la autenticación. Además, estas dos opciones pueden utilizarse juntas para conformar una autenticación de dos factores.
- ✓ Integridad: SSH puede crear una huella digital de los datos transferidos desde una entidad a otra, lo que garantiza que los datos no han sido modificados o manipulados de ningún modo

Seguridad en la red
Capas SSH (Secure Socket Shell)

Application Layer	**ssh-connection** Session multiplexing, X11 and port forwarding, remote command execution, SOCKS proxy, etc.
	ssh-userauth User authentication using public key, password, host based, etc.
	ssh-transport Initial key exchange and server authentication, setup encryption
Transport Layer	**TCP**
Internet Layer	**IP**
Network Access Layer	**Ethernet**

Seguridad en la red
SSH (Secure Socket Shell): software disponible

Microsoft	PUTTY, KPYM SSH SERVER, FREE SSHd, DROP BEAR, OPEN SSH, WINSSHD
	OPEN SSH
	RBROWSER

Seguridad en la red
Proxy: Definición

- ✓ Es una clase especial de servidor HTTP
- ✓ Entre sus funciones principales podemos citar:
  - ✓ Publicación de contenidos
  - ✓ Cache
  - ✓ Brindar anonimidad
  - ✓ Firewall (capa de aplicación)
    - ✓ Bloqueos de URL
    - ✓ Antivirus
- ✓ Encripción / Desencripción

Seguridad en la red
Proxy: Tipos

De acuerdo a su modo de funcionamiento podemos identificar:

1. Proxy de navegación:
   - ✓ Son utilizados para manejar requerimientos de salida
   - ✓ Escucha requerimientos de los clientes
   - ✓ Procesa los requerimientos y toma decisiones acerca de su ''forwardeo''
   - ✓ Los requerimientos son enviados a los servidores destino
   - ✓ Aguarda la respuesta de los servidores destino
   - ✓ Reenvía la respuesta al cliente
   - ✓ El usuario está en conocimiento de su existencia

Seguridad en la red
Proxy: Tipos

De acuerdo a su modo de funcionamiento podemos identificar:

2. Proxy de transparente
   - ✓ Son utilizados para manejar requerimientos de salida
   - ✓ Escucha requerimientos de los clientes
   - ✓ Procesa los requerimientos y toma decisiones acerca de su ‘’forwardeo’’
   - ✓ Los requerimientos son enviados a los servidores destino
   - ✓ Aguarda la respuesta de los servidores destino
   - ✓ Reenvía la respuesta al cliente
   - ✓ El usuario no conoce a priori de su existencia

Seguridad en la red
Proxy: Tipos

De acuerdo a su modo de funcionamiento podemos identificar:

3. Proxy de reverso
   - ✓ Tienen como propósito recolectar el tráfico dirigido hacia uno o mas servidores, y reenviar los requerimientos de los clientes al destino
   - ✓ Brindan:
     - ✓ Seguridad: Los requerimientos de los clientes nunca llegan directamente al servidor
     - ✓ Cifrado: SSL offload pasando datos planos o re-encriptando
     - ✓ Cacheo: Permiten cachear contenido
     - ✓ Balanceo de carga: Balancean los requerimientos en granjas de servidores
     - ✓ Otros…

Seguridad en la red
Proxy: Tipos

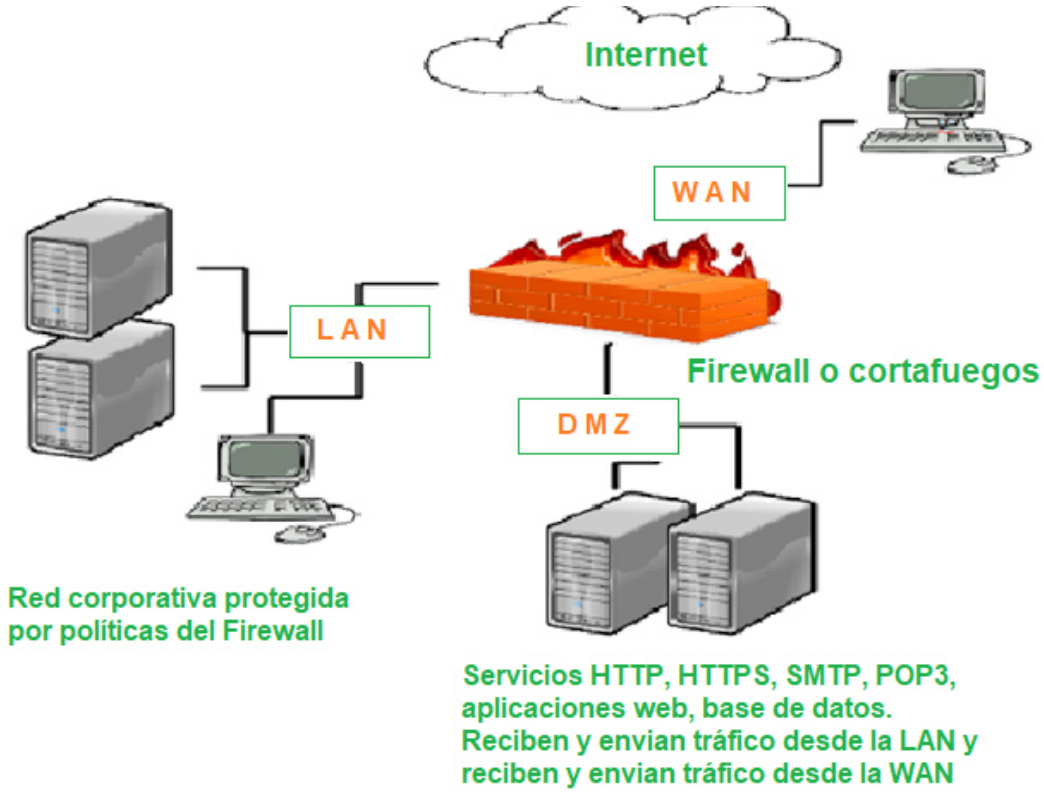
De acuerdo a su modo de funcionamiento podemos identificar:

3. Proxy de reverso
   - ✓ Tienen como propósito recolectar el tráfico dirigido hacia uno o mas servidores, y reenviar los requerimientos de los clientes al destino
   - ✓ Brindan:
     - ✓ Seguridad: Los requerimientos de los clientes nunca llegan directamente al servidor
     - ✓ Cifrado: SSL offload pasando datos planos o re-encriptando
     - ✓ Cacheo: Permiten cachear contenido
     - ✓ Balanceo de carga: Balancean los requerimientos en granjas de servidores
     - ✓ Otros…

Seguridad en la red
Firewall: concepto

- ✓ Un punto de control y monitorización implementado en hardware, o software, o una combinación de ambos
- ✓ Interconecta redes con diferente niveles de confianza
- ✓ Impone restricciones a los servicios de red
- ✓ Solo se permite el tráfico autorizado
- ✓ Auditoría y control de acceso
- ✓ Puede implementar alarmas para un comportamiento anormal
- ✓ Es inmune a la penetración
- ✓ Proporciona defensa perimetral

Seguridad en la red
Firewall: concepto



Seguridad en la red
Firewall: clasificación

Filtrado de Paquetes

- ✓ Filtrado Stateless: filtra paquetes IP según reglas llamadas "listas de control de acceso" (ACL)
- ✓ Filtrado Stateful: filtra controlando el estado de las sesiones

Gateway de Aplicaciones

- ✓ Proxy Server (visto anteriormente)
- ✓ DPI (Deep Packet Inspection)

Seguridad en la red
Firewall: Filtrado de paquetes

Filtra paquete por paquete según reglas:

- ✓ IP origen, IP destino
- ✓ TCP/UDP puerto origen / destino
- ✓ ICMP
- ✓ TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
- ✓ No tiene en cuenta estado de la conexión: Stateless
- ✓ Nivel más básico de filtrado
- ✓ No garantiza buen nivel seguridad para complejidad de ataques actuales
- ✓ Necesita políticas muy restrictivas para mejorar protección

Seguridad en la red
Firewall: Filtrado de paquetes Stateless

Ejemplos

- ✓ Bloquear datagramas entrantes y salientes cuyo campo IP protocol = 47 y tambien cuando campo puerto origen o destino sea = 21

  Resultado: tráfico VPN PPTP over GRE bloqueado y FTP bloqueado

- ✓ Bloquear segmentos TCP entrantes con ACK=0.

  Resultado: evita conexiones TCP iniciadas en la red externa, pero permite que clientes internos inicien sesiones TCP a servidores externos.

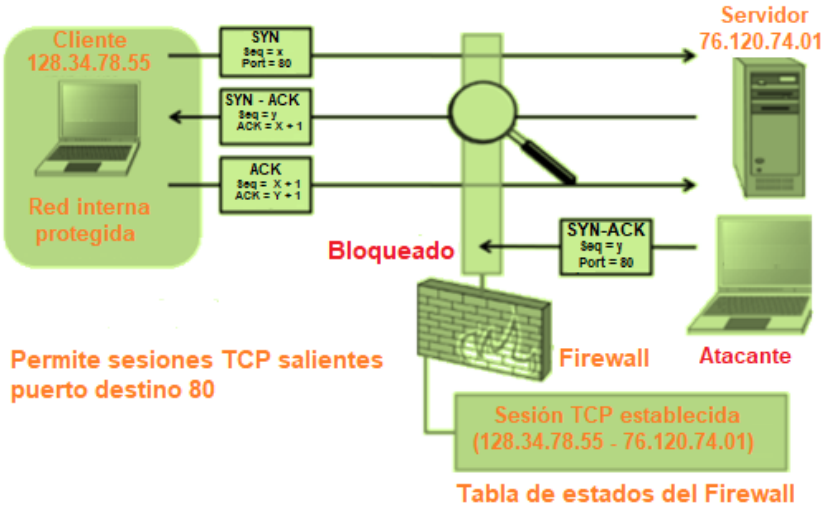
Seguridad en la red
Firewall: Filtrado de paquetes Stateless

Lista de Control de Accesos

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

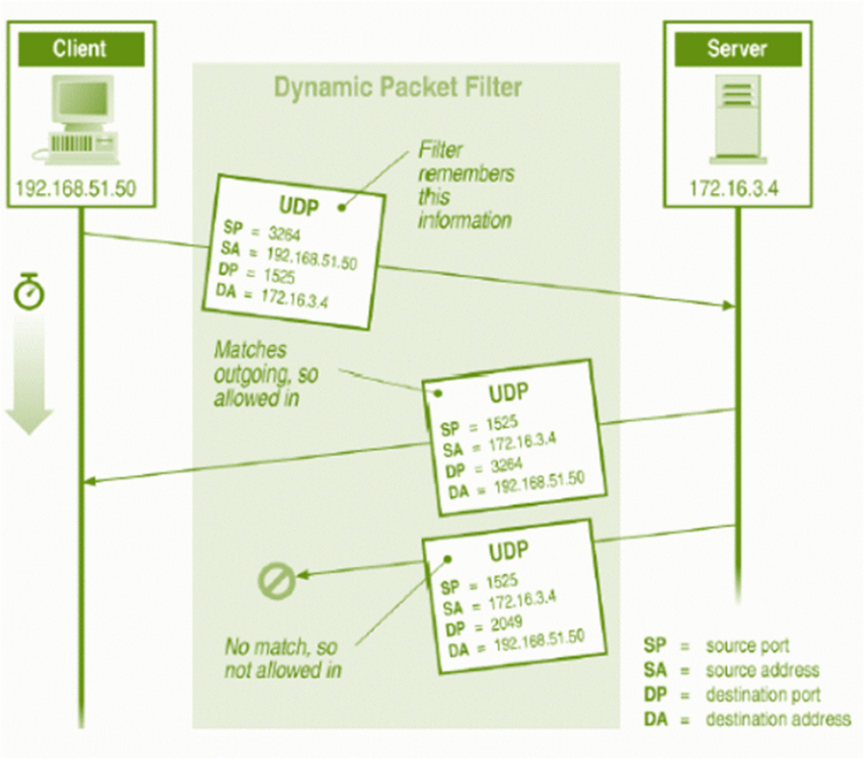
Seguridad en la red
Firewall: Filtrado de paquetes Stateful

- ✓ Lleva un registro del estado cada conexión
- ✓ Registro de establecimientos de conexiones (SYN) y de cierres (FIN)
- ✓ Aumenta seguridad
  - ✓ Detecta tráfico que no pertenece a la sesión
  - ✓ Cierra conexiones inactivas



Seguridad en la red
Firewall: Filtrado de paquetes Stateful

Ejemplo, se permite tráfico UDP sólo si fue generado por un cliente interno



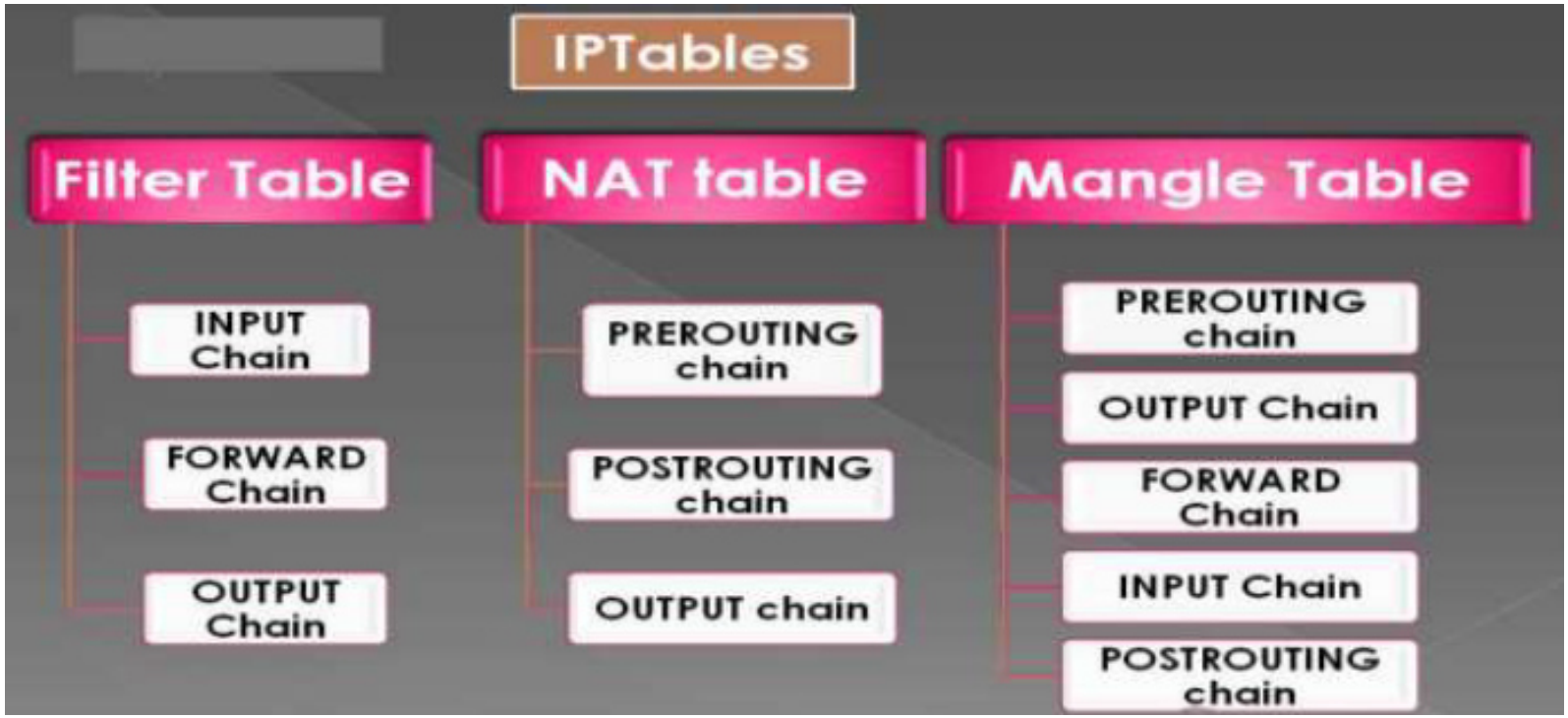
Seguridad en la red
IP-Tables (Proxy Transparente y Firewall)

- ✓ El software básico de cortafuegos utilizado en Linux se llama iptables.
- ✓ iptables es un programa de utilitario para usuario, el cual permite a un administrador de sistema configurar las tablas proporcionadas por el firewall del kernel de Linux (implementadas como diferentes módulos de Netfilter) y las cadenas y reglas que almacena.
- ✓ El subsistema de procesamiento de paquetes de red del kernel de Linux es llamado
- ✓ iptables protege al cliente y al servidor de accesos no autorizado.
- ✓ El Firewall del núcleo de Linux tiene la capacidad incorporada de filtrar paquetes y permitir el tráfico de red saliente y entrante en una PC
- ✓ Es un potente Firewall por software

Seguridad en la red
IP-Tables: ¿Qué se puede hacer?

- ✓ Controlar el tráfico de la red
- ✓ Bloquear todo el tráfico y permitir sólo el tráfico de ciertas direcciones IP.
- ✓ Configurar reglas específicas. Actúa como un filtro de paquetes que examina y dirige el tráfico basado en el puerto, el protocolo y otros criterios
- ✓ Estructura: "Tables" que tienen "Chains" y las "Chains" que contienen "Rules": Tables --> Chain -> Rules
- ✓ Las "Tables' son conjunto de "Chains", y las "Chains' son un conjunto de "Rules" de firewall.
- ✓ Las "Rules" se definen para controlar los paquetes de entrada/salida

Seguridad en la red
IP-Tables: Estructura



Seguridad en la red
IP-Tables

Filtrado de Paquetes (Packet Filtering)

Es el tipo más básico de procesamiento de paquetes de red de la red. Este, implica examinar los paquetes en varios puntos mientras se mueven a través de la red y tomar decisiones sobre qué hacer con ellos: aceptarlos o descartarlos.

Network Address Translation (NAT)

Es un tipo de manipulación de paquetes que consiste en sobrescribir las direcciones origen y/o destino, como así también los números de puerto. Información de seguimiento de la conexión es usada para manipular los paquetes de una u otra forma específica.

Manipulación de paquetes (Packet Mangling)

Implica la realización de cambios en los campos de la cabecera del paquete (como las direcciones de red y los números de puerto) o en el cuerpo del paquete (Payload)

Seguridad en la red
IP-Tables: “Rules” en las “Chains”

Hay cinco tipos de reglas implementadas en todos los tipos de iptables “chains”:

1. Entrada (INPUT): La “chain’ de entrada se utiliza para cualquier paquete que “ingrese” en el sistema. Utilizada por las Tablas Mangle y Filter.

2. Salida (OUTPUT): La “chain” de salida es para cualquier paquete que “egrese” del sistema. Utilizada por las tablas Mangle, NAT y las tablas de filtrado.

3. Reenvío (FORWARD): La “chain” de reenvío es para los paquetes que son reenviados (enrutados) a través del sistema. Utilizada por las Tablas Mangle y Filter.

4. Preenrutamiento (Prerouting): El preenrutamiento permite alterar los paquetes antes de que lleguen a la “chain” de entrada. Utilizadas por las Tablas Mangle y NAT

5. Posenrutamiento (Postrouting): El posenrutamiento permite alterar los paquetes después de que salgan de la “chain” de salida. Se utiliza por las tablas Mangle y NAT

Seguridad en la red
IP-Tables: Target

Todas las reglas de iptables tienen algún “target" que se ejecuta. Si un paquete coincide con la regla (rule), el “target” especifica lo que debe hacerse con él. Por ejemplo, un paquete puede ser aceptado, descartado, registrado o enviado a otra cadena para ser comparado con más reglas.

ACCEPT: El paquete es aceptado y pasa a la aplicación para su procesamiento.

DROP: El paquete ha sido descartado. No se envía al remitente ninguna información acerca del paquete

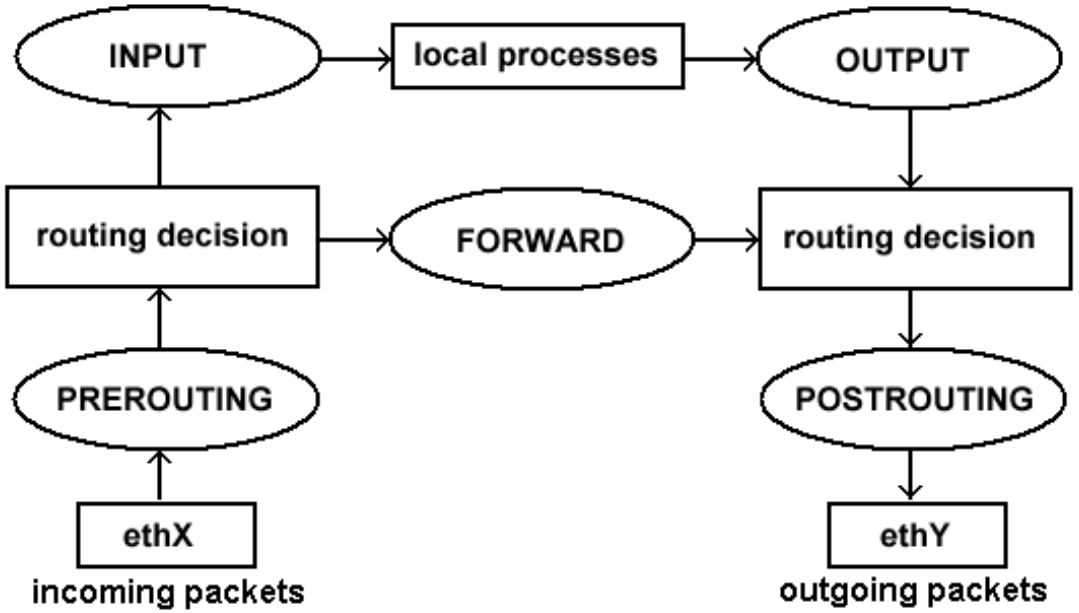
REJECT: El paquete se descarta y se envía un mensaje de información (error) al remitente.

LOG: Se envían los detalles del paquete para su registro.

DNAT: Reescribe la IP de destino del paquete

SNAT: Reescribe la IP de origen del paquete

Seguridad en la red
IP-Tables: Flowchart



Seguridad en la red
IP-Tables: Comandos de inicio

iptables –F : Borra todas las reglas.

iptables –X : Borra cadenas

iptables –Z : Borra los contadores

iptables -t nat –F -t table_name : Selecciona una tabla y elimina reglas

iptables -t nat -X

iptables -t mangle -F

iptables -t mangle -X

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

P: Establece la política por defecto (como DROP, REJECT o ACCEPT)

Creación y borrado de reglas

iptables [-t table] -A chain rule-spec

iptables [-t table] -I chain [rulenum] rule-spec

iptables [-t table] -R chain rulenum rule-spec

iptables [-t table] -D chain rule-spec

iptables [-t table] -D chain rulenum

Las opciones son las siguientes:

-A: añade una regla al final de la lista

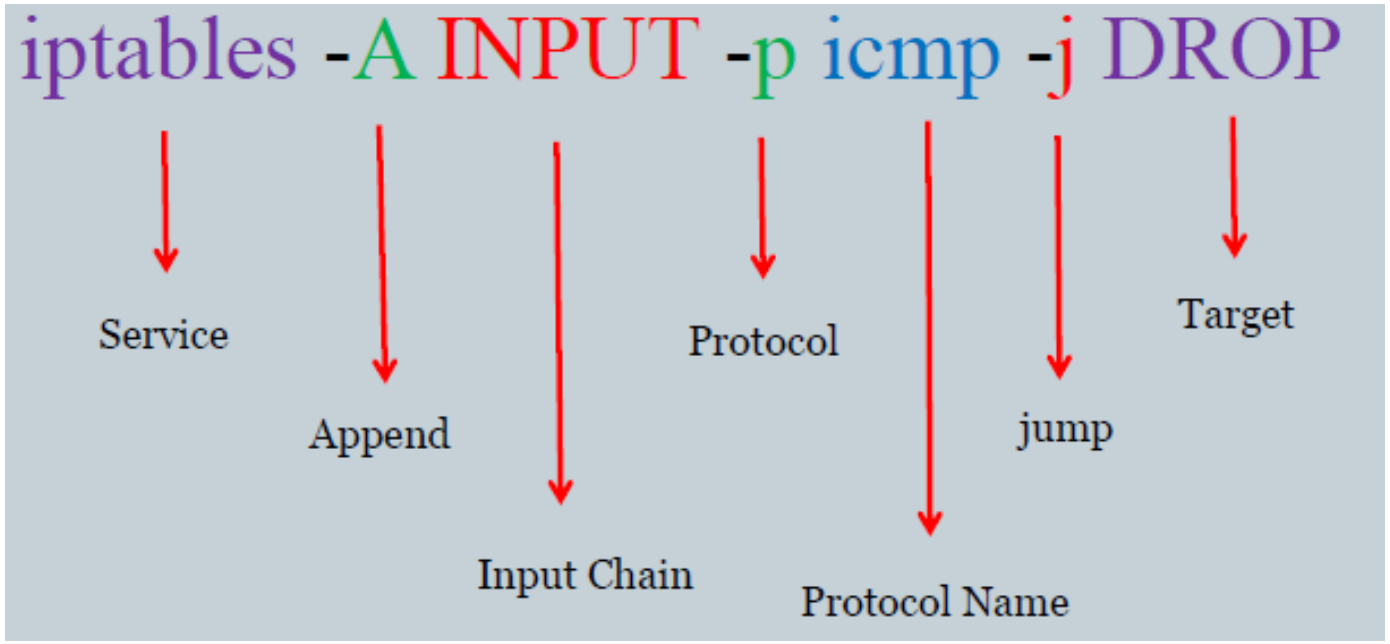
-I: inserta una regla al comienzo de la lista o en el punto especificado

-R: reemplaza una regla (especificada por su número de regla) por otra

-D: borra una regla determinada

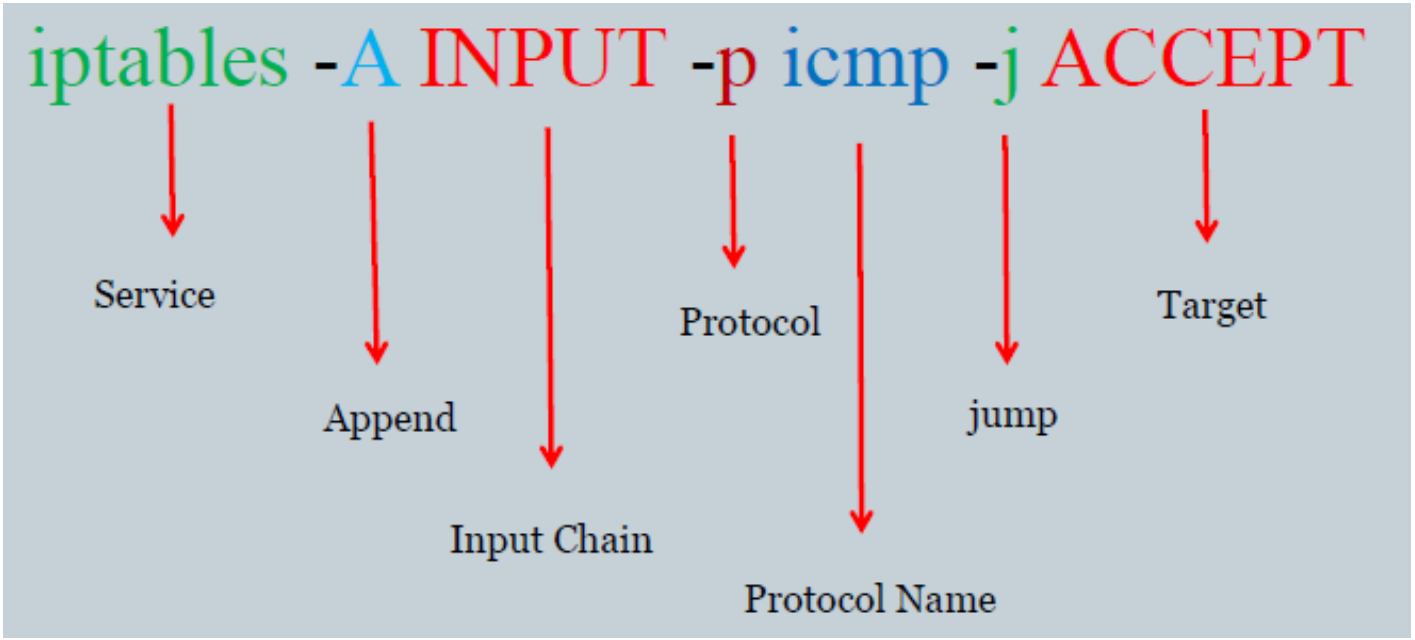
Seguridad en la red
IP-Tables: Ejemplos

iptables -A INPUT -p icmp -j DROP (descarta la solicitud de respuesta a un ping)



Seguridad en la red
IP-Tables: Ejemplos

iptables -A INPUT -p icmp –j ACCEPT (acepta la solicitud de respuesta a un ping)



Temas a tratados

1. Requisitos de seguridad y tipos de ataque
2. Criptografía
   a) Cifrado Simétrico
   b) Cifrado Asimétrico
   c) Función Hash
3. Proxy
4. Firewall
5. Firewall de uso libro: *"iptables"*

FINAL DEL MÓDULO 10