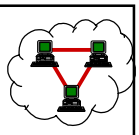
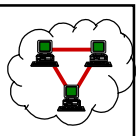


# Seguridad Perimetral

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez

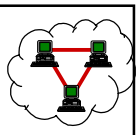




## Protegiendo el ¿perímetro?

- ¿Qué es el perímetro?
- Es una frontera fortificada que puede incluir lo siguiente
  - Ruteadores
  - Firewalls
  - IDSs
  - Dispositivos VPNs
  - Software
  - DMZs y subredes screened

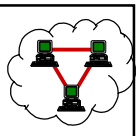
## Los elementos



- Ruteador fronterizo (border router)
  - último ruteador bajo control antes de Internet
- Firewall
  - dispositivo que reúne reglas que especifica que tráfico se permite o se rechaza
- IDS
  - sistema de alarma de la red, para detectar y alertar eventos maliciosos
- VPN
  - es una sesión de red protegida formada a través de canales no protegidos, como Internet

Lámina 3 Roberto Gómez Cárdenas

## DMZ y Screened Subnets



- Hacen referencia a una pequeña red que contiene servicios públicos conectados directamente a una protección ofrecida por el firewall o cualquier dispositivo de filtrado.
- DMZ: Zona Desmilitarizada
  - termino guerra Corea
  - área insegura entre áreas seguras
  - aplicado en firewalls localizada fuera del firewall
- El firewall protoge una subred screened que se encuentran directamente conectada a él.

Lámina 4 Roberto Gómez Cárdenas

## Diferencia DMZ y screened

- Una DMZ se encuentra en frente del firewall mientras que una subred screened esta detrás del firewall

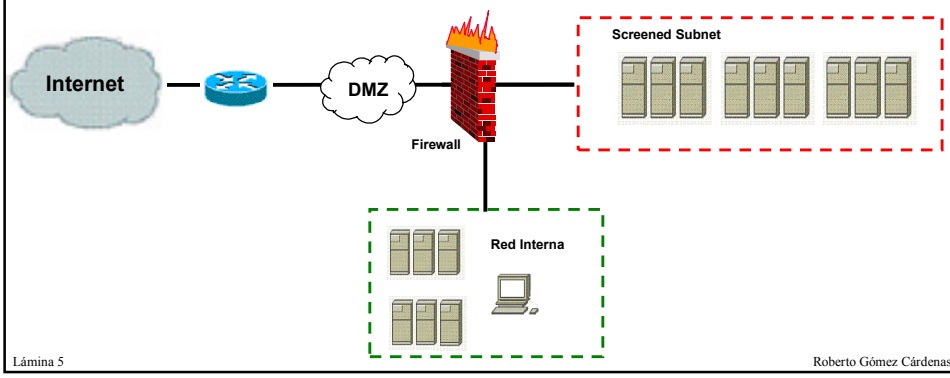


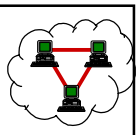

Lámina 5 Roberto Gómez Cárdenas

## El filtrado de información

Filtrado paquetes, firewalls y proxies

Lámina 6 Roberto Gómez Cárdenas

## Filtros paquetes estático



- Uno de los más viejos y usados medios para control acceso a las redes.
- Concepto simple
  - determinar si a un paquete se le permite entrar o salir la red, comparando algunos elementos de información básicos que se encuentran en el encabezado del paquete
- Tecnología filtrado paquetes se puede encontrar en sistemas operativos, software y firewalls tipo hardware, y como una característica de varios ruteadores.

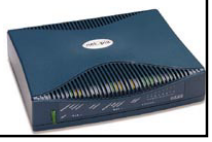
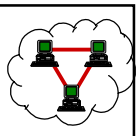


Lámina 7

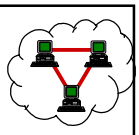
## ¿Por qué filtrado paquetes?



- Vieja tecnología
  - no posee capacidad de diferencias entre diferentes tipos de tráfico de red
- Algunas veces medios más ligeros y menos caros pueden representar una ventaja
  - filtros paquetes más rápidos que tecnologías de firewall
  - filtros de paquetes no realizan un análisis a fondo del flujo de tráfico
  - velocidad a la cual se puede verificar la información de los encabezados de los paquetes
  - paquetes no necesitan ser decodificados a nivel aplicación para tomar una decisión
  - ya son parte de la infraestructura de la red

Lámina 8 Roberto Gómez Cárdenas

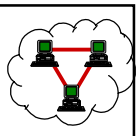
## Ruteador Cisco como filtrado paquetes



- Cisco ACL es uno de los filtros paquetes más disponibles hoy en día.
- Dos tipos de listas de control de acceso:
  - ACL: Access Control List (lista control de acceso)
    - verifica tráfico en base a dirección IP sistema fuente
  - Listas extendidas (Cisco Extended ACL )
    - filtrado dirección destino, tipo protocolo, información número puerto capa 4, banderas y demás

Lámina 9 Roberto Gómez Cárdenas

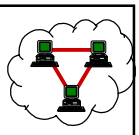
## Problemas filtros paquetes



- Spoofing and source routing
  - spoofing: enviar paquete con una dirección fuente falsa
  - posible enviar paquete con dirección de un host interno o de un host “confiable”
  - source routing: paquete con información que dice al ruteador la forma correcta, o mejor, de regresar de donde viene
  - permite atacante dirigir tráfico de regreso a donde él quiera
  - sugerencia: deshabilitar source-routing

Lámina 10 Roberto Gómez Cárdenas

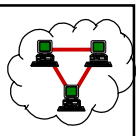
## Problemas filtros paquetes



- Fragmentación
  - ataques fragmentación creados para contrarrestar tecnología de filtro de paquetes
  - paquete es dividido en pequeñas piezas de tal forma que el encabezado con información TCP o UDP es dividido
  - generalmente primer paquete es el único revisado todo el paquete dividido pasará

Lámina 11 Roberto Gómez Cárdenas

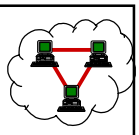
## Soluciones fragmentaciones



- RFC 1858 define métodos para combatirlo
  - eliminar fragmentos tamaño menor que un valor dado
  - eliminar fragmentos secundarios basados en información incluida en ellos
- Verificar que se tienen la última versión en firmware y en parches de seguridad
- Algunos firewalls reensamblan paquetes antes aplicar regla
- Formación de tablas que toman decisiones en base a los fragmentos iniciales
- Chequeo fragmentos no-iniciales en base a precedentes
- Posible deshabilitar fragmentación paquetes

Lámina 12 Roberto Gómez Cárdenas

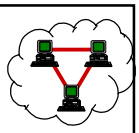
## ACL reflexivas



- Filtros son construidos a “tiempo real” conforme se necesitan y deshabilitados después de una conexión
- Ejemplos de tecnología de filtrado paquetes dinámico
- Criterio definido en base a interfaz de salida que observa conexiones definidas en el mundo de afuera
- Cuando tráfico regresa, es comparado con una lista de acceso creada dinámicamente conforme el tráfico deja la red

Lámina 13 Roberto Gómez Cárdenas

## Ejemplo ACL reflexiva



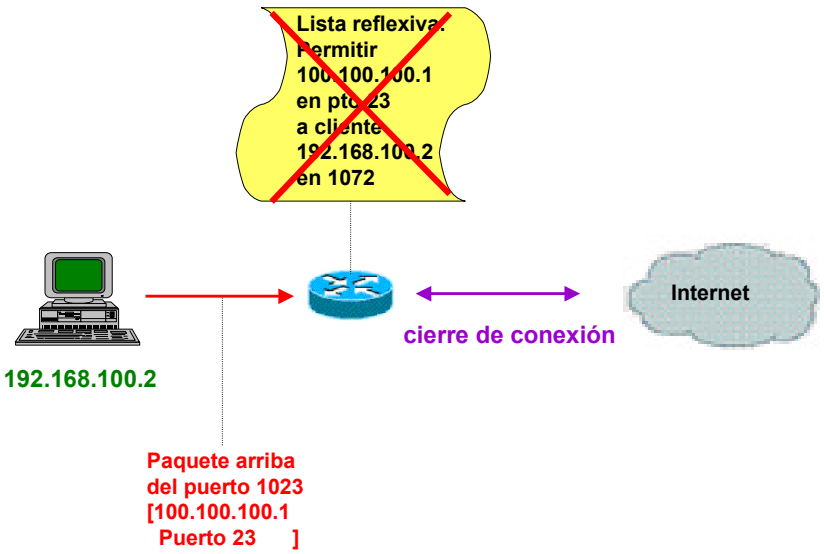
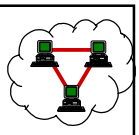



Lámina 14 Roberto Gómez Cárdenas

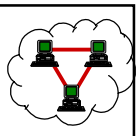
## Stateful Firewalls



- Firewalls que intentan dar seguimiento a una conexión cuando se tiene filtrado de paquetes.
- Se pueden considerar entre un filtro de paquetes y un proxie.
- Predominantemente examinan capa 4 e información paquetes más baja
  - frecuentemente verifican solo capa 7 (aplicación)
- Si paquete coincide con regla del firewall que permite su paso, se crea una entrada en la tabla de estados
  - paquetes posteriores de la misma conexión son permitidos sin realizar más inspecciones

Lámina 15 Roberto Gómez Cárdenas

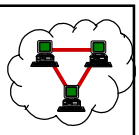
## Concepto de estado

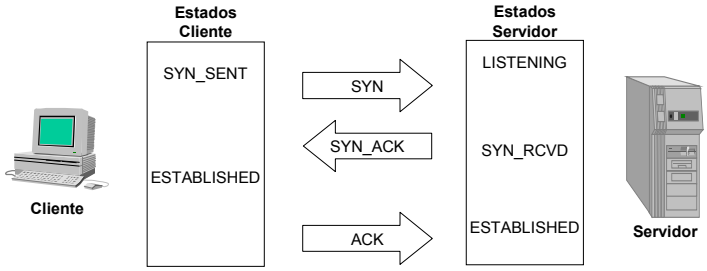


- Concepto confuso
  - puede tener diferentes significados en diferentes situaciones
- Definición básica
  - la condición en que se encuentra una determinada sesión de comunicación
- Diferentes vendedores dan una definición diferente de lo que es un estado.
- Dispositivos que dan seguimiento a un estado lo hacen a través de una tabla.
  - tabla mantiene entradas de lo que representa una sesión de comunicación individual.

Lámina 16 Roberto Gómez Cárdenas

# Estados TCP 3-way handshake

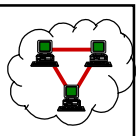


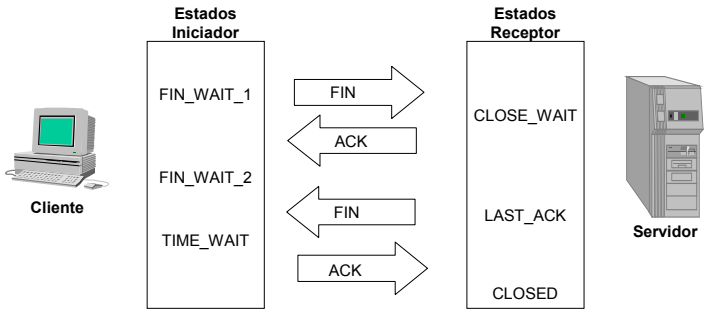



- CLOSED: no-estado antes conexión empiece
- LISTEN: host espera petición conexión
- SYN-SENT: host envió paquete syn y espera syn_ack
- SYN-RCVD: host recibió paquete syn y respondio con syn_ack
- ESTABLISHED: host iniciador recibió un syn-ack y el host receptor recibió paquete ack

Lámina 17 Roberto Gómez Cárdenas

# Estados TCP para cierre conexiones






- FIN-WAIT_1: después envío paquete inicial FIN
- CLOSE-WAIT: después recepción FIN y envío de regreso ACK
- FIN-WAIT-2: host recibió ACK a su envío de paquete FIN
- LAST-ACK: envío del segundo ACK para cerrar la conexión TCP
- TIME-WAIT: host inicial recibió FIN final y envío ACK y cerrar conexión
- CLOSING: la conexión fue cerrada en ambos lados

Lámina 18 Roberto Gómez Cárdenas

## Estados TCP para cierre conexiones simultaneo

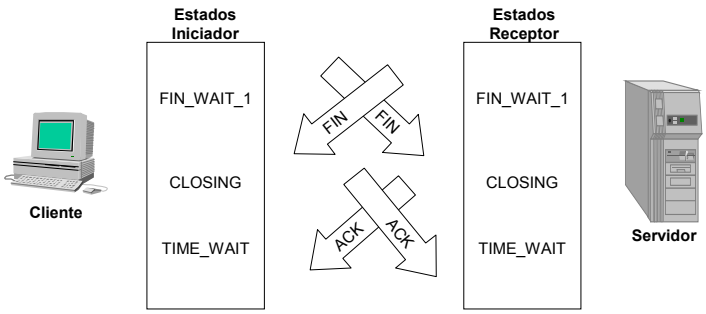


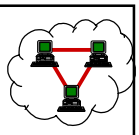

Lámina 19 Roberto Gómez Cárdenas

## Estado UDP

- UDP: protocolo orientado no-conexión
- Seguimiento del estado más complicado
  - no hay números de secuencia ni banderas
  - puertos son aleatorios
  - no hay un protocolo de abertura ni de cierre
- Un protocolo orientado no-conexión no cuenta con estado
  - solo pseudo-estados basados en aspectos específicos a la conexión
- Una opción son los número de puertos y las direcciones IP

Lámina 20 Roberto Gómez Cárdenas

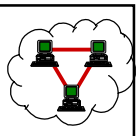
## Netfilter/IPTables



- Los dos piezas principales de producto firewall disponibles gratuitamente para distribuciones Linux
- IPTables es usado para construir las reglas.
- Netfilter es puente entre núcleo linux y las IPTables
- IPTables es como se conoce al módulo Netfilter
  - herramienta estándar actual de firewall de Linux
- Administradores especifican que reglas que protocolos o tipos de tráficos se deben seguir.
  - cuando empieza conexión con protocolos IPTables añade una entrada de estado para la conexión en cuestión

Lámina 21 Roberto Gómez Cárdenas

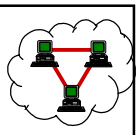
## Un poco de historia



- Linux cuenta con filtrado paquetes (IPFW) incorporado en su núcleo desde versión 1.1
  - adaptación herramienta ipfw del sistema operativo BSD
- Holandés Jos Vos junto con otras personas mejora filtrado paquetes para versiones núcleo 2.0
  - introduce herramienta configuración ipfwadm
- Mediados 1998 aparece ipchains
  - todavía es utilizada en varios Linux
  - solo se asegurará su compatibilidad hasta 2003
- En 1999 Rusty Russell diseña iptables
  - iptables es una modificación que permite construir reglas más precisas y un mejor aprovechamiento de los recursos

Lámina 22 Roberto Gómez Cárdenas

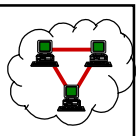
## Filtrado de IPTables



- Filtrado de dirección remota
- Filtrado de dirección destino local
- Filtrado de puerto de origen remoto y destino local
- Filtrado del estado de la conexión TCP
- Sondeos y exploraciones de puertos
- Ataque DoS

Lámina 23 Roberto Gómez Cárdenas

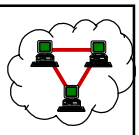
## La utilería *iptables*



- Herramienta para crear las reglas del firewall
  - si se desea un conocimiento exhaustivo de todas las opciones de la utilidad iptables, lo mejor es consultar el manual
  - también se cuenta con un HowTo
- Recordar:
  - tablas compuestas de lista reglas (cadenas)
  - regla es un par condición/acción sobre atributos paquetes
  - paquete pasa secuencialmente por cada una de las reglas
  - si paquete cumple con regla se realiza acción regla
  - si paquete no cumple con ninguna regla, se ejecuta la acción por default asociada a dicha cadena

Lámina 24 Roberto Gómez Cárdenas

## Un primer ejemplo



- Un ping normal y un ping bloqueado

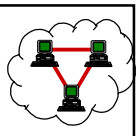
```
# ping -c 1 127.0.0.1
    PING 127.0.0.1 (127.0.0.1): 56 data bytes
    64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.2 ms

    --- 127.0.0.1 ping statistics ---
    1 packets transmitted, 1 packets received, 0% packet loss
    round-trip min/avg/max = 0.2/0.2/0.2 ms
# iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
# ping -c 1 127.0.0.1
    PING 127.0.0.1 (127.0.0.1): 56 data bytes

    --- 127.0.0.1 ping statistics ---
    1 packets transmitted, 0 packets received, 100% packet loss
#
```

Lámina 25 Roberto Gómez Cárdenas

## Restringiendo accesos servicios

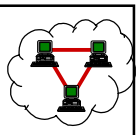


- Para permitir accesos al servidor HTTP, FTP o SSH del host cognac, desde cualquier lugar

```
# iptables –t filter –A INPUT –p TCP – s 0/0 - - dport 21 –j allowed
# iptables –t filter –A INPUT –p TCP – s 0/0 - - dport 22 –j allowed
# iptables –t filter –A INPUT –p TCP – s 0/0 - - dport 80 –j allowed
```

Lámina 26 Roberto Gómez Cárdenas

## Ejemplo bitácoras



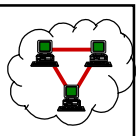
```
# iptables -A INPUT -s 192.168.1.1 -j LOG -log-prefix Test:
#
```

- Indica añadir una regla a la cadena de INPUT (-A INPUT) que verifique los paquetes que vengan de 192.168.1.1 (-s 192.168-1-1) y brinca a la fuente log (-j LOG) con una línea que empieza con los caracteres Test:
- La bitácora generada es detallada y completa
- Un ejemplo sería:

```
Test:IN=ppp0 OUT=
SRC=192.168.1.1 DST=1.2.3.4
LEN=100 TOS=0x00 PREC=0x00
TTL=253 ID=0 PROTO=ICMP
TYPE=8 CODE=0 ID=56 SEQ=58
```

Lámina 27 Roberto Gómez Cárdenas

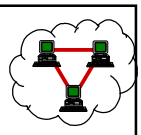
## Firewalls tipo proxy



- Servidor proxy algunas veces application gateway
  - aplicación que proporciona comunicación vía protocolos de Internet entre la red protegida y el mundo exterior (Internet).
- En general proxies trabajan para programas basados en el protocolo TCP/IP.
- Servidores proxies ejecutan algunos programas (proxies) que pueden ser asegurados y confiables.
- Específicos a la aplicación
  - cada protocolo que es soportado debe contar con su propio servicio de proxy o debe ser manejado por un proxy general.

Lámina 28 Roberto Gómez Cárdenas

## Esquema general

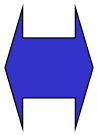


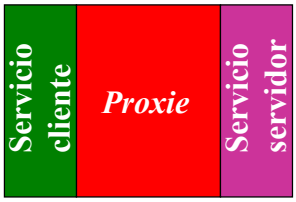
1. cliente realiza petición al servidor

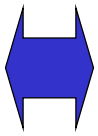
7. proxy le responde al cliente.

6. proxy toma la respuesta y la verifica

5. servidor envia respuesta al cliente





***Cliente***

2. el proxy toma la petición y realiza un chequeo

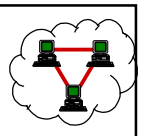
3. después del chequeo se envía la petición al servidor

***Servidor***

4. servidor toma la petición "depurada" y la procesa

Lámina 29 Roberto Gómez Cárdenas

## Bastion host y dual homed hosts



- Servidor proxy corre tipicamente en un host conocido como dual-homed bastion o gateway y soporta uno o más protocolos de internet.
- Bastion hosts
  - sistemas asegurados y configurados con funciones accesibles por Internet
- Dual homed gateway
  - host con un sistema con dos interfaces de red
  - una de ellas protege la red interna
  - la otra para la red externa

Lámina 30 Roberto Gómez Cárdenas

## Esquema dual homed y bastion host

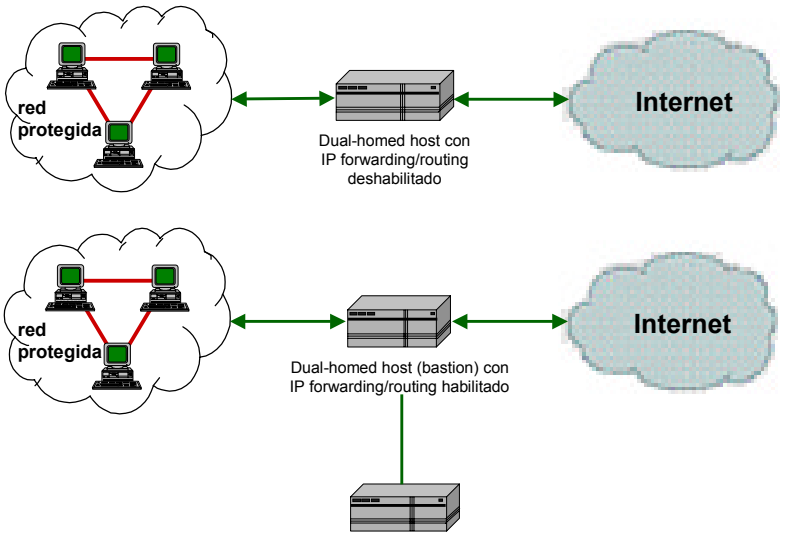


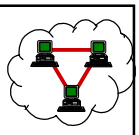

Lámina 31 Roberto Gómez Cárdenas

## Firewalls tipo proxies

- Actuan a nivel capa de aplicación
- Proxies proporcionan más habilidad para auditorias
- Requieren más configuración y reduce el número de servicios disponibles para los usuarios.
- Requiere modificar los procedimientos usuarios
  - especificar número puerto para acceder una página web
  - el puerto 80 es bloqueado el servidor web y solo se acepta tráfico HTTP en el puerto 8080
  - otro servicio a modificar puede ser FTP

Lámina 32 Roberto Gómez Cárdenas

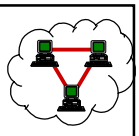
## Check Point FireWall-1



- Uno de los firewalls más populares
- Software puede ser implementado en un servidor hardware o en varios tipos de plataformas:
  - NT, 2000, Solaris y Linux Red Hat
- Nokia ofrece una solución de tipo hardware
- Utiliza una tabla de estados para el seguimiento de conexiones a nivel protocolos y una máquina de inspección para reglas más complicadas
  - involucra tráfico capa aplicación y comportamiento de protocolo no estándar

Lámina 33 Roberto Gómez Cárdenas

## Chequeo paquetes en Checkpoint



- Para decidir si un paquete pasa o no, se prueba contra las siguientes estructuras de datos, especificadas en orden
  1. Tabla de estados: verifica si una conexión se encuentra en la tabla de estados, para un paquete que entra.
     - Si es así es redireccionado sin ningún escrutiño extra.
  2. Política de seguridad: si la tabla de estado no contiene ninguna entrada relacionada con el paquete, este es comparado contra la política de seguridad.
     - Si una regla permite al paquete pasar, será redireccionado y una entrada será añadida a la tabla de estados.

Lámina 34 Roberto Gómez Cárdenas

## Los objetos de Checkpoint

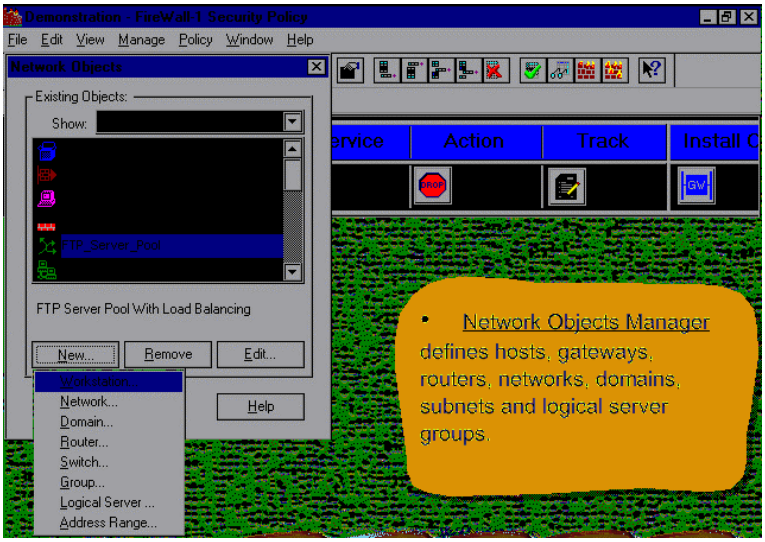



Lámina 35 Roberto Gómez Cárdenas

## Las acciones en Checkpoint

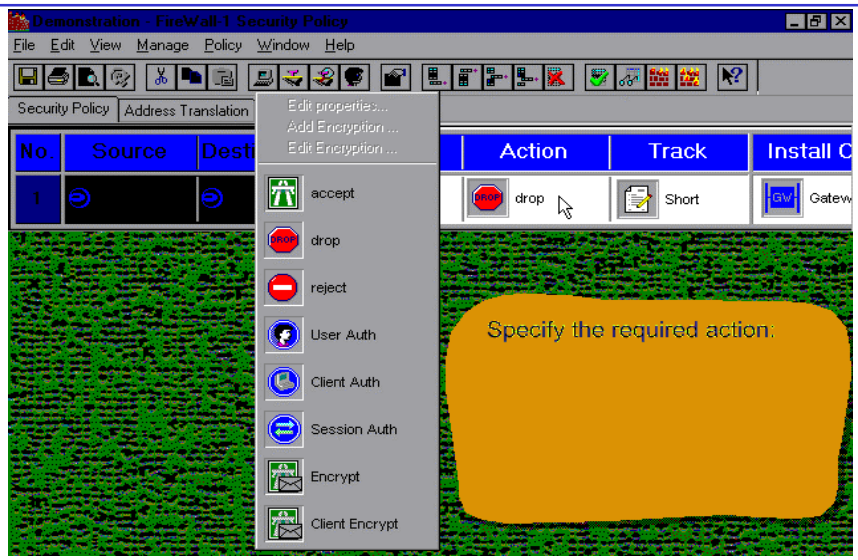



Lámina 36 Roberto Gómez Cárdenas

# Ejemplos reglas

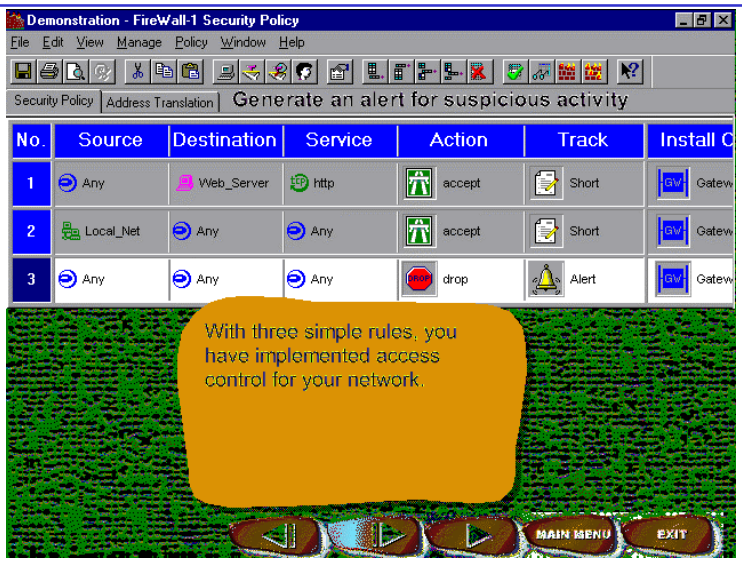



Lámina 37 Roberto Gómez Cárdenas

# Autenticación en Checkpoint

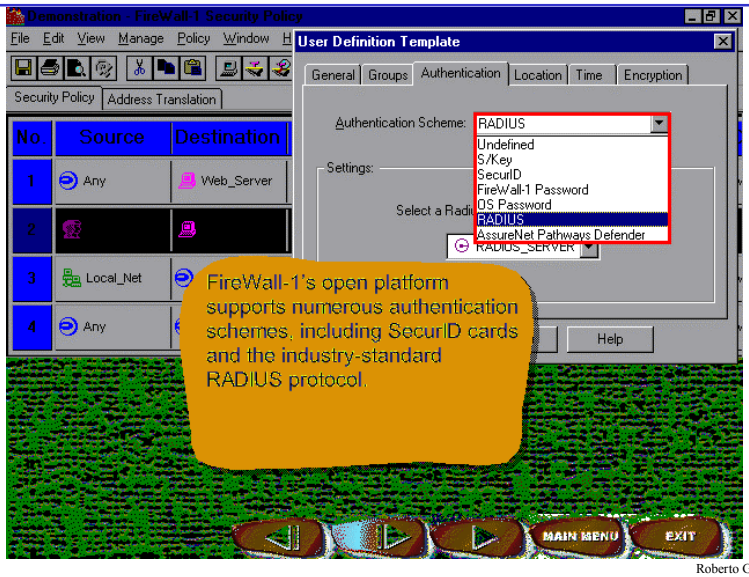



Lámina 38 Roberto Gómez Cárdenas

# Encripción en Checkpoint

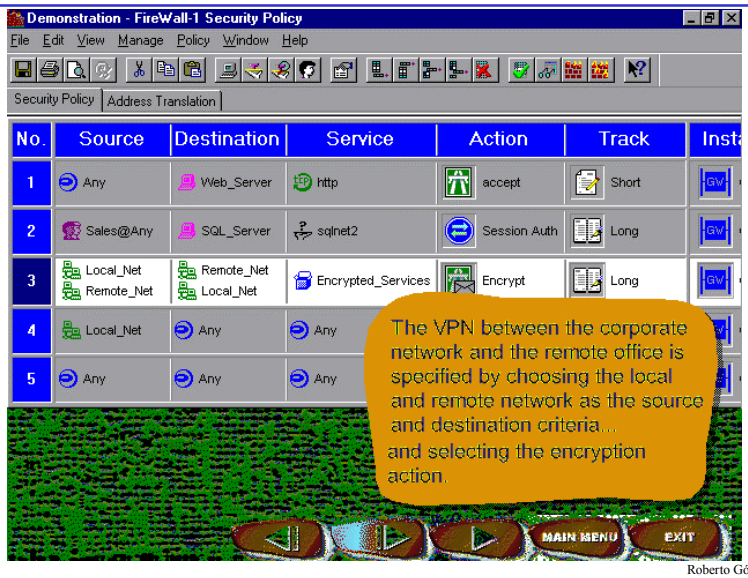



Lámina 39 Roberto Gómez Cárdenas

# NAT en Checkpoint

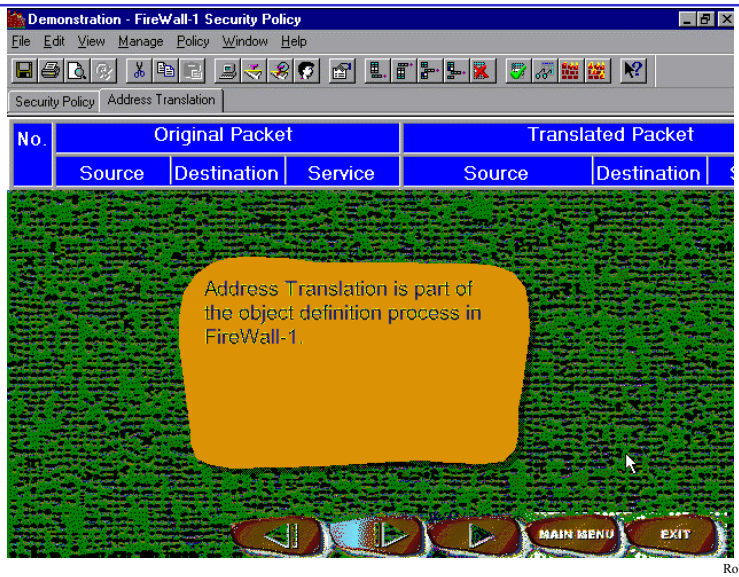
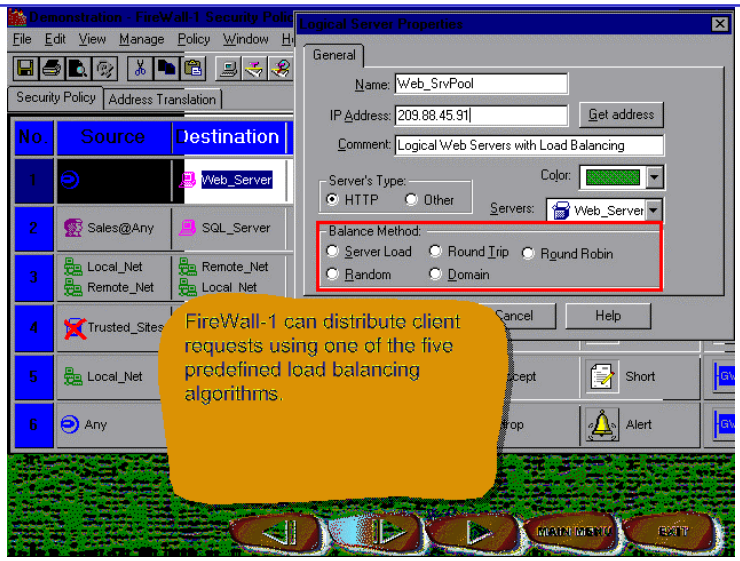



Lámina 40 Roberto Gómez Cárdenas

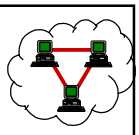
# Balanceo de carga en checkpoint






# Ejemplo bitácoras generadas por checkpoint

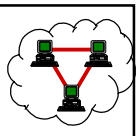
## Ventajas Firewalls Proxy



- Administradores son capaces de monitorear violaciones de políticas de seguridad, a través de los registros generados.
- No son vulnerables a IP Spoofing ya que su conexión NO esta basada en servicio de conexiones físicas.

Lámina 43 Roberto Gómez Cárdenas

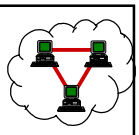
## Desventajas Firewalls Proxy



- Reducción desempeño debido a verificación de peticiones
- Un proxy se debe desarrollar por cada nueva aplicación.

Lámina 44 Roberto Gómez Cárdenas

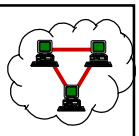
## Socks



- Conjunto herramientas (toolkit) que permite que las aplicaciones sean "proxieadas" sin contar con software proxy específico para cada aplicación.
- Surge como un framework genérico para que los nuevos protocolos de aplicación que vayan surgiendo, pasen de manera segura a través de un firewall.
- La idea es que los proxies específicos para una aplicación tardan en ser implantados.
- Socks permitiría un circuito seguro para cualquier protocolo.

Lámina 45 Roberto Gómez Cárdenas

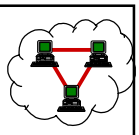
## Carácterísticas socks



- Es un protocolo proxy para ambientes Cliente/Servidor.
- El servidor de socks se encuentra en la capa aplicación.
- El cliente de socks se encuentra entre las capas de aplicación y transporte.

Lámina 46 Roberto Gómez Cárdenas

## Versiones socks



- Existen dos versiones de socks en uso, la versión 4 y la 5.

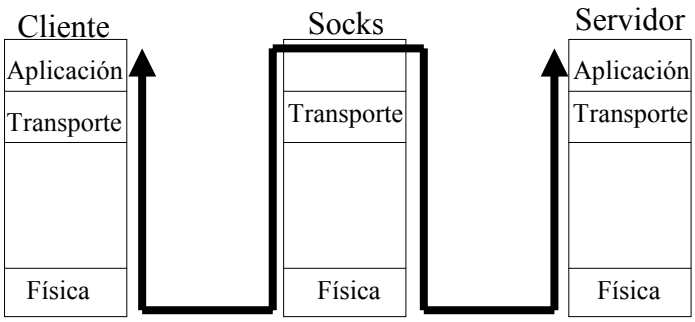
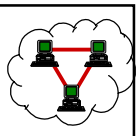



Lámina 47 Roberto Gómez Cárdenas

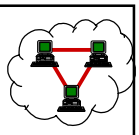
## Funciones socks v4 y v5



- La versión 4 del protocolo de socks realiza 3 funciones:
  - Solicitud de conexión
  - Establecimiento del circuito
  - Y encaminamiento de datos (relay)
- La versión 5 agrega la posibilidad de autentificación. También se le conoce como AFT (Authenticated Firewall Traversal)

Lámina 48 Roberto Gómez Cárdenas

## Esquema funcionamiento socks



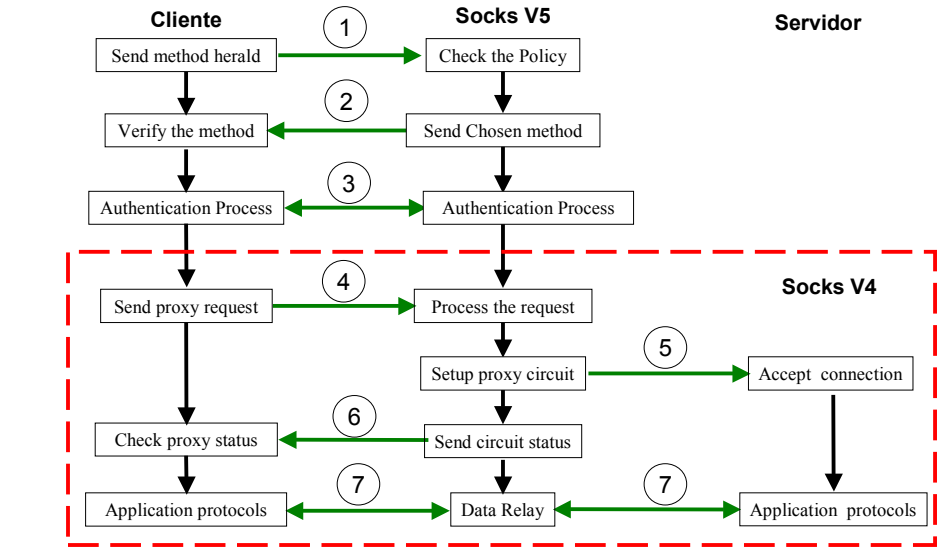
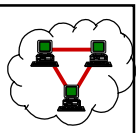



Lámina 49 Roberto Gómez Cárdenas

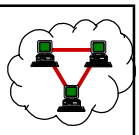
## El lado cliente de socks



- El cliente establece una conexión con el puerto del servidor de socks (generalmente el puerto 1080).
- Si se tiene éxito, se procede a negociar el método de autentificación.
- Si se llega a un acuerdo, se procede a establecer un circuito seguro.

Lámina 50 Roberto Gómez Cárdenas

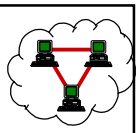
## Arquitecturas firewalls



- ¿Dónde poner el firewall?
  - red privada o afuera
- Se presentan varios esquemas
  - Dual homed host architecture
  - Screened host
  - Screened subnet

Lámina 51 Roberto Gómez Cárdenas

## Dual Homed Host Architecture




No hay tráfico directo entre las redes

Lámina 52 Roberto Gómez Cárdenas

## Screened host

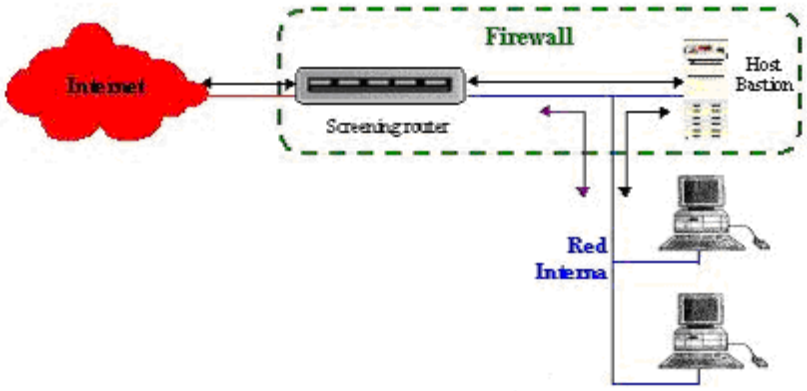



Lámina 53 Roberto Gómez Cárdenas

## Screened subnet

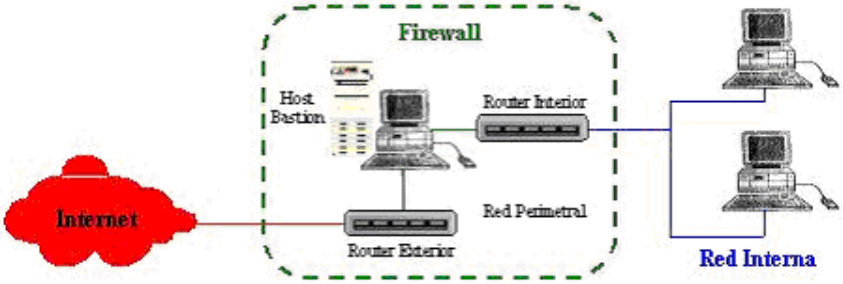
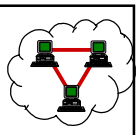



Lámina 54 Roberto Gómez Cárdenas

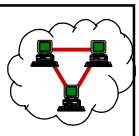
## Firewalls Personales



- Es un producto relativamente nuevo
- Son instalados en computadoras personales de usuarios principiantes y expertos
- Utiles para gente que pasa horas o dias conectada a internet desde su casa
- Posibilidad de que alguien robe información o que use la máquina para atacar a otros

Lámina 55 Roberto Gómez Cárdenas

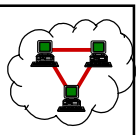
## Ventajas Firewalls Personales



- Proteje el sistema operativo de ataques cuando se conecta a redes hostiles (Internet)
- Si se logro instalar un backdoor, el FP se prevenira acceso al backdoor desde la red
- Cuando se utilizan nuevas aplicaciones se pueden ver las comunicaciones que se llevan a cabo
- Academico: posible darse cuenta los riesgos que existen al conectarse a una red.

Lámina 56 Roberto Gómez Cárdenas

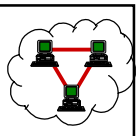
## Firewalls personales



- McAfee Firewall
- PGP7 Firewall
- VirusMD
- BlackICE
- ZoneAlarm
- Norton (equivalente to Symantec Personal Firewall)
- eSafe
- ZoneAlarm Pro
- Sygate
- Tiny
- Conseal

Lámina 57 Roberto Gómez Cárdenas

## Tiny Personal Firewall V.2



- Sitio: http://www.tinysoftware.com
- Requerimientos del sistema:
  - 586 Pentium
  - 16 MB de RAM
  - 1 MB espacio disco
  - Windows 9x / 2000 / NT

Lámina 58 Roberto Gómez Cárdenas

## Elementos Firewall

- Engine
  - es lo primero que debe ejecutarse
  - posible ejecutarlo desde el start-up de Windows
- Utilidad de administración
  - es la interfaz que permite modificar los parámetros del firewall
- Monitor de status
  - permite ver los puertos y otra información asociada con comunicaciones

Lámina 59 Roberto Gómez Cárdenas

## Accediendo a los elementos

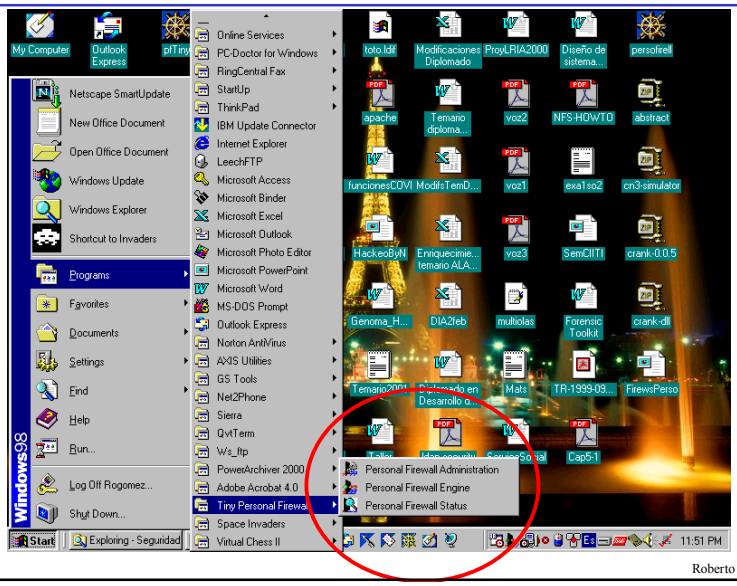
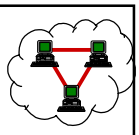



Lámina 60 Roberto Gómez Cárdenas

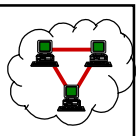
## Estatus Firewall Personal



- Se despliega información de la comunicación entre aplicaciones y el mundo exterior.
- Cuenta con 10 columnas de información
  - aplicación
  - protocolo
  - dirección local
  - dirección remota
  - estado
  - -- tiempo creación
  - -- Rx (Bytes)
  - -- Rx Speed (kB/s)
  - -- Tx (Bytes)
  - -- Tx Speed (kB/s)

Lámina 61 Roberto Gómez Cárdenas

## Ejemplo



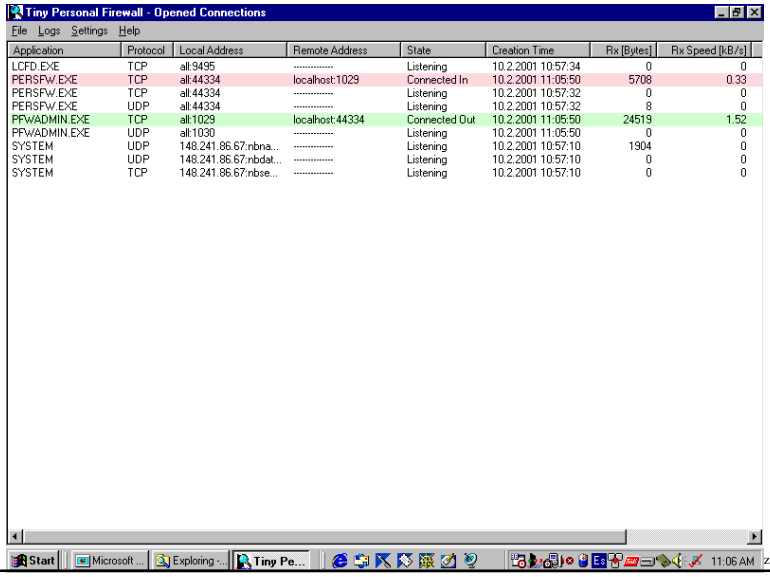
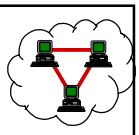



Lámina 62 z Cárdenas

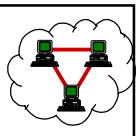
## Administración Remota



- Permite configuración remota
- Lo anterior debe activarse de la pantalla miscellaneous en la ventana principal
- Adicionalmente es posible ver el estado de la red y logs remotamente

Lámina 63 Roberto Gómez Cárdenas

## Seguridad del Firewall



- Grupo direcciones confiables
- Usuarios LAN
- Firmas MD5
- Niveles seguridad
  - Seguridad minima
  - Seguridad mediana
  - Maxima seguridad

Lámina 64 Roberto Gómez Cárdenas

## Primer ejemplo alarma

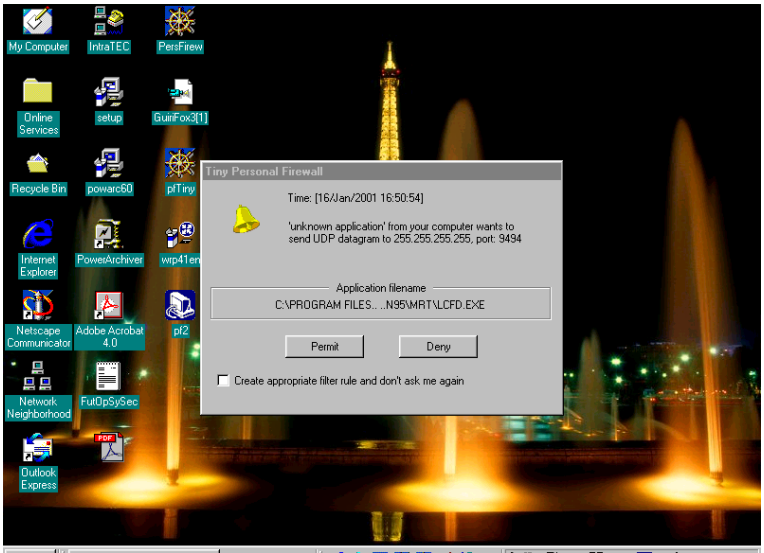
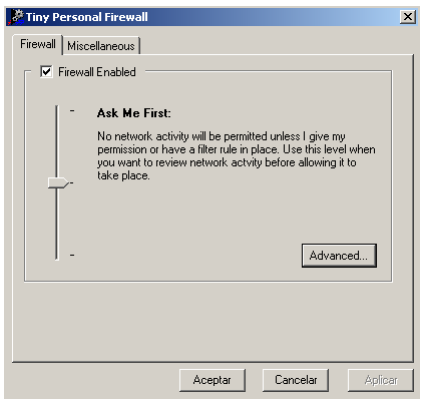



Lámina 65 z Cárdenas

## La administración local



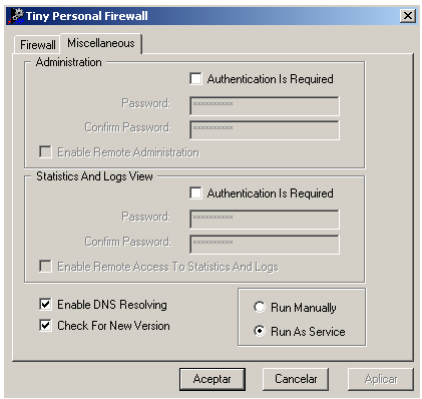




Lámina 66 Roberto Gómez Cárdenas

# Ejemplo reglas filtrado

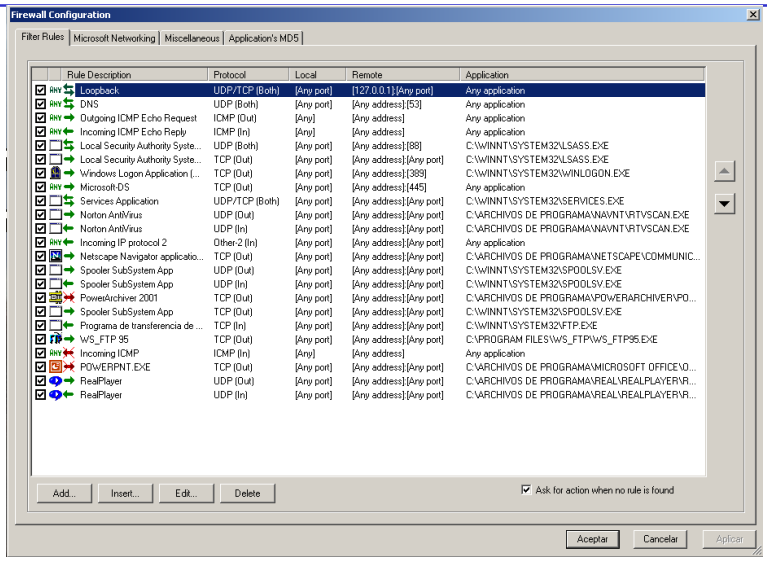
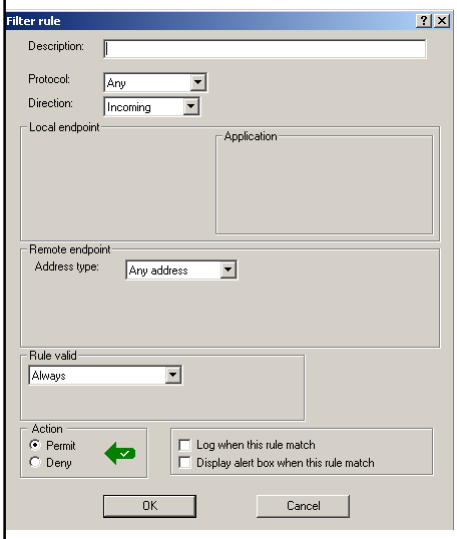



Lámina 67 Roberto Gómez Cárdenas

# Definiendo una regla



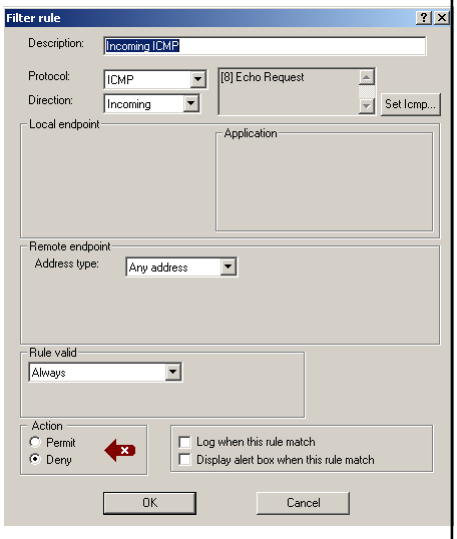




Lámina 68 Roberto Gómez Cárdenas

## Otras características

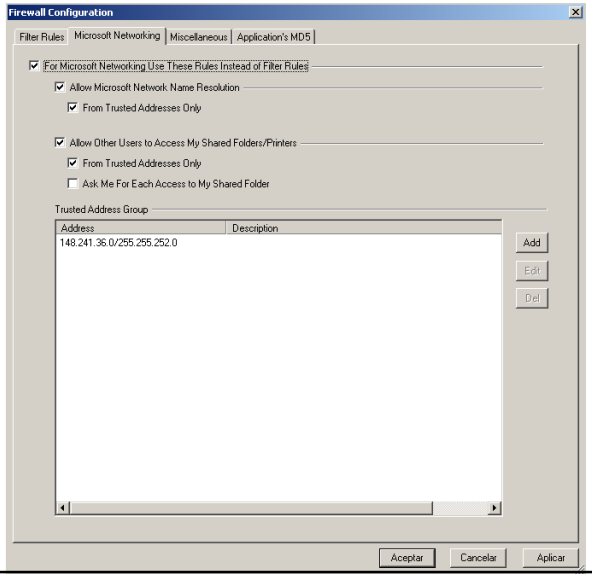



Lámina 69 Roberto Gómez Cárdenas

## Bitácoras en Tiny

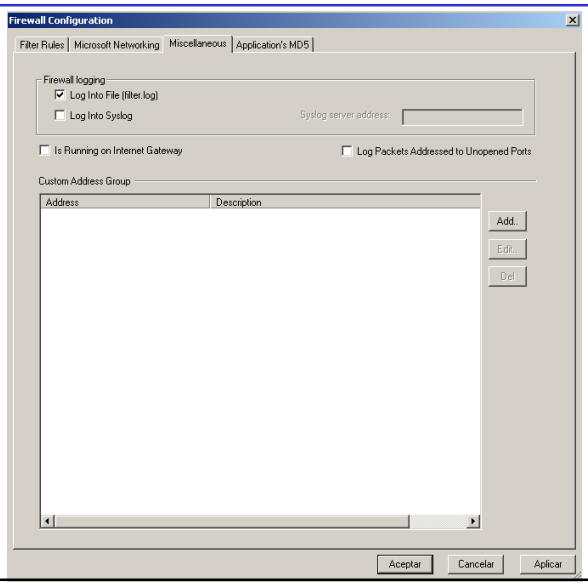



Lámina 70 Roberto Gómez Cárdenas

# Integridad aplicaciones

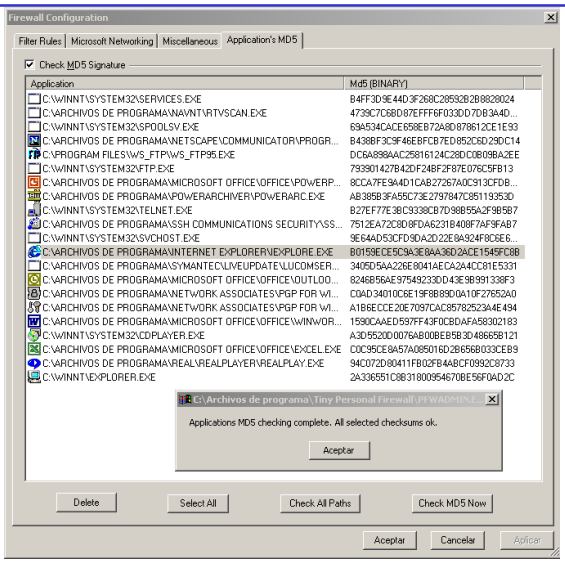
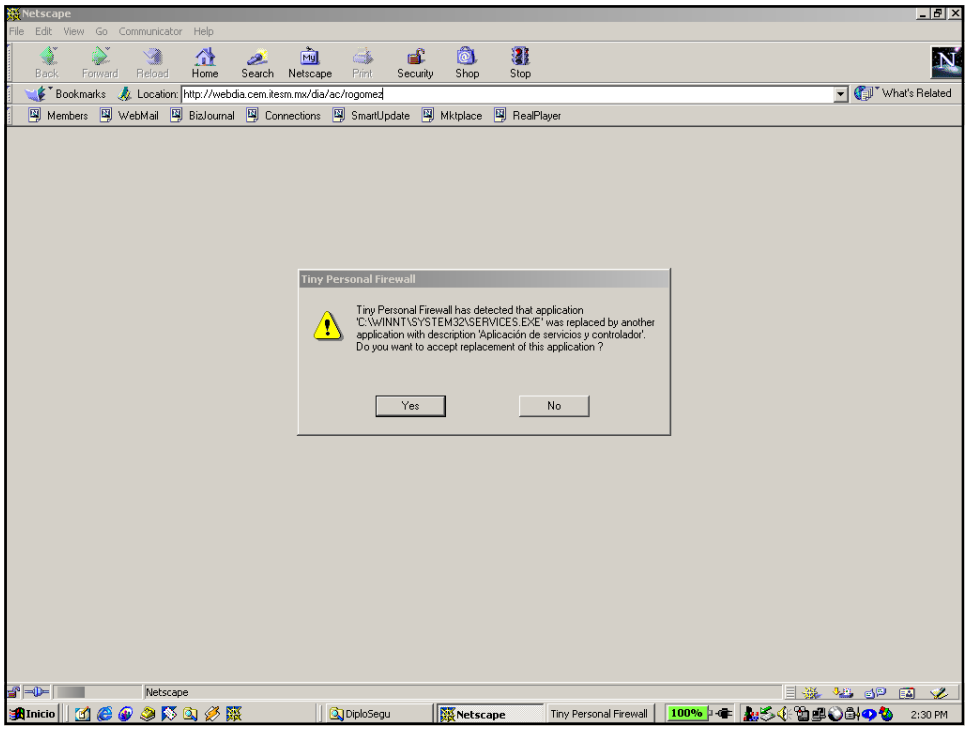



Lámina 71 Roberto Gómez Cárdenas



## Ejemplo alarma

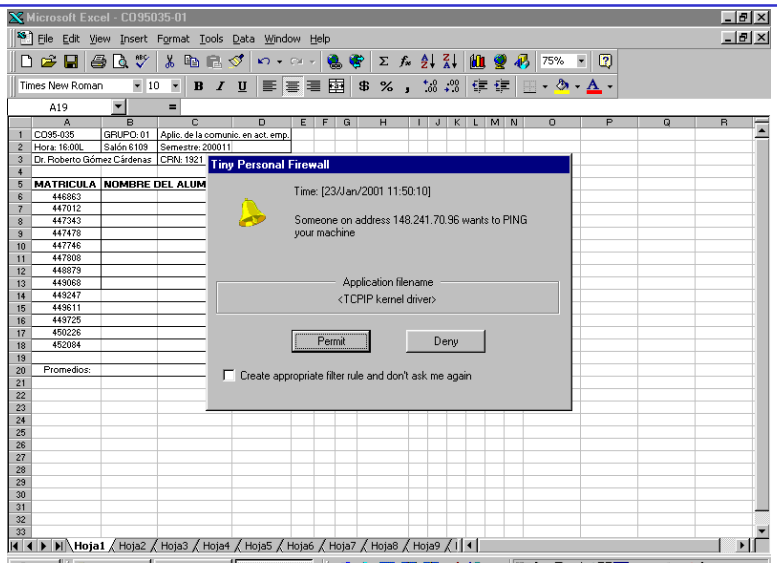


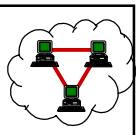

Lámina 73 z Cárdenas

## Las VPNs

Redes Privadas Virtuales

Lámina 74 Roberto Gómez Cárdenas

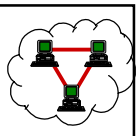
## Redes Virtuales Privadas: VPN



- Conexión establecida sobre una infraestructura pública o compartida
  - uso tecnologías encripción o autenticación para asegurar su payload
- Se crea un segmento "virtual" entre cualesquiera dos entidades que tengan acceso.
- Puede darse a través de infraestructura compartida, LAN, WAN o el internet
- Tecnología barata y efectiva para una solución de red remota que cualquiera con Internet puede aprovechar.

Lámina 75 Roberto Gómez Cárdenas

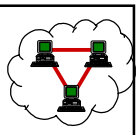
## Categorías VPN



- VPN puede clasificarse en tres configuraciones básicas
  - host to host
  - host to gateway
  - gateway to gateway
- Los escenarios anteriores pueden ser usados con una VPN que atraviesa internet
- VPNs host-to-host son muy usadas como un medio de comunicación privada en segmentos de red locales.

Lámina 76 Roberto Gómez Cárdenas

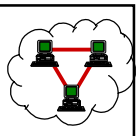
## Metodología VPN básica



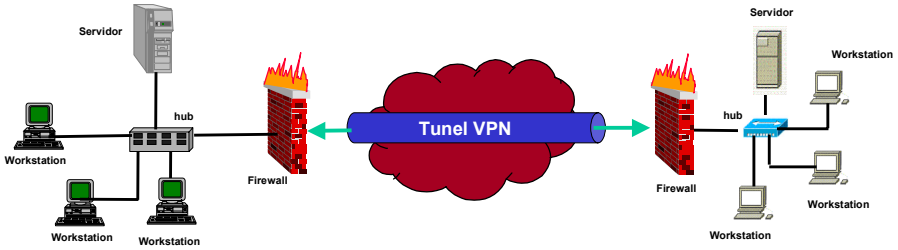
- Concepto básico
  - asegurar canal comunicación con encripción
- Comunicación puede asegurarse a diferentes capas:
  - aplicación (PGP o SSH)
    - varios programas trabajan de host a host
    - solo protegen el payload del paquete y no el paquete
  - transporte (SSL)
    - contenido comunicación es protegido, pero paquetes no
  - red (IPSec)
    - no solo encripta el payload sino la información TCP/IP
    - posible si dispositivos usan encapsulación
  - enlace de datos: Layer 2 Tunneling Protocol (L2TP)
    - encripción paquetes sobre PPP

Lámina 77 Roberto Gómez Cárdenas

## Concepto: tuneleo



- Tuneleo (tunneling)
  - proceso de encapsular un tipo de paquete dentro de otro para facilitar el transporte de este.

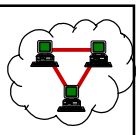



- Ejemplo

```
00:05:18.671517 192.168.44.129 > 172.16.1.128 AH(spi=580532459, seq=0x3):
1232 > 80: P 1:260(259) ack 1 win 17520 (DF)
```

Lámina 78 Roberto Gómez Cárdenas

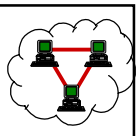
## Ventajas/desventajas VPN



- Beneficios de VPN
  - Seguridad
  - Ventajas de implementación
  - Costos
- Desventajas de VPN
  - overhead en el procesamiento
  - overhead en los paquetes
  - aspectos de implementación
  - aspectos de control y manejo de errores
  - aspectos de disponibilidad internet

Lámina 79 Roberto Gómez Cárdenas

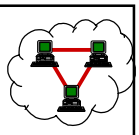
## IPSec



- Este protocolo desarrollado por el grupo de trabajo de seguridad del IETF (Internet Engineering Task Force).
- Surgió a partir del desarrollo de IPv6.
- Empezó siendo una extensión del encabezado en Ipv6
  - debido a que cubría las necesidades de un gran número de clientes, se decidió implantar en parte para Ipv4.
- Consiste de varios protocolos
  - IPSec Protocol Suite
- RFC 2401-2412

Lámina 80 Roberto Gómez Cárdenas

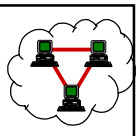
## Objetivos IPSec



- Soportar los protocolos IP existentes (IPv4, IPv6)
- Incremento pequeño en el tamaño de las tramas
- Permitir implantación progresiva en Internet
- Permitir el establecimiento de túneles
- Ofrecer los siguientes servicios
  - Integridad de los contenidos
  - Confidencialidad de los contenidos
  - Autentificación de los participantes

Lámina 81 Roberto Gómez Cárdenas

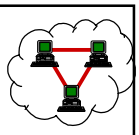
## Modos Operación



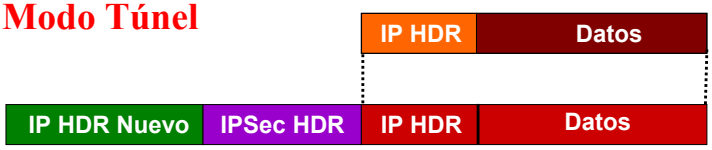
- Modo Transporte
  - Para comunicación punto a punto entre hosts
  - Modo normal de utilización
  - Confidencialidad total de la comunicación
- Modo Túnel
  - Para comunicación punto a punto entre gateways
  - Para introducción de IPSec en redes IPv4 normales
  - Confidencialidad de la comunicación sólo en el túnel
  - Para creación de islas IPSec en VPNs

Lámina 82 Roberto Gómez Cárdenas

## Comparando modos



- **Modo Túnel**




- **Modo Transporte**

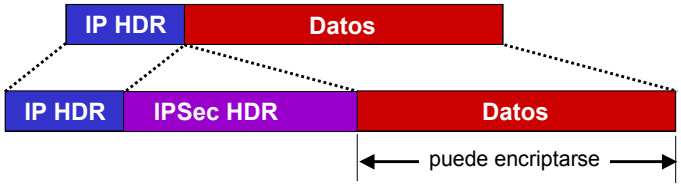
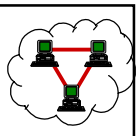



Lámina 83 Roberto Gómez Cárdenas

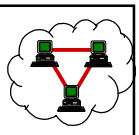
## Security Association



- Se trata de un acuerdo entre dos entidades acerca de cómo se transmitirá información de forma segura.
  - conexión lógica unidireccional entre dos sistemas
- IPSec soporta varios protocolos, diferentes modos de comunicación, así como algoritmos de encripción y de hash.
  - todo esto debe negociarse antes de que la comunicación se lleve a cabo
- El resultado de la negociación es una SA
- Cada sesión de comunicación cuenta con dos SA
  - una para cada participante de la comunicación

Lámina 84 Roberto Gómez Cárdenas

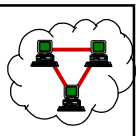
## Base Datos de la SA



- Después de negociar una SA, esta se almacena en una base de datos de SA
- Formadas por una tripleta *<SPI, IP-DA, SP>*
  - Security Parameter Index (SPI)
    - Identificador único de cada SA
  - IP Destination Address (IP-DA)
    - Dirección del receptor (unicast, multicast, broadcast)
  - Security Protocol (SP)
    - El modo de operación (transporte, túnel)
    - El protocolo usado (ESP, AH)
      - Sólo se puede especificar uno de los dos
      - Pueden ser necesarias hasta 4 SAs para una conexión

Lámina 85 Roberto Gómez Cárdenas

## Ejemplo negociación



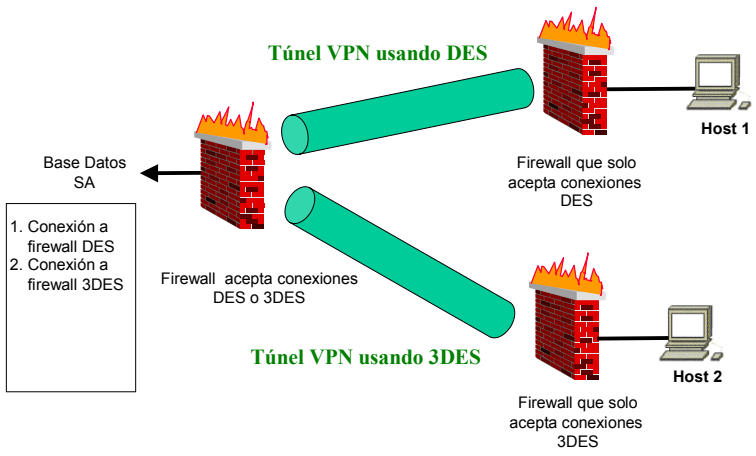
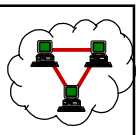



Lámina 86 Roberto Gómez Cárdenas

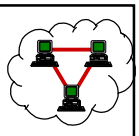
## Protocolos usados



- AH
  - Authentication Header
  - proporciona un servicio de autenticación a nivel paquete
- ESP
  - Encapsulating Security Payload
  - proporcionar encripción más autenticación
- IKE
  - Internet Key Exchange
  - negocia parámetros de conexión, incluyendo llaves para los otros dos protocolos

Lámina 87 Roberto Gómez Cárdenas

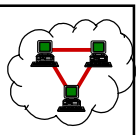
## Protocolo AH



- Proporciona integridad y autentificación
  - opcionalmente protege contra reenvío (replay)
- Añade un encabezado adicional al paquete IP
  - encabezado contiene una firma digital (ICV: integrity check value)
  - garantiza información IP es correcta, pero no se oculta
  - AH usa encabezado IP para calcular la firma digital, dirección fuente es autentica y viene de donde dice
- Soporta números de secuencia para prevenir ataques de tipo replay
  - dispositivos usan números para seguir flujo comunicación
  - atacante no puede re-enviar un paquete capturado para intentar acceder a la VPN

Lámina 88 Roberto Gómez Cárdenas

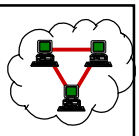
## Autenticación



- Autentica los campos del datagrama, salvo los no mutables de IPv4
  - Type of Service (TOS)
  - Flags
  - Fragment Offset
  - Time to Live (TTL)
  - Header Checksum
- Solo autentica los no mutables en el modo túnel
- Usar información IP para autenticar lo hace incompatible con cambios de encabezado IP (NAT)

Lámina 89 Roberto Gómez Cárdenas

## Encabezado AH en IPV6



- AH es parte del protocolo IPv6, y se consideran datos de extremo a extremo
- Aparece después de las cabeceras de extensión
- Aparece antes o después de las opciones de destino

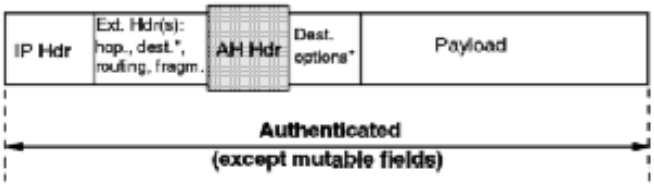
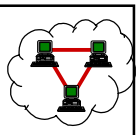



Lámina 90 Roberto Gómez Cárdenas

## Encabezado AH en modo transporte



- La cabecera AH es insertada justo después de la IP
- Si ya hay cabecera IPSec, se inserta justo antes
- Sólo lo usan los hosts (no los gateways)
  - Ventajas: hay poca sobrecarga de procesamiento
  - Desventajas: los campos mutables no van autentificados

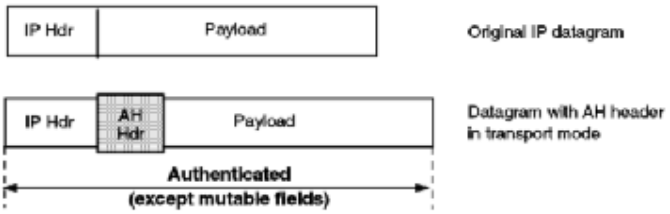
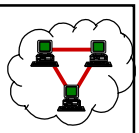



Lámina 91 Roberto Gómez Cárdenas

## Encabezado AH en modo túnel



- El paquete original se encapsula en uno nuevo IP, al que se le aplica AH en modo de transporte
- Se usa si uno de los extremos es un gateway
  - Ventajas: los campos mutables van autentificados, y se pueden usar direcciones IP privadas
  - Desventajas: hay sobrecarga de procesamiento

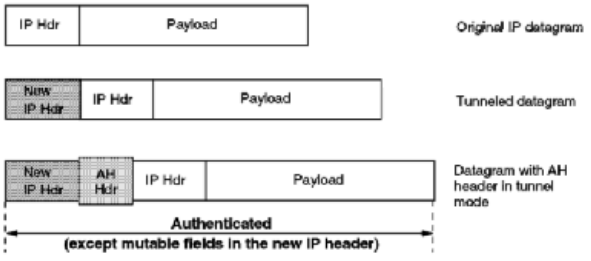
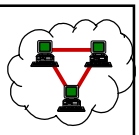



Lámina 92 Roberto Gómez Cárdenas

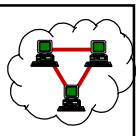
## Protocolo ESP



- Encapsulating Security Payload (ESP)
- Se utiliza para integridad, autentificación, y cifrado
  - Opcionalmente protege contra reenvío
  - Servicios no orientados a conexión
  - Selección opcional de servicios
    - Al menos uno debe de estar activado
- Encripta el payload de los paquetes IP
- Como varios protocolos IPSec es modular
  - usa diferentes algoritmos encripción DES, 3DES e IDEA
- Trabaja diferente, dependiendo del modo usado

Lámina 93 Roberto Gómez Cárdenas

## ESP en IPV6



- ESP es parte del protocolo IPv6, y se consideran datos de extremo a extremo
- Aparece después de los encabezados de extensión
- Aparece antes o después de las opciones de destino

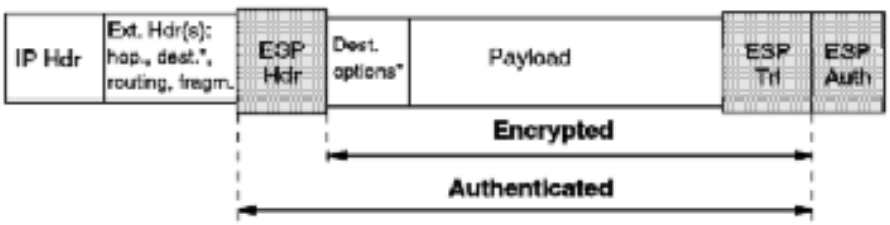
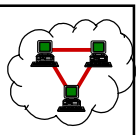



Lámina 94 Roberto Gómez Cárdenas

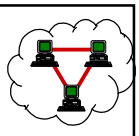
## ESP en modo transporte



- Encabezado ESP es insertado justo después de la IP
  - encripta el resto de la información del paquete, de capa 4 para arriba
- Si se especifica servicio de autenticación durante la negociación
  - se añade información del ICV para autenticación e integridad de del paquete
  - contrariamente al protocolo AH el ICV de ESP no es calculado con información del encabezado IP
- Sólo lo usan los hosts (no los gateways)

Lámina 95 Roberto Gómez Cárdenas

## Ventajas y desventajas ESP en modo transporte



- Ventajas: hay poca sobrecarga de procesamiento
- Desventajas: ni se autentifica ni se cifra el encabezado IP

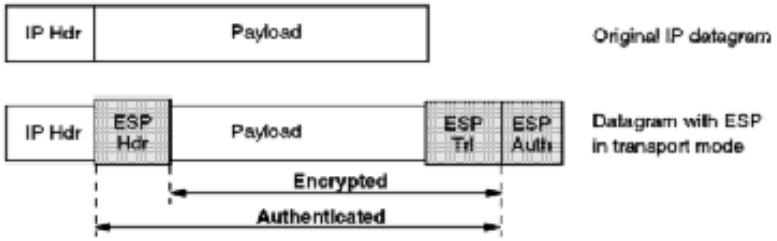
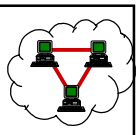



Lámina 96 Roberto Gómez Cárdenas

## ESP en modo túnel



- El paquete original se encapsula en uno nuevo IP, al que se le aplica ESP en modo de transporte
- Se usa si uno de los extremos es un gateway
  - Ventajas: los encabezados IP van encriptados, y se pueden usar direcciones IP privadas
  - Desventajas: hay sobrecarga de procesamiento

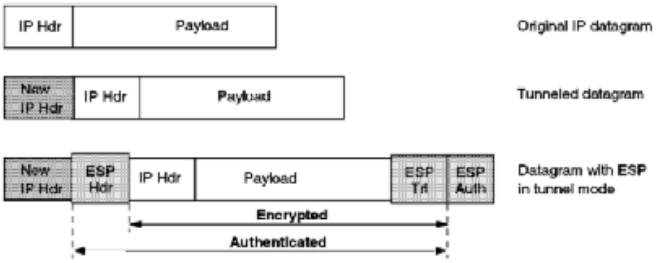
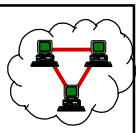



Lámina 97 Roberto Gómez Cárdenas

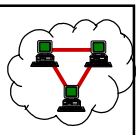
## ¿Porqué dos encabezados/protocolos?



- ESP requiere criptografía fuerte, se use o no, mientras que AH sólo requiere hashing
  - la criptografía está regulada en muchos países
  - la firma no suele estar regulada
- Si sólo se requiere autentificación, AH es mejor
  - formato más simple
  - menor tiempo de procesamiento
- Al tener dos protocolos se tiene un mejor control sobre la red IPSec, así como opciones flexibles

Lámina 98 Roberto Gómez Cárdenas

## Combinando AH/ESP



- Si se requiere autenticación de direcciones (AH) y confidencialidad (ESP)
  - posible combinar ambos protocolos
- Hay muchas combinaciones posibles, lo normal:
  - AH en modo túnel
  - ESP en modo transporte

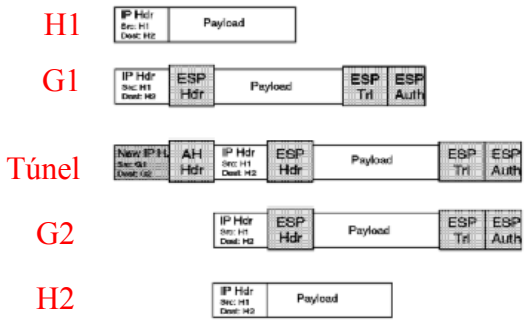
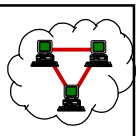



Lámina 99 Roberto Gómez Cárdenas

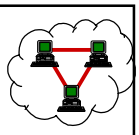
## El protocolo IKE



- Protocolo autenticador y negociador de IPSec
- Verifica que la parte que desea iniciar una comunicación con un dispositivo, este autorizada a hacerlo.
  - después negocia el tipo de encripción a utilizar
- Es la combinación de dos protocolos
  - ISAKMP: Internet Security Association and Key Management Protocol, maneja las negociaciones de seguridad
  - Oakley: variación Diffie Hellman, responsable del intercambio de llaves

Lámina 100 Roberto Gómez Cárdenas

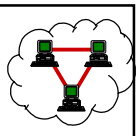
## Las fases de IKE



- IKE se desarrolla con un protocolo en dos fases
- Fase 1
  - Se establece un secreto del cual derivan las claves
  - Se utiliza criptografía asimétrica
    - Para establecer una SA de IKE entre los extremos
    - Para establecer las claves que protejan los mensajes IKE
  - Sólo se ocupa de la protección de la *Fase 2*
- Fase 2
  - Se negocian las SAs y las claves para éstas
  - Se refrescan estas claves cada cierto tiempo
  - Se producen mensajes más frecuentemente

Lámina 101 Roberto Gómez Cárdenas

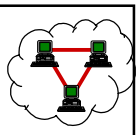
## Tuneles IPSec



- Seguridad de extremo a extremo
- Soporte básico VPN
- Seguridad extremo a extremo con soporte VPN
- Seguridad en acceso remoto

Lámina 102 Roberto Gómez Cárdenas

## Seguridad de extremo a extremo



- Equipos con IPSec
- Sin gateways IPSec
  - Entre H1 y H2, AH/ESP en modo túnel o transporte

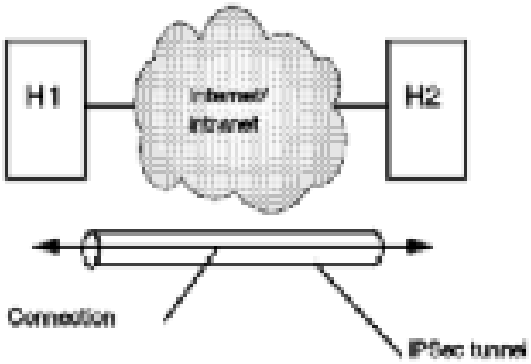
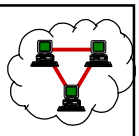



Lámina 103 Roberto Gómez Cárdenas

## Soporte básico VPN



- Equipos sin IPSec
- Gateways con IPSec
  - Entre G1 y G2, AH/ESP en modo túnel o transporte

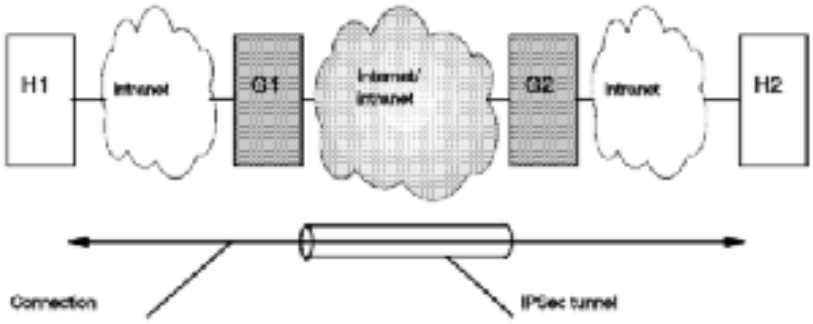
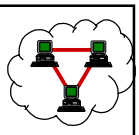



Lámina 104 Roberto Gómez Cárdenas

## Seguridad extremo a extremo con soporte VPN



- Equipos con IPSec
- Gateways con IPSec
  - Entre G1 y G2, AH en modo túnel
  - Entre H1 y H2, ESP en modo transporte

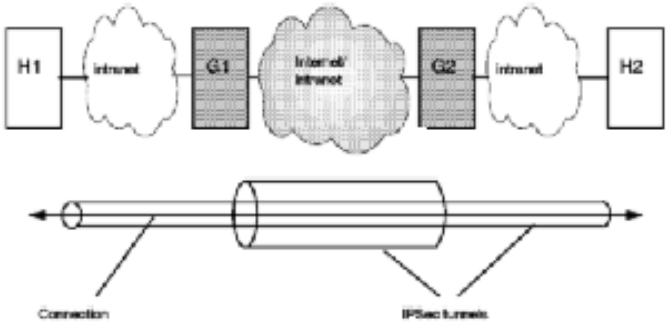
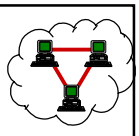



Lámina 105 Roberto Gómez Cárdenas

## Seguridad en acceso remoto



- Equipo remoto con IPSec
- Gateway con IPSec
  - Entre H1 y G2, AH en modo túnel
  - Entre H1 y H2, ESP en modo transporte

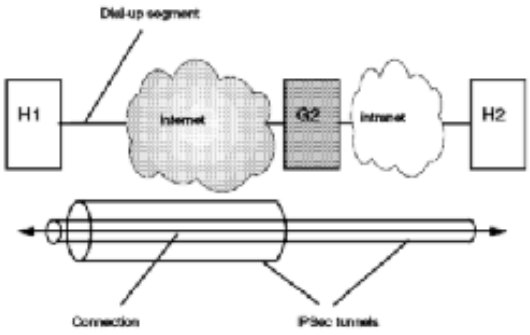
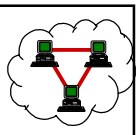


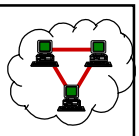

Lámina 106 Roberto Gómez Cárdenas



## Protocolos capa 2

PPTP, L2F y L2TP

Lámina 107 Roberto Gómez Cárdenas

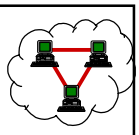


## Protocolo de Túneleo Punto a Punto (Point-to-Point Tunneling Protocol-PPTP)

- Protocolo de red que permite la transferencia de segura de datos de un cliente remoto a un servidor de una empresa
- Crea una VPN a través de una red de datos basada en TCP/IP.
- Extensión del protocolo PPP (RFC 1171)
- Protocolo incluido en Windows NT® Server version 4.0 y Windows NT Workstation versión 4.
- Soporta VPNs usando redes de telefonía switcheada (PSTNs).

Lámina 108 Roberto Gómez Cárdenas

## Características PPTP



- Inicialmente propuesto por Ascend, desarrollado por Microsoft
  - RFC 2637
- Usa encripción de 40 o 128-bit RC4
- Existen implementaciones disponibles de terceros
- Soporte IPX

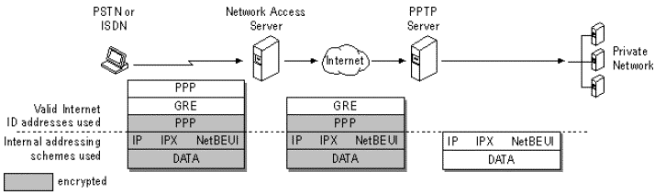
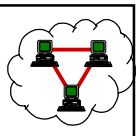



Lámina 109 erto Gómez Cárdenas

## Túneleo de Avance de Capa 2-L2F (Layer 2 Forwarding)



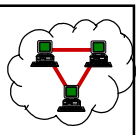
- Desarrollado por Cisco
- Referencia: RFC 2341
- Autenticación de la dirección
- Utiliza atenticación PPP (PAP, CHAP) también soporta RADIUS y TACACS+
- No provee encripción de los datos
- Implementaciones de Cisco, Shiva, Nortel

| Media | L2F | PPP | PPP Payload |
|---|---|---|---|

Encapsulación del Paquete L2F

Lámina 110 Roberto Gómez Cárdenas

## Layer Two Tunneling Protocol L2TP



- Extensión del Point-to-Point Tunneling Protocol (PPTP) usado por un ISP para habilitar la operación de una a VPN sobre Internet.
- Referencia: RFC 2661
- Combina lo mejor de dos protocolos de tuneleo
  - PPTP de Microsoft y
  - L2F de Cisco Systems

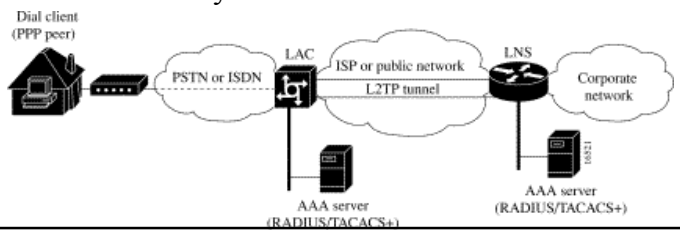
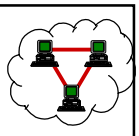



Lámina 111 Roberto Gómez Cárdenas

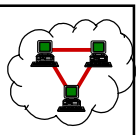


## Protocolos capa aplicación

SSL y SSH

Lámina 112 Roberto Gómez Cárdenas

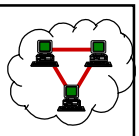
## Secure Sockets Layer



- Es una propuesta de estándar para encriptado y autenticación en el Web.
  - diseñado en 1993 por Netscape
- Es un esquema de encriptado de bajo nivel usado para encriptar transacciones en protocolos de nivel aplicación como HTTP, FTP, etc.
- Con SSL puede autentificarse un servidor con respecto a su cliente y viceversa.

Lámina 113 Roberto Gómez Cárdenas

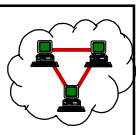
## Características de SSL



- Se basa en un esquema de llave pública para el intercambio de llaves de sesión.
- Las llaves de sesión son usadas para encriptar las transacciones sobre HTTP.
- Cada transacción usa una llave de sesión. Esto dificulta al “cracker” el comprometer toda una sesión.

Lámina 114 Roberto Gómez Cárdenas

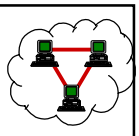
## Objetivos de SSL



- Seguridad criptográfica.
  - Se sugiere el uso de SSL para establecer conexiones seguras entre dos partes.
- Interoperabilidad
  - Programadores deben poder desarrollar aplicaciones basadas en SSL, que intercambien parámetros criptográficos sin tener conocimiento de los códigos de los programas de cada uno.
- Extensibilidad.
  - SSL provee un marco donde pueden incorporarse métodos criptográficos según se necesite.

Lámina 115 Roberto Gómez Cárdenas

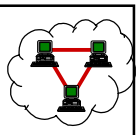
## Objetivos de SSL



- Eficiencia relativa.
  - Puesto que las operaciones criptográficas demandan demasiado CPU, el protocolo SSL incorpora un esquema opcional de “caching”, que reduce el número de conexiones que deben establecerse desde inicio.
  - Además se ha tomado en cuenta el reducir en lo posible la actividad de la red.

Lámina 116 Roberto Gómez Cárdenas

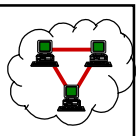
## Protocolo SSL



- El estándar de IETF “Transport Layer Security” (TLS) se basa en SSL.
- Ha pasado por varias versiones
  - las más comunes son las versiones 2 y 3
  - problemas criptográficos conocidos en versión 2, solucionados en la versión 3
- Requiere un transporte confiable.
- Provee seguridad en el canal:
  - Privacía. Se usa un criptosistema simétrico (DES, RC4)
  - Autenticación. Se usa un criptosistema asimétrico (RSA)
  - Integridad:Se usan funciones hash (MD2, MD4, MD5)

Lámina 117 Roberto Gómez Cárdenas

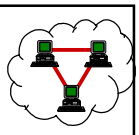
## Protocolos de SSL



- Existen dos subprotocolos
  - SSL record protocol
  - SSL handshake protocol

Lámina 118 Roberto Gómez Cárdenas

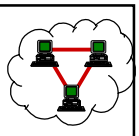
## SSL record protocol



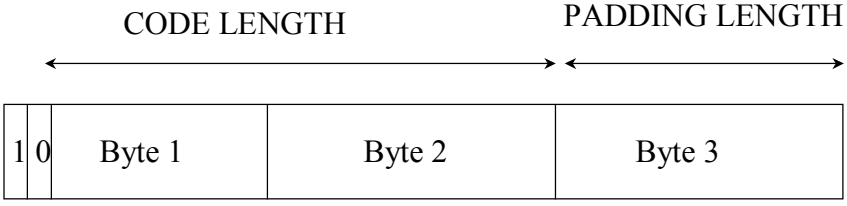
- Construido arriba de un servicio orientado conexión confiable
  - por ejemplo: TCP
- Define los formatos de los mensajes empleados en SSL.
- Proporciona compresión de datos, chequeo de integridad, autenticación del origen del mensaje, encripción y define el tamaño del paquete
  - posible cambiar algoritmo protección durante la comunicación

Lámina 119 Roberto Gómez Cárdenas

## Record Header Format



Está compuesto de 2 o 3 bytes

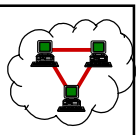



Con 0 indica que se están enviando datos
Con 1 se trata de un byte reservado

Si 1 indica que el byte 3 es necesario.
Es decir, se requiere un padding

Lámina 120 Roberto Gómez Cárdenas

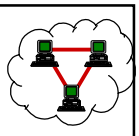
## Record Data Format



- MAC DATA. Message Authentication Code
  - Calculado a partir de diferentes datos:
    - Un secreto, p.e. un password
    - El campo ACTUAL DATA
    - El campo PADDING DATA
    - Un número de secuencia (SEQUENCE NUMBER)
- ACTUAL DATA.
  - Contiene los datos a enviar
- PADDING DATA.
  - Es el PADDING agregado a los datos
- Un número de secuencia

Lámina 121 Roberto Gómez Cárdenas

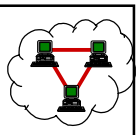
## SSL handshake protocol

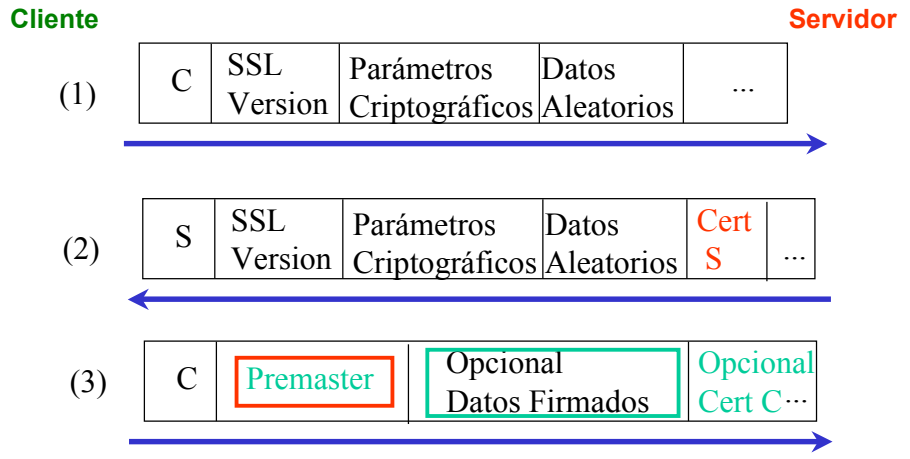


- Autentifica al servidor para el cliente.
- Permite al cliente y servidor seleccionar algoritmos criptográficos, que sean soportados por ambos.
- Opcionalmente autentifica al cliente para el servidor.
- Usa criptografía de llave pública para generar secretos compartidos.
- Establece una conexión SSL encriptada.

Lámina 122 Roberto Gómez Cárdenas

## Pasos del protocolo handshake

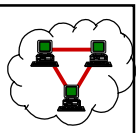





El cliente autentifica al servidor basándose en Cert S
Si falla error
Crea el secreto "Premaster"

Lámina 123 Roberto Gómez Cárdenas

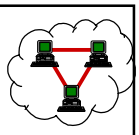
## El protocolo SSH



- Desarrollado por Communications Security Ltd.
- Es un programa (protocolo) para acceder a otra computadora a través de una red, ejecutar comandos a una maquina remota y mover archivos de una computadora a otra.
- Provee una fuerte autenticación y comunicaciones seguras por medio de encripción sobre canales inseguros.
- Es un sustituto para el telnet, ftp, rlogin, rsh, rcp y rdist.

Lámina 124 Roberto Gómez Cárdenas

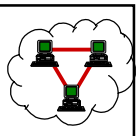
## El nombre SSH



- Existe confusión acerca nombre ssh
- Originalmente existía un programa llamado ssh
  - con el tiempo otras entidades han crecido
- Existe un paquete, que incluye programa ssh y otros, el cual es usualmente llamado ssh
- Existe un protocolo de comunicaciones sobre el que el programa ssh (y otros) esta basado
  - usualmente llamado ssh
- Compañía llamada SSH Communications Security
  - cuenta con otros productos que usan el nombre

Lámina 125 Roberto Gómez Cárdenas

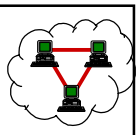
## Versiones SSH



- Existen dos versiones: SSH v1 y SSH v2.
- Son dos protocolos totalmente diferentes.
- SSH1 y SSH2 encriptan los paquetes en diferentes partes
  - SSH1 usa llaves de servidor y cliente para autenticar sistemas, en cambio SSH2 solo usa llaves de host.
- SSH2 es una completa reescritura del protocolo y no usa la misma implementación de red que usa SSH1.
  - se le considea mas seguro.
- Debido a la diferente implementación ambos protocolos son incompatibles.

Lámina 126 Roberto Gómez Cárdenas

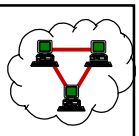
## Diferencias SSH v1 y SSH v2



- SSH 1 es la versión original.
- SSH 2 incluye nuevas características
  - soporte protocolo TLS
- SSH 1 es distribuido con todo y código
  - licencia permite obtenerlo gratis para usos no-comerciales
- SSH 2 fue desarrollado por SSH Comm. Security
  - se vende comercialmente, aunque esta disponible para diferentes usos
- Varios programas basados en los protocolos SSH son desarrollados por otra gente.

Lámina 127 Roberto Gómez Cárdenas

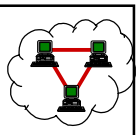
## Autenticación servidor



- No se basa en nombre servicio o direcciones IP
- En ambas versiones, criptografia llave pública es usada para probar identidad servidor.
- Primera parte verifica que cliente posee un llave pública correcta del servidor a conectarse.
  - Problema durante desarrollo V1: no existía estándar global para distribuir y verificar llaves públicas
  - SSH V2: puede usar autoridades certificadoras para verificar una llave pública (en base a TLS)
  - SSH V2 también soporta mecanismo desarrollado para V1

Lámina 128 Roberto Gómez Cárdenas

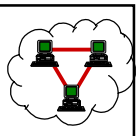
## Solución versión 1



- Cliente retira llave pública del mismo servidor.
- Verifica si conoce una llave para un servidor con el mismo nombre.
  - si no coinciden se imprime una alerta
- Si el cliente no tiene almacenada una llave
  - imprime una alerta y
  - opcionalmente almacena la llave para la proxima vez que se conecte al servidor
- Solución pone al cliente vulnerable a un servidor hostil en la primera conexión
  - más seguridad que tener cliente vulnerable a un servidor hostil en cada conexión

Lámina 129 Roberto Gómez Cárdenas

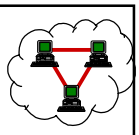
## Continuación de la autenticación servidor



- Posible contar con un sistema local de base de datos de las llaves de los servidores a los que los usuarios se quieran conectar.
  - SSH V2 no siempre usa algoritmos llave pública para esto
- Después verificar validez una llave, SSH verifica identidad del servidor enviando un mensaje encriptado con la llave pública.
- Cuando servidor prueba que decriptó con éxito el mensaje, conoce la parte secreta de la llave, el cliente comprueba que esta hablando con el servidor correcto

Lámina 130 Roberto Gómez Cárdenas

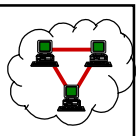
## Autenticación usuario



- Puede ser autenticado de diferentes formas
- Dialogo dirigido por el cliente
  - envía peticiones al servidor.
- Primera petición:
  - siempre solicita al usuario su login name.
- Servidor responde peticiones: un éxito o falla.
- Los métodos soportados actualmente son:
  - autenticación de password tradicional
  - combinación de autenticación .rhost con RSA basada en host
  - autenticación RSA pura
  - autenticación kerberos V5 y autenciación servidor TIS
  - se incluye soporte para otros métodos

Lámina 131 Roberto Gómez Cárdenas

## Diagrama autenticación host



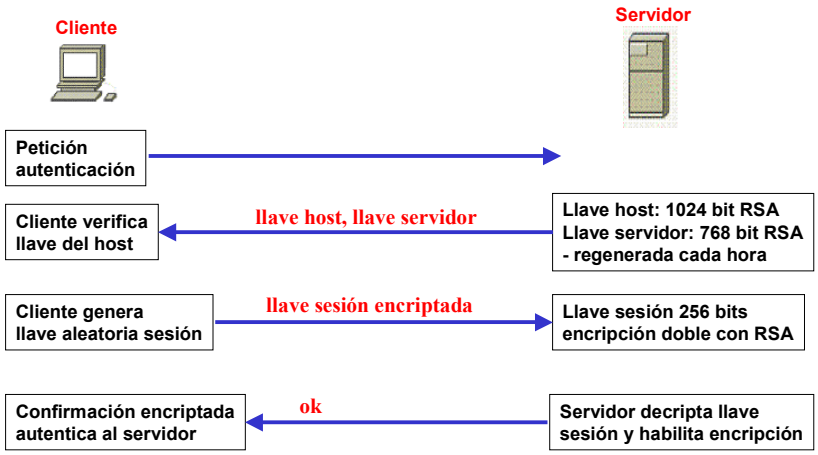
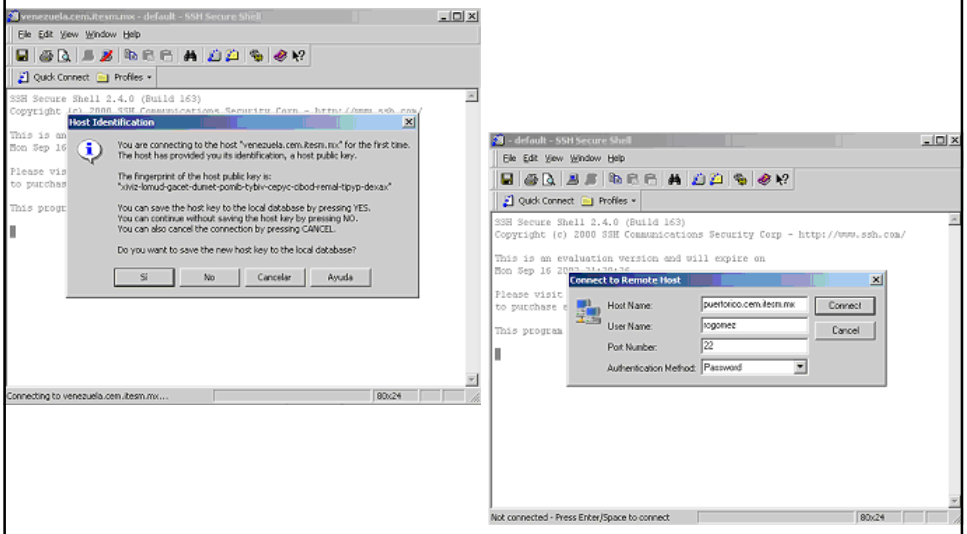


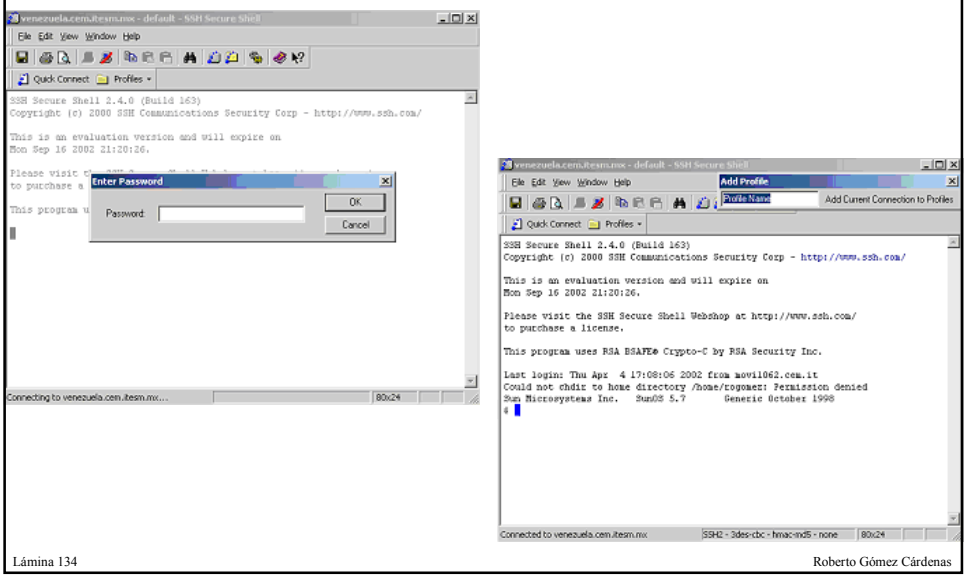

Lámina 132 Roberto Gómez Cárdenas

# Ejemplo SSH (1/2)

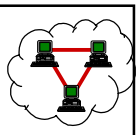





# Ejemplo SSH (2/2)

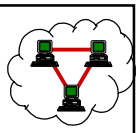


## SSH vs SSL



- La capa en la que actúan
  - SSH: aplicación
  - SSL: transporte
- El método de autenticación
  - SSH: llaves
  - SSL: certificados

Lámina 135 Roberto Gómez Cárdenas

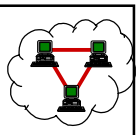


## Traductores Direcciones de Red

NAT y PAT

Lámina 136 Roberto Gómez Cárdenas

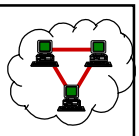
## Traductores de direcciones de red



- NAT: Network Address Translation
- En un principio usado para resolver el problema de direcciones IP disponibles.
  - permite a una compañía usar más direcciones IP internas.
- Proporciona un tipo de bloqueo escondiendo las direcciones IP internas.
- Refuerza el nivel de seguridad dentro de la Red escondiendo su estructura interior.

Lámina 137 Roberto Gómez Cárdenas

## ¿En qué consiste NAT?



- Permite la asignación de una dirección pública, en el "mundo" exterior a un dispositivo que posee una dirección IP privada en el interior.
  - la dirección interna permanece oculta al exterior
- NAT es responsable de "traducir" el tráfico entre el público exterior y el direccionamiento privado.
  - solo el dispositivo NAT conoce la dirección interna del dispositivo

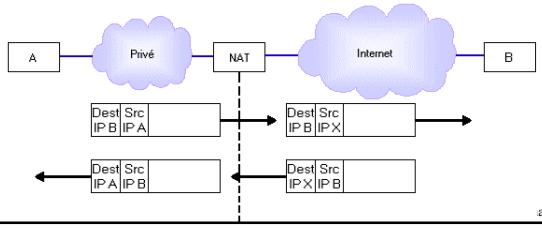
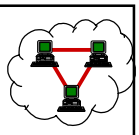



Lámina 138 .as

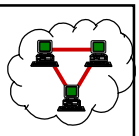
## Direcciones homologadas



- Debido a la gran demanda de direcciones se decide reservar intervalos de direcciones para uso privado (RFC 1918)
- Estas direcciones son
  - 10.0.0.0 a 10.255.255.255 (10/8 prefijo)
  - 172.16.0.0 a 172.31.255.255 (172.16/12 prefijo)
  - 192.168.0.0 a 192.168.255.255 (192.168/16 prefijo)
- Consecuencia
  - estas direcciones no son ruteables en internet y no deben ser utilizadas por las máquinas de esta gran red
  - todas las redes privadas pueden utilizar estas direcciones sin problema

Lámina 139 Roberto Gómez Cárdenas

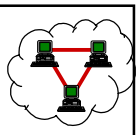
## Técnicas traducción direcciones



- Traducción de direcciones estaticas
  - se tienen el mismo numero de direcciones en la red a traducir que las disponibles
- Traducción de direcciones dinámicas
  - el numero de direcciones disponibles es menor a las que se tienen
  - se crea una “piscina” de direcciones disponibles
  - no es forzoso contar con un mapeo uno a uno de las direcciones de la piscina con las internas
  - cuando todas las direcciones de la piscina estan usadas y se tiene un petición de conexión del mundo exterior, se usa una variante de NAT llamada overloading o PAT

Lámina 140 Roberto Gómez Cárdenas

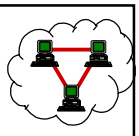
## PAT



- También conocido como NAPT
  - o single address NAT
- Mapea varias direcciones internas en una direccion externa pública, a través de un seguimiento de la sesión de comunicación del puerto usado en esta.
- Ejemplo:
  - host 192.168.1.5 desea contactar servidor web
  - genera puerto "efimero" 1035 y envía petición al ruteador gateway
    - dispositivo OAT
  - ruteador traduce la dirección en una dirección IP pública y asigna un puerto nuevo ( p.e. 1111)

Lámina 141 Roberto Gómez Cárdenas

## PAT

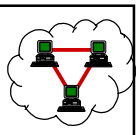


- lo anterior se logra sobre-escribiendo la dirección IP y el número de puerto
- lo anterior, y la dirección IP original de la estación, se almacena en una tabla, como:

| Source ip/part | Translated IP/port | contacted IP/port |
|---|---|---|
| 192.168.1.5.1035 | 200.200.200.2.1111 | 255.255.255.1.80 |

- el dispositivo PAT intenta asignar el mismo número de puerto al exterior que el usado al interior
  - sin embargo si el numero de puerto ya esta siendo usado se asigna uno nuevo
- cuando el tráfico regresa el dispositivo PAT mira a su tabla y traduce

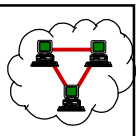
Lámina 142 Roberto Gómez Cárdenas



## Autenticando usuarios externos

Radius y Tacacs

Lámina 143 Roberto Gómez Cárdenas

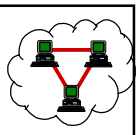


## TACACS y RADIUS

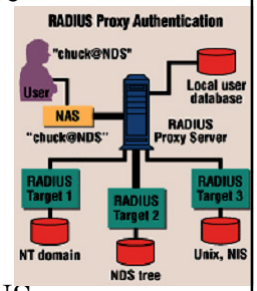
- Sistemas de autenticación y control de acceso a una red vía conexión remota.
- Permiten redireccionar el “username” y “password” hacia un servidor centralizado.
- Este servidor decide el acceso de acuerdo a la base de datos del producto o la tabla de passwords del Sistema Operativo que maneje.

Lámina 144 Roberto Gómez Cárdenas

## Radius



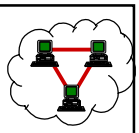
- Remote Authentication Dial-In User Service
- Sistema de autenticación y accounting usado por varios proovedores de internet (ISPs)
- Cuando un usuario se conecta (dial) a su ISP, este debe proporcionar su username y password.
- Esta información se pasa a servidor RADIUS
  - verifica que información es correcta y autoriza el acceso al sistema ISP
- No es un estándar oficial, la especificación la mantiene un grupo del IETF




¡DIAMETER!

Lámina 145 Roberto Gómez Cárdenas

## TACACS



- Terminal Access Controller Access-Control System
- Es la especificación de un protocolo estándar en la industria. RFC 1492.

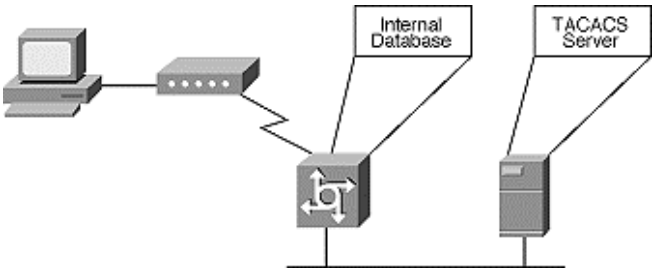
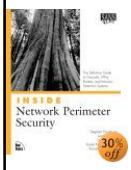



Lámina 146 Roberto Gómez Cárdenas

# Referencias


- Firewalls and Internet Security : Repelling the Wily Hacker by William R. Cheswick, Steven M. Bellovin, 2nd edition (February 15, 2001), Addison-Wesley Pub Co




- Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems by Stephen Northcutt, Karen Fredrick, Scott Winters, Lenny Zeltser, Ronald W Ritchey, New Riders Publishing; 1st edition (June 28, 2002)

Lámina 147 Roberto Gómez Cárdenas