



Seguridad en Redes y Telecomunicaciones

Roberto Gómez Cárdenas
 rogoa@gmail.com
 http://cryptomex.org

Lámina 1 Dr. Roberto Gómez Cárdenas



El efecto domino

- Si una capa es atacada
- La seguridad es tan fuerte como el eslabón más débil
- La capa dos puede ser una capa muy débil.

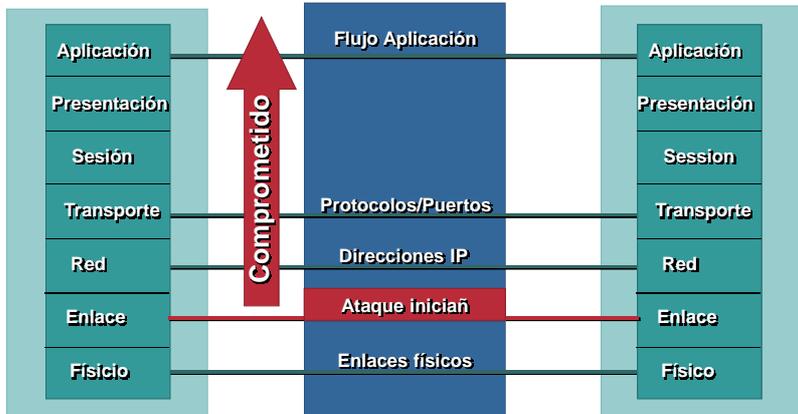


Lámina 2 Dr. Roberto Gómez Cárdenas



Principales ataques a capa 2

- **ARP**
 - Address Resolution Protocol
 - Mapear direcciones IP (capa 3 - 32 bits) hacia direcciones MAC (capa 2 - 48 bits)
 - Protocolo broadcast
- **Ataques**
 - ARP poisoning
 - ARP flooding - saturación del switch con lo cual se puede detener el switcheo de paquetes y convertirlo en un hub)
 - Sniffing/Spoofing (arp spoof - dnsiff)
 - Spanning tree attack
 - VLAN "Hopping" Attacks
- **Wireless (802.11)**
 - también requiere de mecanismos de seguridad a nivel capa 2

Lámina 3

Dr. Roberto Gómez Cárdenas



Sniffers y Analizadores

- Un sniffer es un proceso que "olfatea" el tráfico que se genera en la red *a nivel de enlace*;
 - puede leer toda la información que circule por el tramo de red en el que se encuentre.
 - se pueden capturar claves de acceso, datos que se transmiten, números de secuencia, etc...
- Un analizador de protocolos es un sniffer al que se le ha añadido funcionalidad suficiente como para entender y traducir los protocolos que se están hablando en la red.
 - debe tener suficiente funcionalidad como para entender las tramas de nivel de enlace, y los paquetes que transporten.
- **Diferencia:**
 - normalmente la diferencia entre un sniffer y un analizador de protocolos, es que el segundo está a la venta en las tiendas y no muestra claves de acceso.

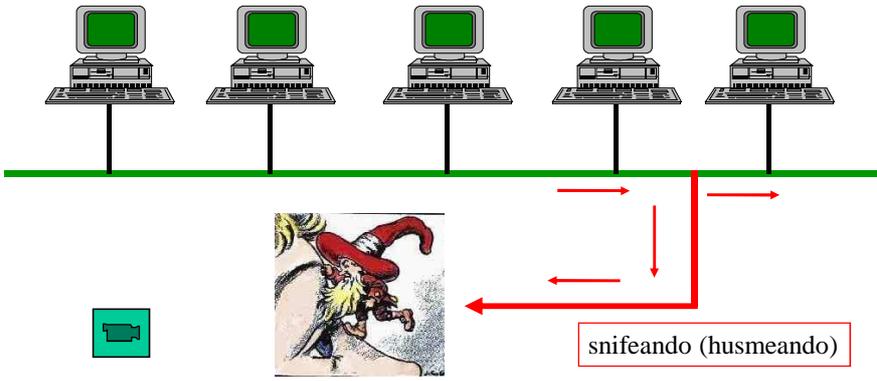
Lámina 4

Dr. Roberto Gómez Cárdenas



Sniffers

¿Cómo se comunican dos computadoras en una red local?



computadora en modo promiscuo

Lámina 5

Dr. Roberto Gómez Cárdenas



¿¿Y las redes switcheadas??



Introducción a los sniffers activos

ettercap

Lámina 6

Dr. Roberto Gómez Cárdenas



Tipos de sniffers

- Pasivos
 - sniffers no realizan actividad alguna
 - solo capturan paquetes
- Activos
 - sniffers intentan apoderarse de las sesiones
 - uso de técnicas para lograr lo anterior
 - spoofing
 - envenenamiento de la tabla de arp

Lámina 7

Dr. Roberto Gómez Cárdenas



Spoofing

- Spoofing es la creación de paquetes de comunicación TCP/IP usando una dirección IP de alguien más.
- Lo anterior permite entrar en un sistema haciéndose pasar por un usuario autorizado.
- Una vez dentro del sistema, el atacante puede servirse de éste como plataforma para introducirse en otro y así sucesivamente.
- Ejemplo
 - hacer un telnet al puerto 25 y enviar correos a nombre de otra persona

Lámina 8

Dr. Roberto Gómez Cárdenas


1er ejemplo spoofing: ataque ARP

- Consiste en hacerse pasar por una máquina que no es.
- Aprovecha el principio de funcionamiento del protocolo ARP.
- Sólo es útil en redes/máquinas que utilizan este protocolo (locales).
- También conocido como envenenamiento de ARP

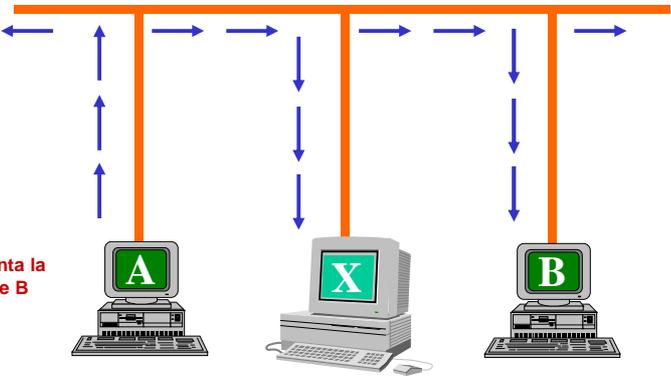


Lámina 9 Dr. Roberto Gómez Cárdenas


Protocolo ARP
 (funcionamiento normal)

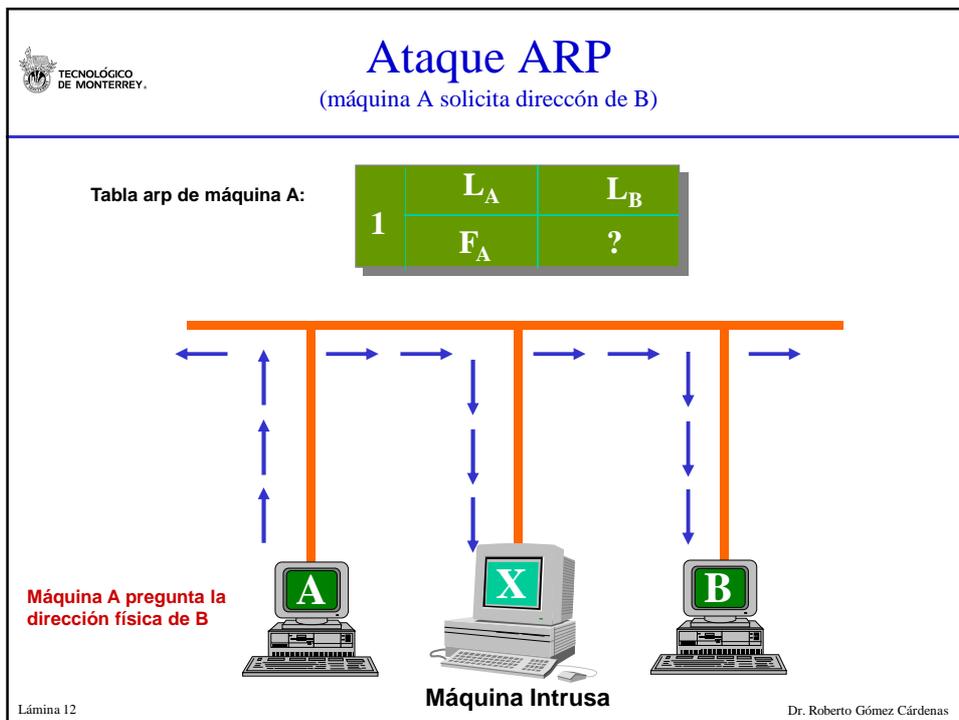
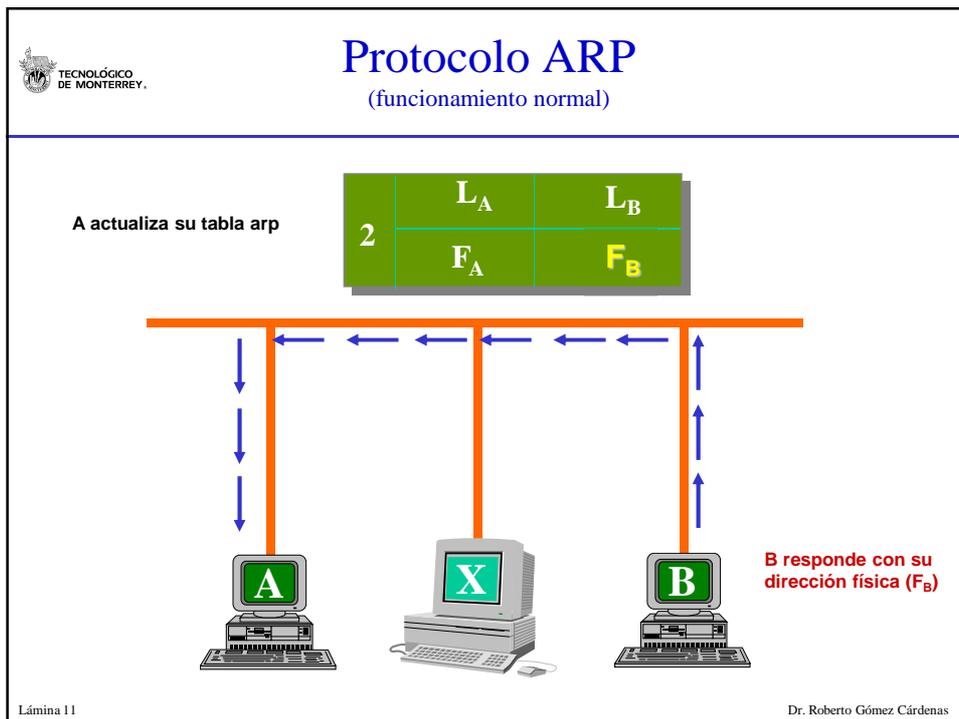
Tabla arp de máquina A:
 L_A : dirección lógica A, F_A dirección física A
 se desconoce la dirección física de B (F_B)

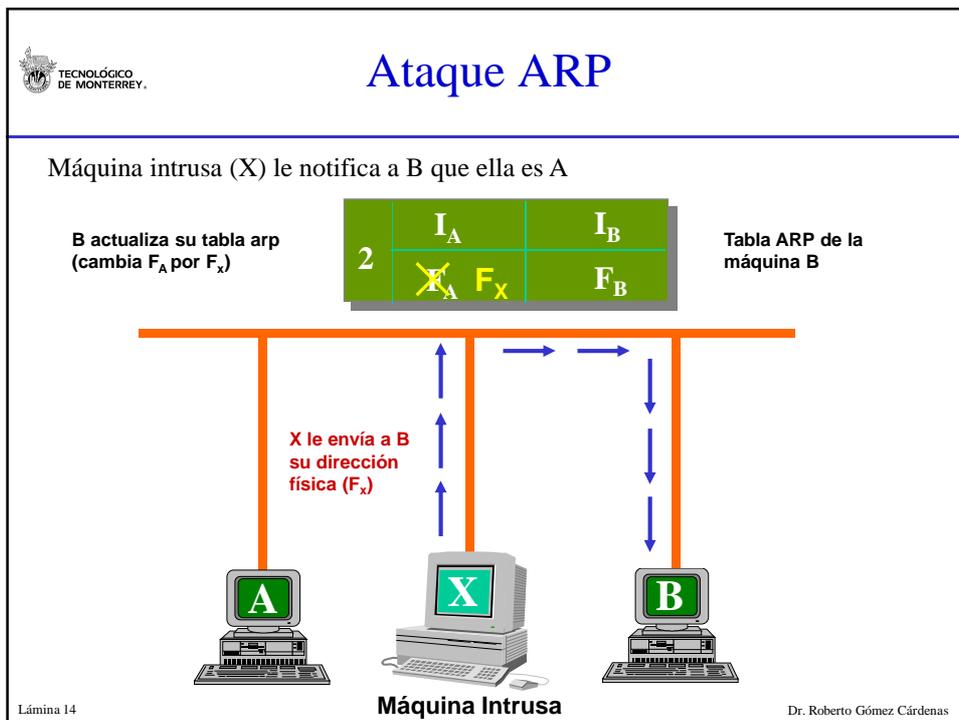
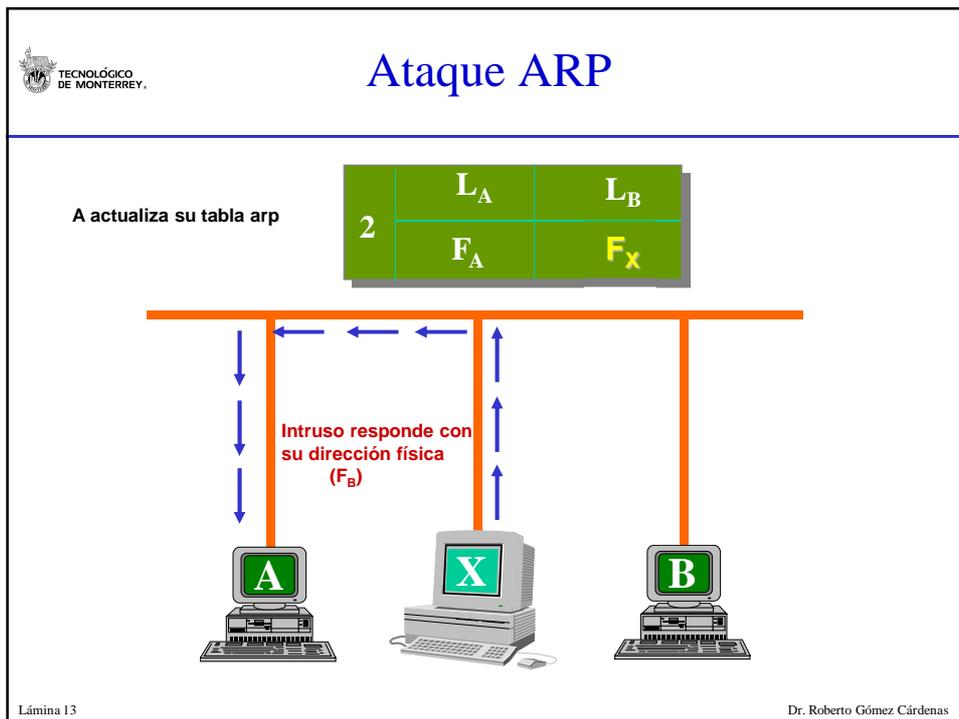
	L_A	L_B
1	F_A	?

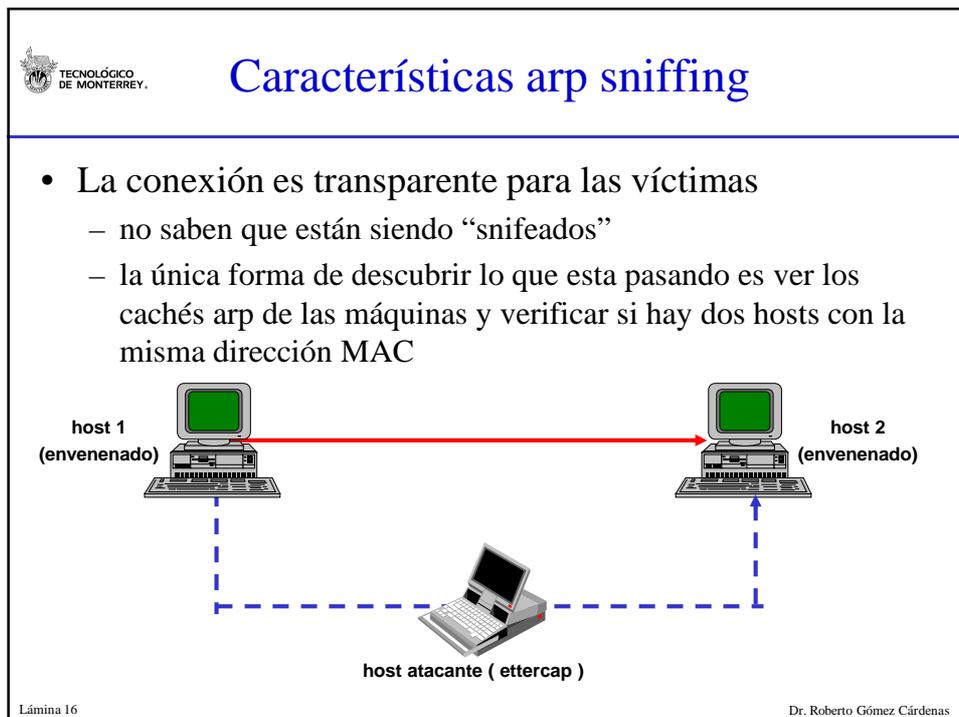
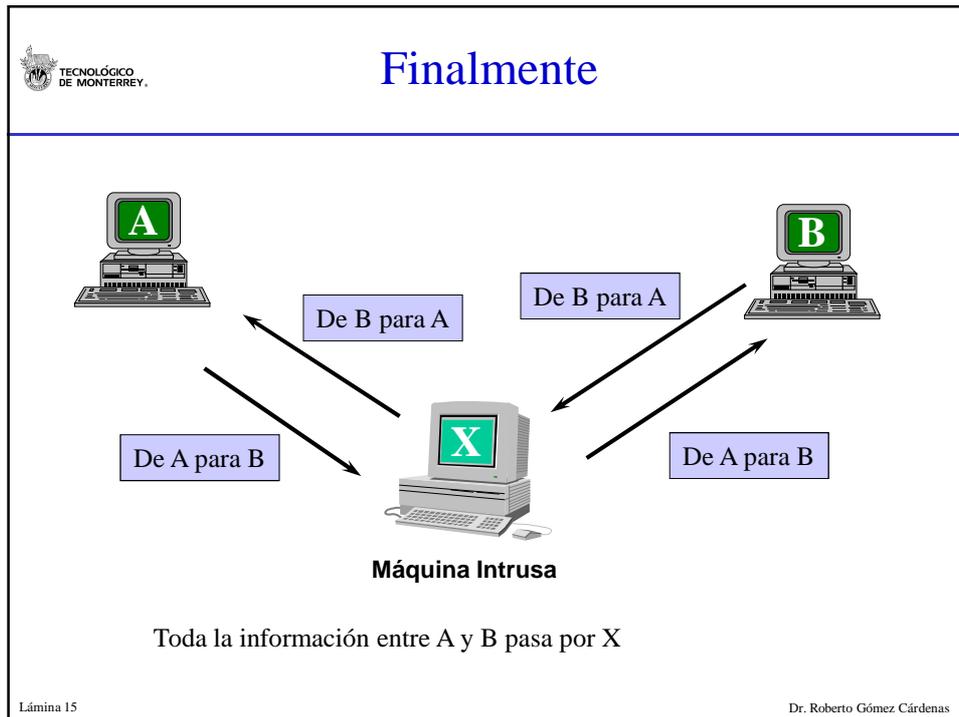


Máquina A pregunta la dirección física de B

Lámina 10 Dr. Roberto Gómez Cárdenas









Tablas CAM y direcciones MAC

- Tablas CAM: Content Addressable Memory.
- Tabla almacena información como direcciones MAC disponibles en los puertos físicos con sus parámetros de VLAN asociados.
- Las tablas tienen un tamaño fijo.

1234.5678.9ABC
48 bits hexadecimales (base 16)

Primeros 24 bits = Código Fabricante
asignado por la IEEE

0000.0cXX.XXXX

Segundos 24 bits = Interfaz Específica
asignado por el fabricante

XXXX.XX00.0001

Todos F's = Broadcast

FFFF.FFFF.FFFF

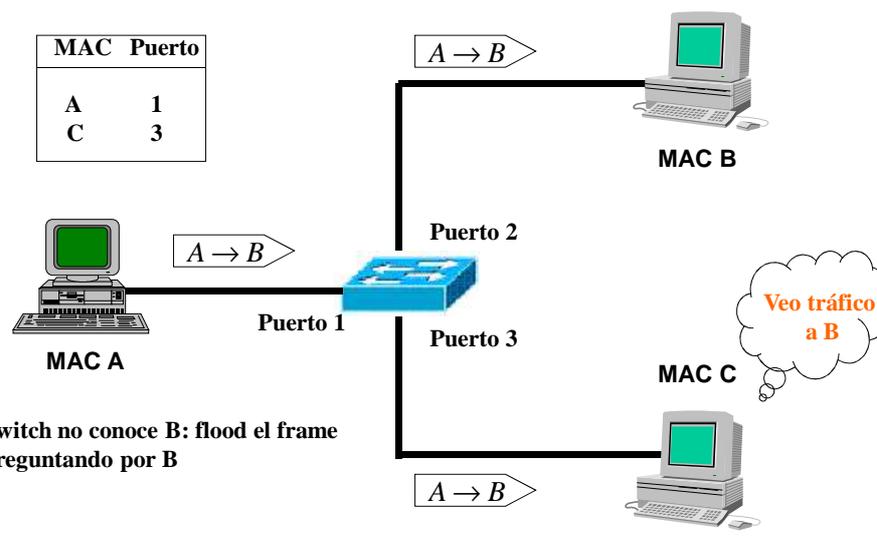
Lámina 17
Dr. Roberto Gómez Cárdenas



Comportamiento normal CAM

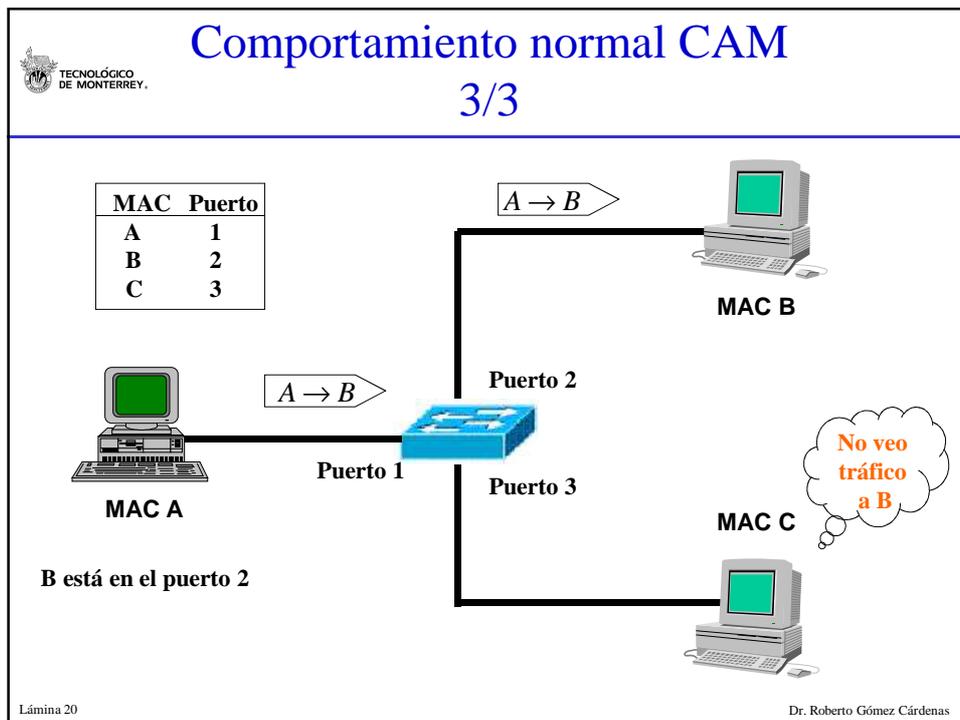
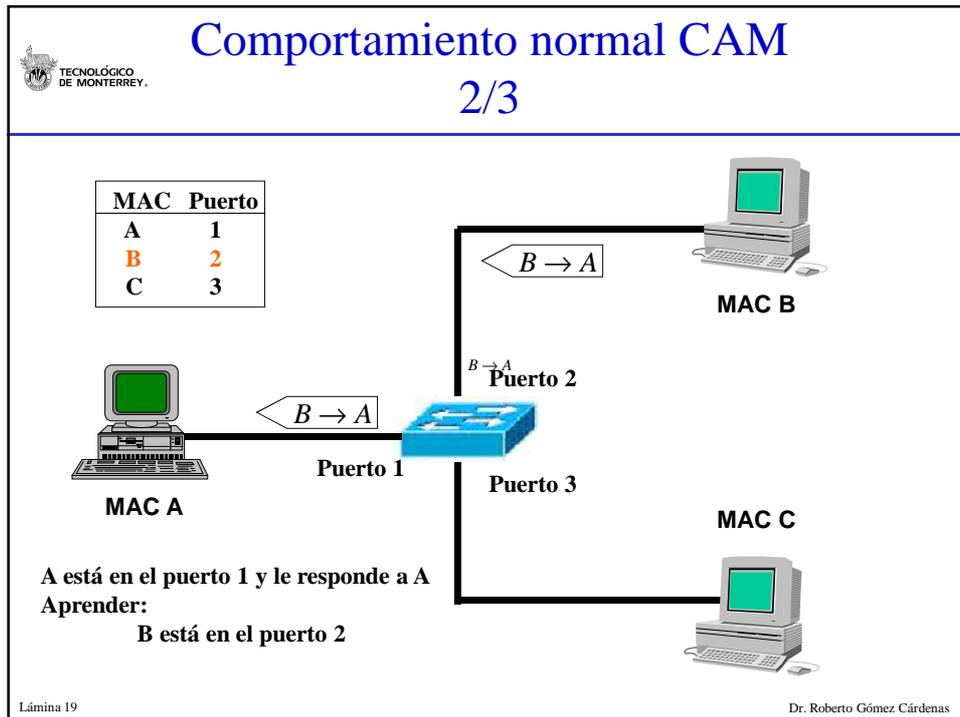
1/3

MAC	Puerto
A	1
C	3



Switch no conoce B: flood el frame preguntando por B

Lámina 18
Dr. Roberto Gómez Cárdenas





Catalyst CAM Tables

- Switches catalyst usan hash para dar de alta MACs en una tabla CAM

1	A	B	C					
2	D	E	F	G				
3	H							
:	I							
:	J	K						
16,000	L	M	N	O	P	Q	R	S

T inundando

- 63 bits de fuente (MAC, VLAN, misc) crea un valor hash de 17 bits
 - si el valor es el mismo (colisión) existen 8 columnas para ubicar entradas CAM, si las 8 están llenas el paquete inunda la VLAN

Lámina 21
Dr. Roberto Gómez Cárdenas



Llenando la tabla CAM

- Dsniff (macof) puede generar 155,000 entradas MAC por minuto en un switch.
- Asumiendo una función hash perfecta la tabla CAM se llenará después de 128,000 direcciones (16,000 x 8 = 31,052 para ser exactos).
- La función hash no es perfecta
 - actualmente toma 70 segundos llenar la tabla CAM

**CAT6506 (enable) sho cam count dynamic
Total Matching CAM entries = 131052**

- Una vez que la tabla esta llena, tráfico sin una entrada CAM inunda la VLAN, pero no existe tráfico con una entrada en la tabla CAM

Lámina 22
Dr. Roberto Gómez Cárdenas

 TECNOLÓGICO DE MONTERREY.

Dsniff



- Es una colección de herramientas que pueden implementar diferentes ataques.
- Realizado por Dug Song
- ARP spoofing
- MAC flooding
- Selective sniffing
- SSH/SSL interception



Lámina 23 Dr. Roberto Gómez Cárdenas

 TECNOLÓGICO DE MONTERREY.

Contra medidas sniffers

- Privilegios usuarios.
- Auditoría software máquinas usuarios.
- Detectores de sniffers.
- Redes switcheadas.
- Cifrado de las comunicaciones.

Lámina 24 Dr. Roberto Gómez Cárdenas

 **VLAN “Hopping” Attacks**

- Este tipo de ataque pretende engañar a un switch (sobre el cual se implementan VLANs) mediante técnicas de Switch Spoofing logrando conocer los paquetes de información que circulan entre VLANs.

Lámina 25 Dr. Roberto Gómez Cárdenas

 **Puertos “troncales”**

- Este tipo de puertos tienen acceso a todas las VLANs por default.
- Empleados para transmitir tráfico de múltiples VLANs a través del mismo enlace físico (generalmente empleado para conectar switches).

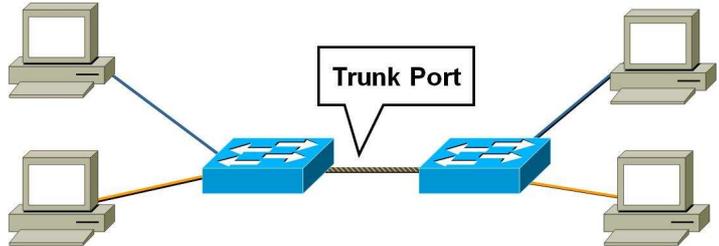


Lámina 26 Dr. Roberto Gómez Cárdenas



DTP: Dynamic Trunk Protocol

- Automatiza la configuración de los troncales (trunk) 802.1Q/ISL.
- Sincroniza el modo de trunking en los extremos.
- Hace innecesaria la intervención administrativa en ambos extremos.
- El estado de DTP en un puerto trunk puede ser “Auto”, “On”, “Off”, “Desirable”, o “Non-Negotiate”.
- Por default en la mayoría de los switches es “Auto”.

Lámina 27

Dr. Roberto Gómez Cárdenas



Ataque VLAN Hopping

- Un equipo puede hacerse pasar como un switch con 802.1Q/ISL y DTP, o bien se puede emplear un switch.
- El equipo se vuelve miembro de todas las VLAN.
- Requiere que el puerto este configurado con trunking automático.

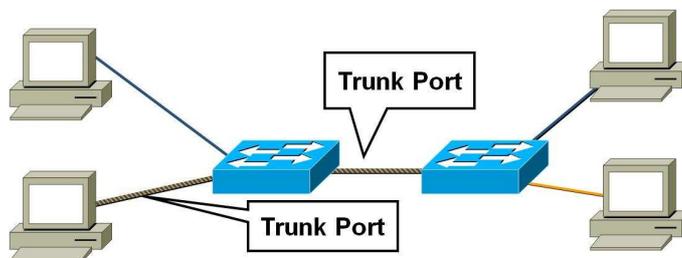


Lámina 28

Dr. Roberto Gómez Cárdenas


**Double Encapsulated 802.1Q
VLAN Hopping Attack**

Strip off First, and Send Back out

Atacante

Victim

Nota: solo funciona si el troncal tiene la misma VLAN nativa que el atacante.

- Se envía una trama 802.1Q de la VLAN de la víctima dentro de otra trama 802.1Q de nuestra VLAN.
- Los switches realizan un solo nivel de desencapsulado.
- Solo permite tráfico en una sola dirección..
- Funciona aunque el puerto del atacante tenga desactivado el trunking.

Lámina 29 Dr. Roberto Gómez Cárdenas


Contramedidas

- Usar switches recientes.
- Deshabilitar auto-trunking
- Nunca poner hosts en el troncal nativa de la VLAN.
- Poner puertos sin usar en una VLAN sin usar.

Lámina 30 Dr. Roberto Gómez Cárdenas

 **Spanning Tree Protocol**

- Solución a los problemas de ciclos es no tener ciclos en la topología de la red.
- IEEE 802.1 tiene un algoritmo que construye y mantiene un spanning tree en un ambiente dinámico.
- Los switches intercambian mensajes BPDU (Configuration Bridge Protocol Data Unit) para configurar el switch para luego este construir el árbol.

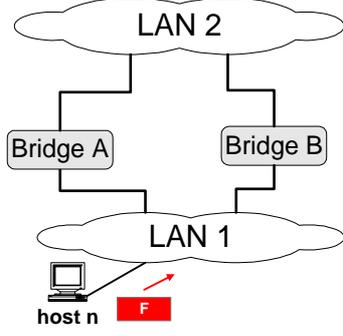
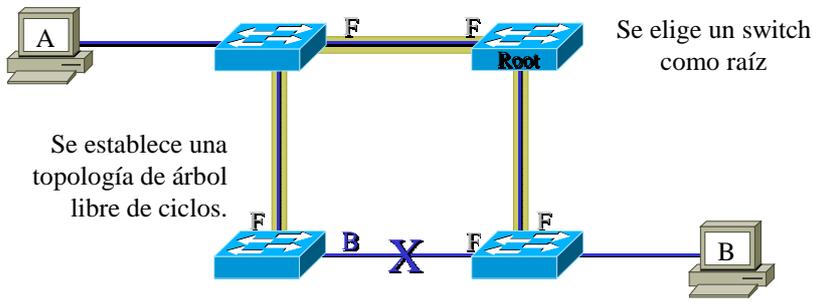


Lámina 31 Dr. Roberto Gómez Cárdenas

 **Conectividad libre de ciclos**



Se establece una topología de árbol libre de ciclos.

Se elige un switch como raíz

Lámina 32 Dr. Roberto Gómez Cárdenas

 Ejemplo ataque Spanning Tree

- Se envían mensajes BPDU desde el atacante para forzar a recalcular el árbol de expansión.
 - Impacto de DoS
- Enviar mensajes para convertirse en la raíz.

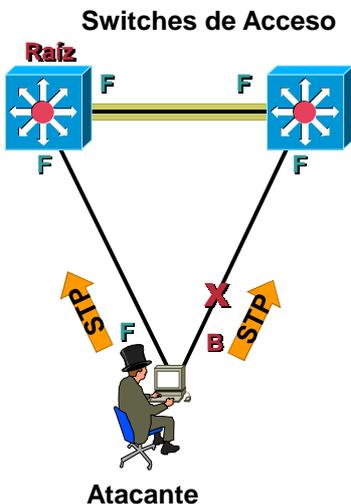


Lámina 33 Dr. Roberto Gómez Cárdenas

 Segundo paso del ejemplo ataque Spanning Tree

- Se envían mensajes BPDU desde el atacante para forzar a recalcular el árbol de expansión.
 - Impacto de DoS
- Enviar mensajes para convertirse en la raíz.
 - El atacante empieza a ver paquetes que no debería.
 - MITM, DoS, etc.
- Requiere que el atacante se encuentre con dos tarjetas de red entre los dos switches.

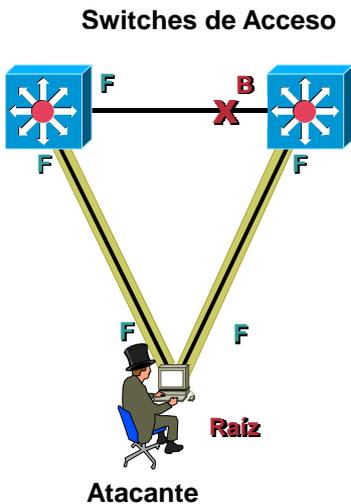


Lámina 34 Dr. Roberto Gómez Cárdenas



Contramedidas

- **Deshabilitar STP**
 - Si no se necesita en topologías libres de ciclos.
- **BPDU Guard**
 - Deshabilita puertos cuando detecta mensajes BPDU en el puerto
- **Root Guard**
 - Deshabilita puertos que se convertirán en el nodo raíz debido a un mensaje BPDU.

Lámina 35 Dr. Roberto Gómez Cárdenas



Ataque de servidor rojo DHCP

- Instalación de un Servidor DHCP desconocido en la subred local.
- Otro ataque: acabar con los pools de DHCP.
- RFC 3118 “Authentication for DHCP Messages” puede ayudar, pero aún no ha sido implementado.
- **Contramedidas**
 - Considerar el uso de múltiples servidores DHCP para diferentes zonas de seguridad de la red.
 - Usar ACL para las VLANs para bloquear tráfico DHCP desde un servidor desconocido.
 - Asignación de direcciones IP estáticas
 - Utilización de controles a nivel MAC
 - Monitoreo de ARP/RARP (arpwatch puede ayudar a identificar “rouge” DHCP o BOOTP servers
 - Control de puertos en el switch.

Lámina 36 Dr. Roberto Gómez Cárdenas



Contra medidas capa 2: ARP

- Control de puertos (switch)
 - asignación de dirección MAC de un sistema y puerto del switch.
- Monitoreo de tráfico ARP (arpwatch)
- Caches de ARP estáticos
 - principalmente en elementos críticos como firewalls, routers y servidores clave).
 - el problema es que se vuelve poco práctico si se quiere aplicar a todos los sistemas y elementos de conectividad.

Lámina 37

Dr. Roberto Gómez Cárdenas



¿Y si lo autenticamos?

- Protocolo 802.1x
 - Estándar IEEE para Port Based Network Access Control
 - Basado en EAP
 - EAP: Extensible Authentication Protocol
 - Autenticación usuario
 - Puede trabajar en 802.3 o 802.11

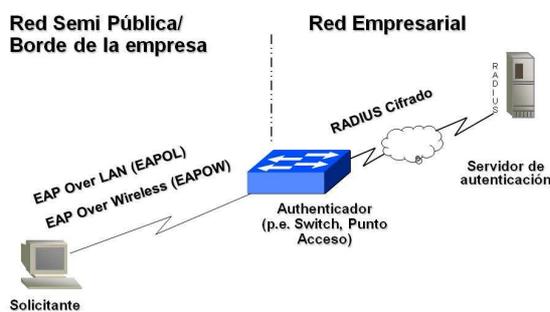
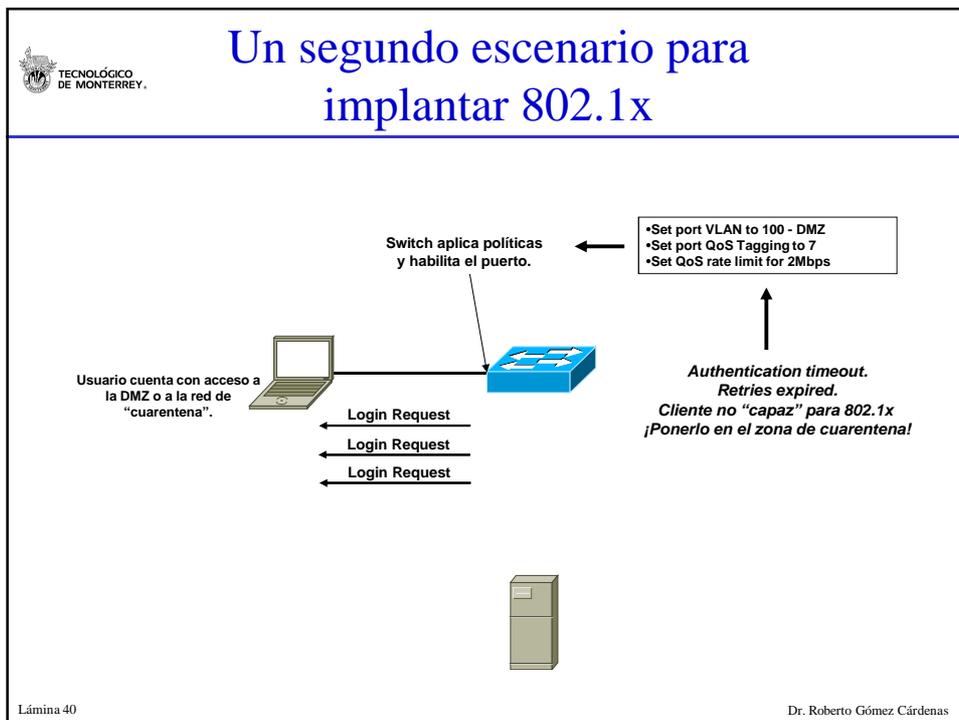
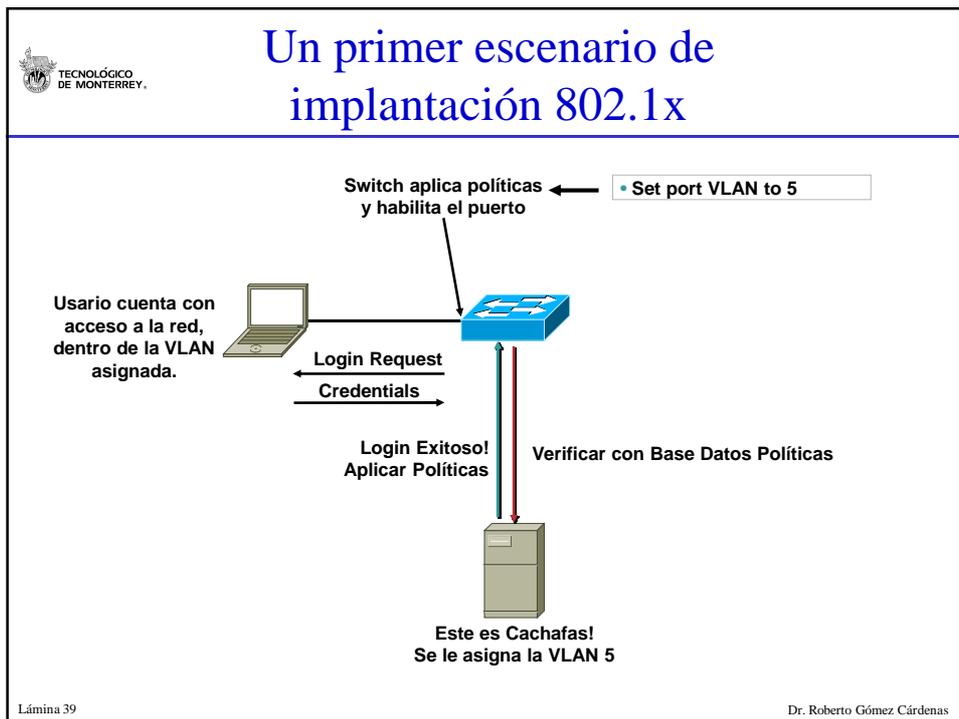


Lámina 38

Dr. Roberto Gómez Cárdenas





Negación de servicio

- Su objetivo principal es impedir que un organismo proporcione el servicio para el que fue creado.
 - busca elevar los índices de utilización de algún servicio o sistema hasta bloquear totalmente el acceso al mismo desde el exterior
- Generalmente se basa en un ataque a una sola máquina
- Un ataque de DoS desorganiza o niega completamente un servicio a los usuarios legítimos
- Por regla general es más fácil realizar un ataque de DoS que introducirse en un sistema
- Es más fácil esconder el origen de un ataque de DoS

Lámina 41 Dr. Roberto Gómez Cárdenas



Algunos tipos negación servicio

- Consumo de Ancho de Banda
- Inanición de recursos
- Defectos de programación
- Paquetes mal formados
- Ataques DNS y de enrutamiento

Lámina 42 Dr. Roberto Gómez Cárdenas



Consumo ancho banda

- Buscan consumir todo el ancho de banda disponible
- Pueden definirse 2 escenarios
 1. Los atacantes buscan inundar la conexión de la red de la víctima utilizando un ancho de banda disponible mayor.
 2. El atacante une multitud de sitios para inundar la conexión de la víctima. El atacante hará que varios sitios envíen información de forma concentrada hacia la red víctima.

Lámina 43 Dr. Roberto Gómez Cárdenas



Inanición de recursos

- Está enfocado al consumo de recursos del sistema.
- Los recursos abusados pueden ser:
 - CPU
 - Memoria
 - Cuotas del Sistema de Archivos
 - Número de proceso
 - Capacidad de un servicio
- Muchos virus distribuidos por email realizan su ataque de esta forma

Lámina 44 Dr. Roberto Gómez Cárdenas



Defectos de programación

- Son fallos de una aplicación, sistema operativo o elemento de hardware
- Estos fallos tienden a ocurrir cuando un usuario envía datos imprevistos al elemento vulnerable.
- Ejemplo:
 - Paquetes ICMP mal formados
 - Mensajes TCP de longitud anormal
 - Ejecución de instrucciones erróneas

Lámina 45

Dr. Roberto Gómez Cárdenas

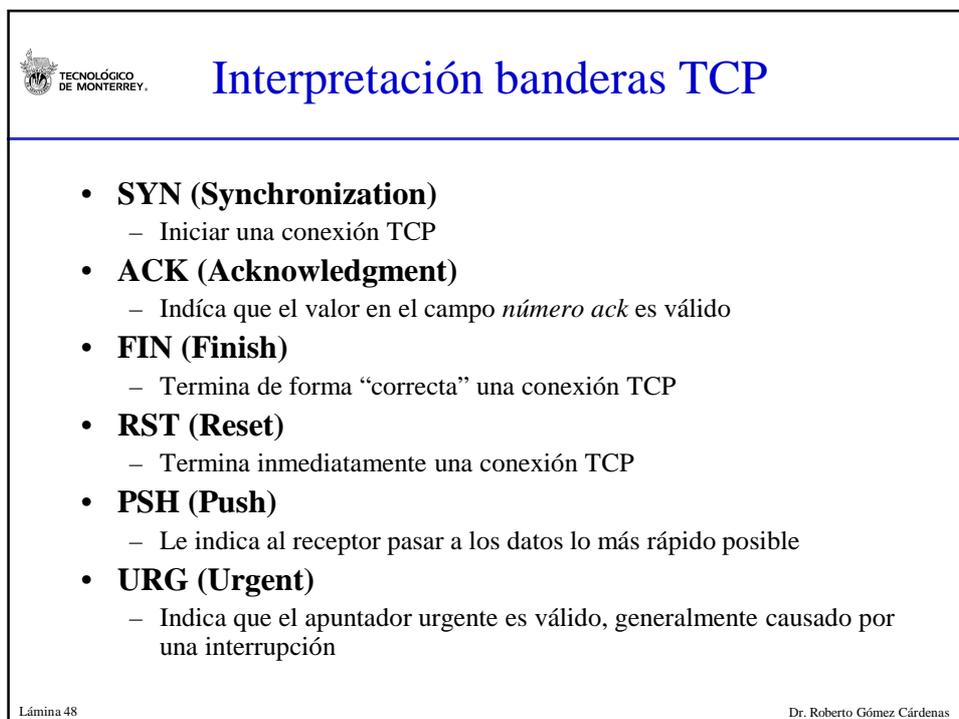
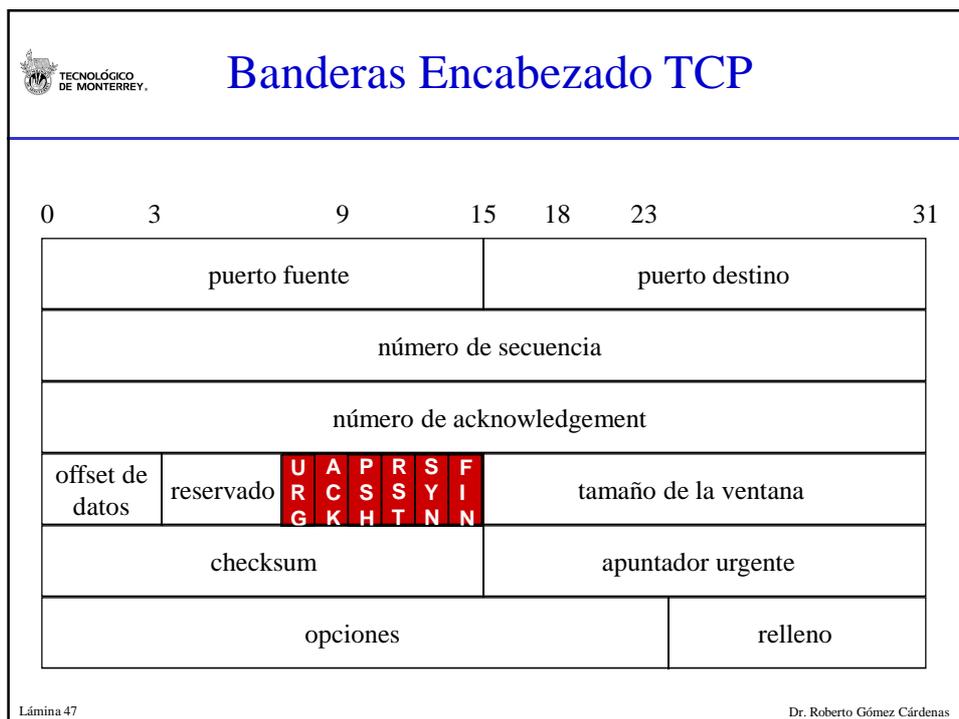


Paquetes Mal Formados

- Una de las formas más comunes de detener un servicio.
- Explotan un error en el stack TCP/IP de la máquina destino enviando uno o más paquetes, mal formados, a la máquina destino.
- Si la maquina destino es vulnerable es posible que:
 - termine con un proceso
 - toda la red de comunicaciones
 - provocar que el sistema operativo de la victima se detenga

Lámina 46

Dr. Roberto Gómez Cárdenas





Valores normales banderas

- **SYN, SYN ACK y ACK**
 - usados durante el three-way handshake
- **ACK**
 - a excepción paquete inicial SYN, cada paquete en una conexión debe tener el bit ACK activo
- **FIN ACK y ACK**
 - son usados para terminar una conexión existente
- **PSH FIN ACK**
 - también pueden ser vistos al principio de una desconexión
- **RST o RST ACK**
 - pueden usarse para terminar inmediatamente una conexión existente
- Paquetes durante “conversación” (después handshake y antes desconexión) solo contienen un ACK por default
 - opcionalmente puede contener **PSH** y/o **URG**

Lámina 49

Dr. Roberto Gómez Cárdenas



Valores anormales

- **SYN FIN**
 - probablemente la combinación ilegal más conocida
- **SYN FIN PSH, SYN FIN RST, SYN FIN RST PSH**
 - y otras variantes de **SYN FIN** también existen
 - objetivo: evadir IDS que buscan paquetes con solo bits **SYN** y **FIN** activos
- Paquetes con solo la bandera **FIN** activa
 - paquetes usados para scaneos de puertos
- Paquetes sin ninguna bandera activa
 - paquetes conocidos como paquetes nulos

Lámina 50

Dr. Roberto Gómez Cárdenas



Otros posibles valores anormales

- Paquetes nunca deben tener una dirección fuente o destino igual a 0
- El número de ack nunca debe tener un valor de 0 cuando la bandera ACK esta activa
- Un paquete con solo SYN activo no debe contener datos
 - lo anterior se da cuando una nueva conexión se inicia
- Paquetes no deben usar una dirección destino que sea una dirección de broadcast
 - usualmente terminan en .0 o .255
 - .0 es un viejo estilo de broadcast
- Normalmente no se realizan broadcasts usando TCP

Lámina 51
Dr. Roberto Gómez Cárdenas



Ataques paquetes mal formados

Nombre	Funcionamiento	Plataformas vulnerables
Land	Envía paquetes con direccion IP y puerto destino/origen es iguales	Sistemas Windows, varios Tipos Unix, impresoras, ruteadores
Latierra	Variante distribuida de Land	Sistemas Windows, varios Unix, ruteradores, impresoras
Ping de la muerte	Paquete ping grande	Windows, variantes Unix, impresoras
Jolt2	Envío paquetes fragmentados con valor de <i>fragment offset</i> NO cero	Windows 95, 98, NT y 2000
Teardrop, Newtear, Bonk, Syndrop	Herramientas que envían fragmentos de paquetes IP que se sobreponen, con valores tales que no se pueden reensamblar.	Windows 95, 98, NT y Linux
Winnuke	Envía basura a un puerto 139 TCP en una máquina Windows, afectando formateo SMB.	Windows 95 y NT

Lámina 52
Dr. Roberto Gómez Cárdenas



Otros ataques DoS

- Inundación Syn
- Smurfing
- Fraggle
- Connection flood
- DoS Distribuido

Lámina 53 Dr. Roberto Gómez Cárdenas



Inundación syn

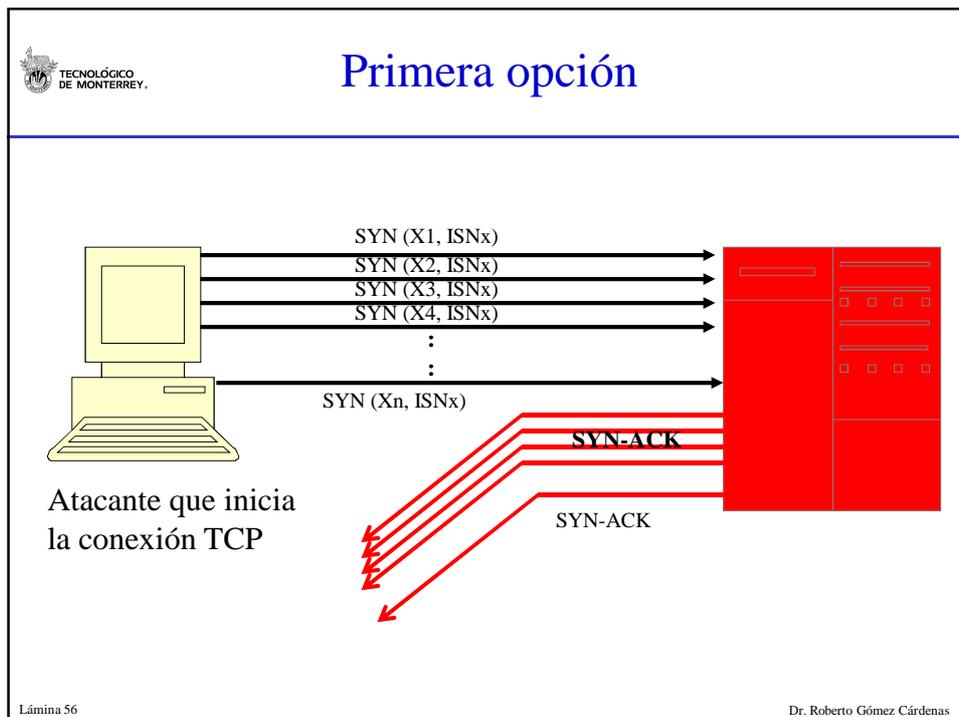
- El ataque se basa en el mecanismo de establecimiento de una conexión TCP.
- El problema que explota es que cada sistema reserva una cantidad finita de recursos una vez ha enviado el mensaje SYN/ACK para terminar el establecimiento de la conexión.
- El objetivo del atacante es abrumar la máquina destino con paquetes SYN.
 - cuando la víctima recibe más paquetes SYN de los que puede manejar, otro tipo de tráfico no podrá llegar a la víctima

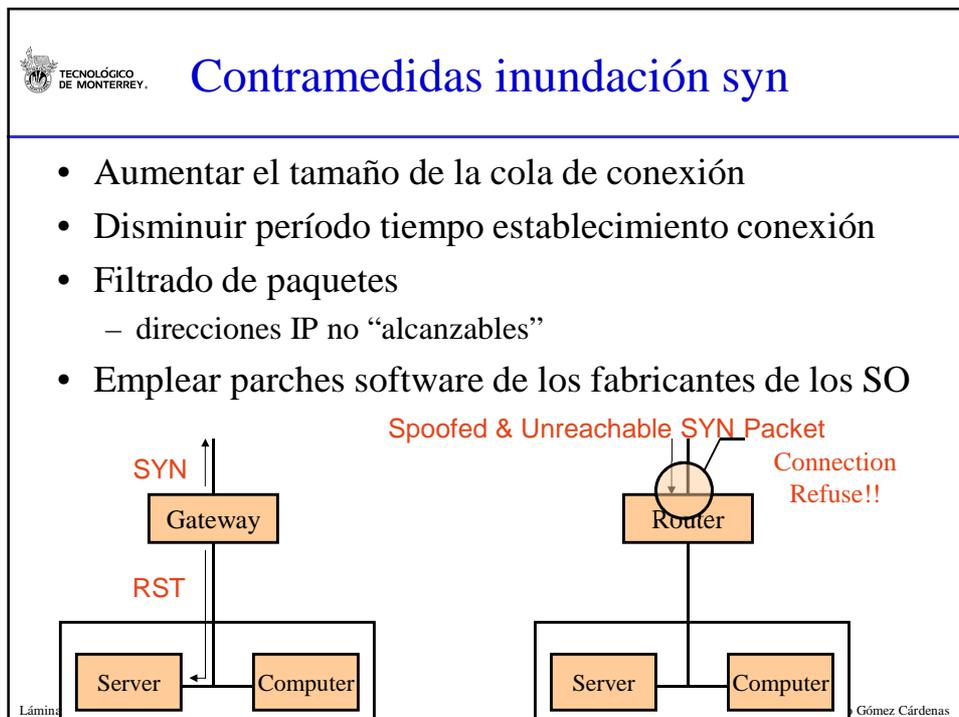
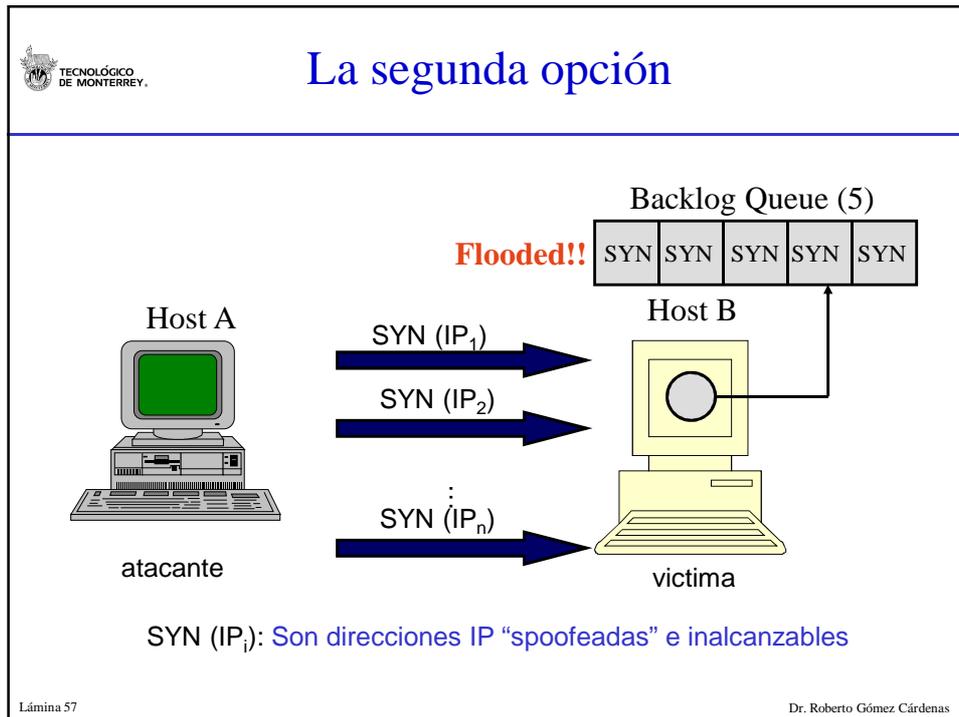
Lámina 54 Dr. Roberto Gómez Cárdenas

 **¿Y cómo se hace?**

- Dos formas de hacerlo
- La primera inunda la cola de conexiones del sistema objetivo con medias conexiones abiertas
- La segunda es enviar paquetes syn de conexión con la dirección IP de otras máquinas.

Lámina 55 Dr. Roberto Gómez Cárdenas







Smurfing/Fraggle

- Se lleva a cabo principalmente en ruteadores Cisco y probablemente en otras marcas.
- Consiste en pedir una respuesta a varias máquinas y haciendo pasar por otra computadora.
 - de esta forma todas las respuestas llegaran a la víctima
 - diferencia: tipo de respuesta solicitada
- Requiere 3 actores: la víctima, el atacante y la red amplificadora
 1. El atacante originará un paquete ICMP hacia la dirección de broadcast de la red amplificadora, haciendo aparecer que su origen es una interfaz de la red de la víctima
 2. Cada interfaz de la red amplificadora enviará respuestas a la supuesta interfaz de origen

Lámina 59

Dr. Roberto Gómez Cárdenas



Definición IP Spoofing

1. The creation of IP packets with counterfeit (spoofed) IP source addresses.
2. A method of attack used by network intruders to defeat network security measures such as authentication based on IP addresses.

Note 1: An attack using IP spoofing may lead to unauthorized user access, and possibly root access, on the targeted system

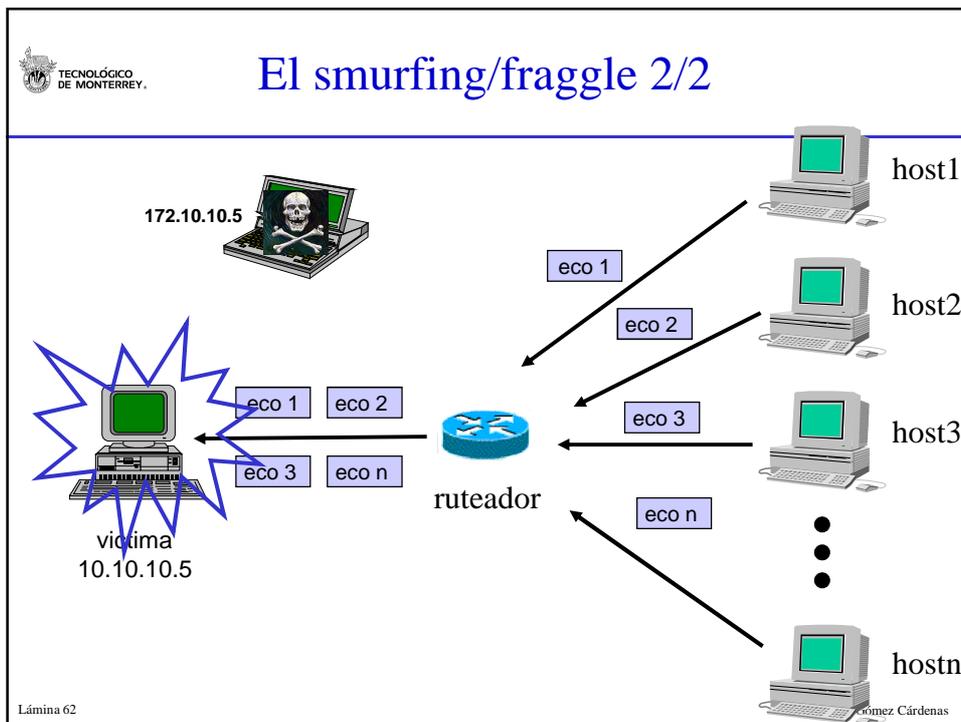
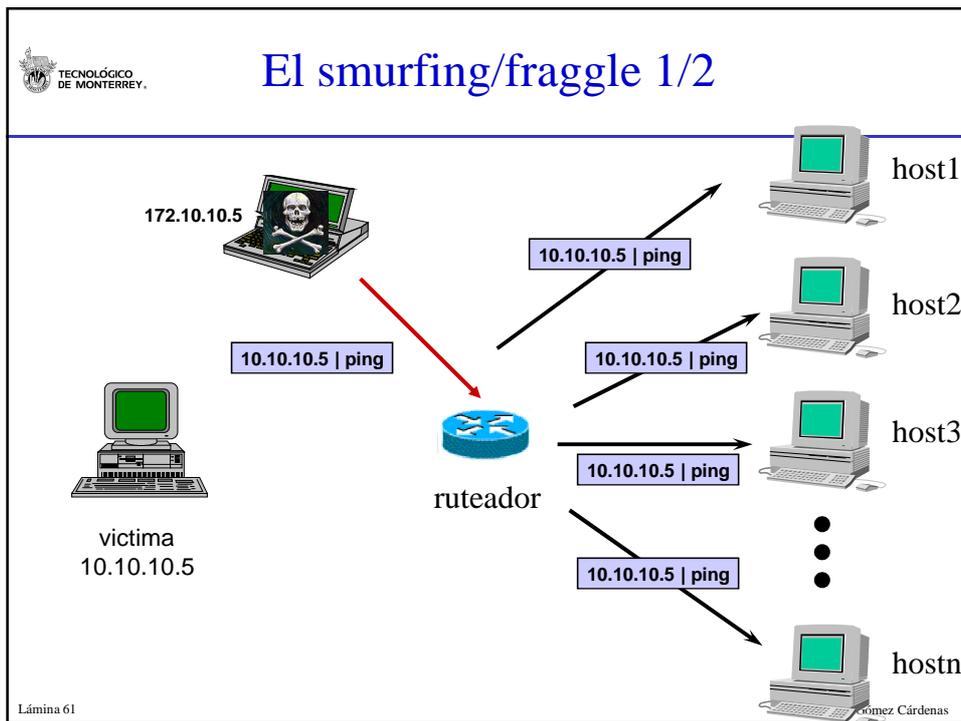
Note 2: A packet-filtering-router firewall may not provide adequate protection against IP spoofing attacks. It is possible to route packets through this type of firewall if the router is not configured to filter incoming packets having source addresses on the local domain

Note 3: IP spoofing is possible even if no reply packets can reach the attacker.

Note 4: A method for preventing IP spoofing problems is to install a filtering router that does not allow incoming packets to have a source address different from the local domain. In addition, outgoing packets should not be allowed to contain a source address different from the local domain, in order to prevent an IP spoofing attack from originating from the local network

Lámina 60

Dr. Roberto Gómez Cárdenas





Previniendo smurf/fraggle

- Para no permitir ser utilizado como red amplificadora debe deshabilitar el paso de mensajes destinados a broadcast a través de los routers de frontera
 - Cisco: no ip direct-broadcast
- Para limitar el daño ocurrido por un ataque de este tipo sobre su red, limite el tráfico ICMP a un valor razonable de acuerdo a su disponibilidad de ancho de banda
- Verifique si realmente necesita permitir tráfico de entrada ICMP a toda su red

Lámina 63

Dr. Roberto Gómez Cárdenas



Otro tipo de ataque smurf



Lámina 64

Dr. Roberto Gómez Cárdenas



Connection Flood

- Se basa en la característica de la mayoría de los proveedores de Internet (ISP) de tener un tope máximo de conexiones simultáneas, que tras ser alcanzado no acepta más conexiones.
- Si por ejemplo un servidor Web tiene un tope de 1000 conexiones, y el atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor.
- Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita establecer nuevas conexiones para mantener fuera de servicio el servidor.

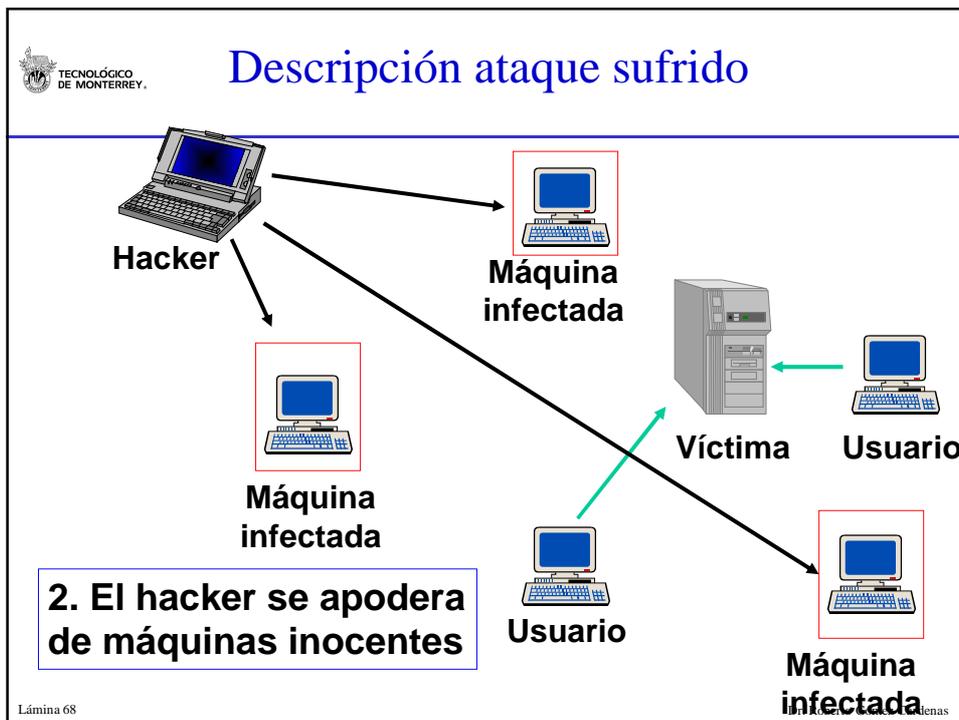
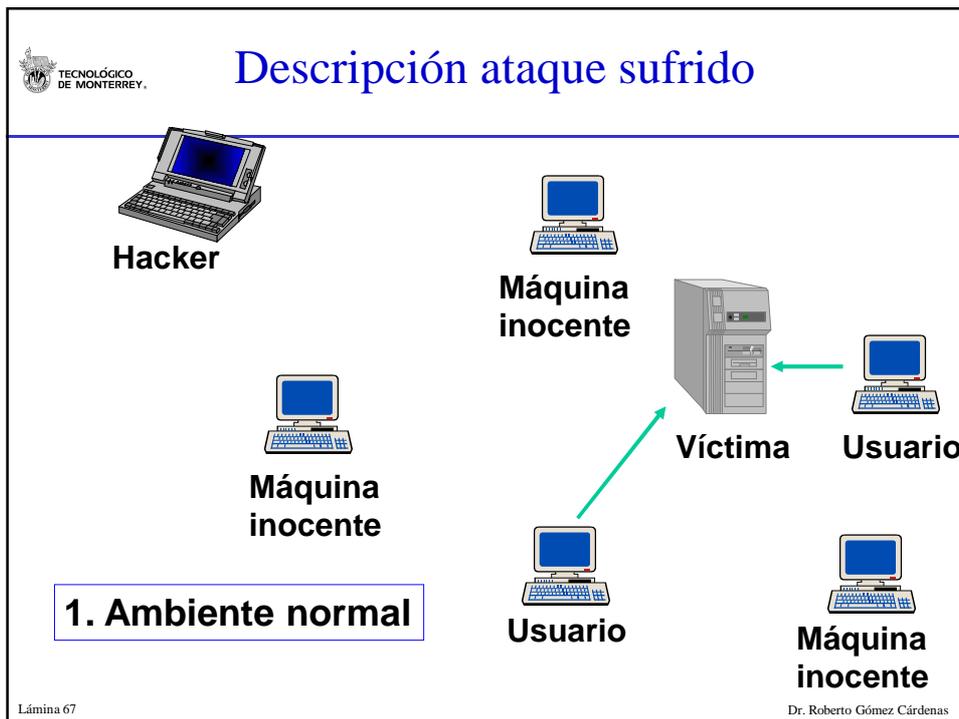
Lámina 65 Dr. Roberto Gómez Cárdenas

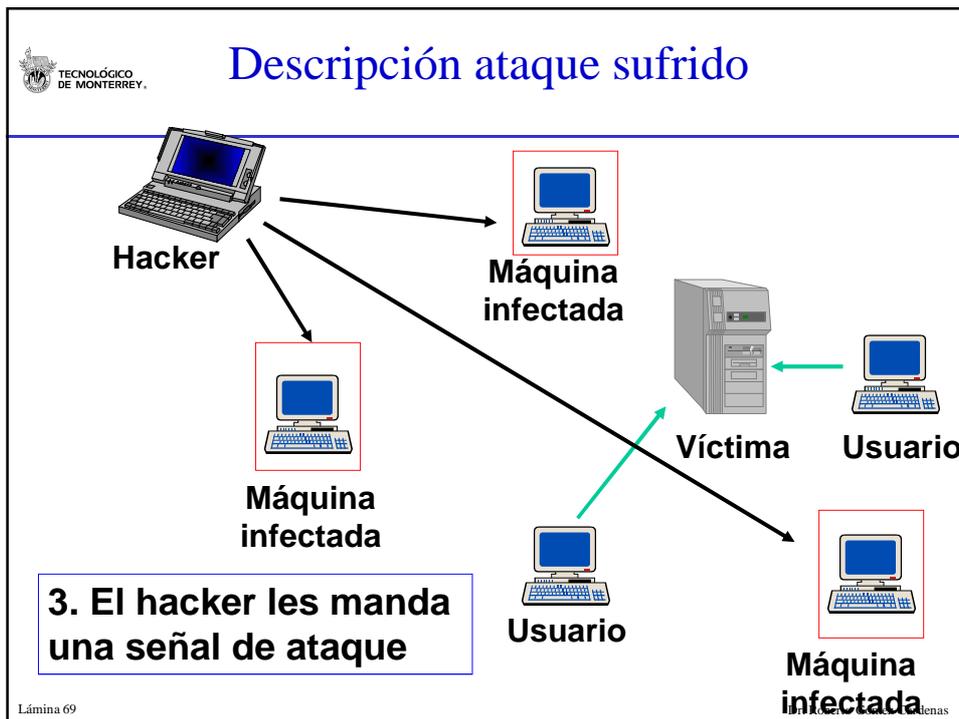


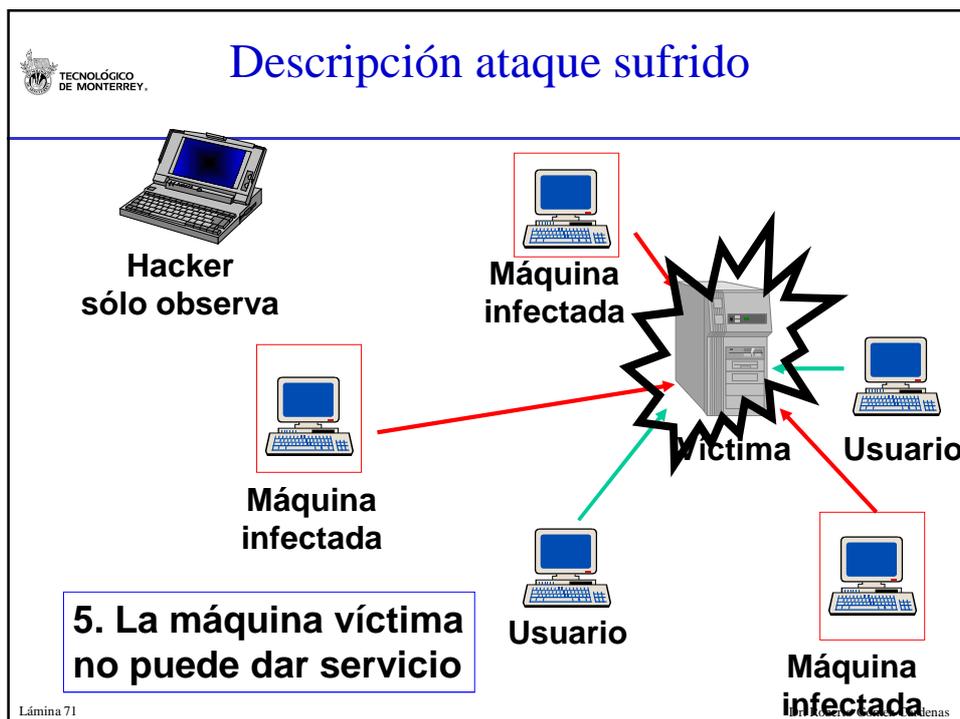
DoDS: Negación Servicio Distribuido

- En febrero/marzo del 2000, varias empresas que apoyan su estrategia en Internet fueron atacadas.
 - Yahoo! estima pérdidas por US\$500,000 dls por dejar de dar servicio durante 3 horas
- Entre ellas destacan:
 - CNN (Agencia Noticiosa)
 - Amazon (Venta de libros, discos, etc.)
 - e-Bay (Venta de artículos en remate)
 - e-Trade (compra y venta de acciones)
 - Yahoo (Correo gratuito)

Lámina 66 Dr. Roberto Gómez Cárdenas









¿Y cómo creo un paquete mal formado?

- Programas inyectoros de paquetes
- Objetivo
 - formar sus propios paquetes de red e inyectarlos en la red
- Diferentes tipos de protocolos soportados
- Diferentes tipos de red soportadas
- En un principio usados para probar firewalls, detectores de intrusos y servidores.

Lámina 73 Dr. Roberto Gómez Cárdenas



Paquetes Inyectores

- Send IP
 - Herramienta de comando línea que permite enviar paquetes IP arbitrarios
 - <http://www.earth.li/projectpurple/progs/sendip.html>
- wINJECT:
 - Inyección de paquetes para Win9x & Win2k
 - home19.inet.tele.dk/moofz/about_o.htm
- Nemesis (packet injection)
 - Inyección de paquetes de comando de línea Unix
 - <http://www.packetfactory.net/Projects/nemesis>
- Hping
 - Analizador y creador de paquetes TCP/IP a nivel línea de comandos.
 - <http://www.hping.org/>

Lámina 74 Dr. Roberto Gómez Cárdenas



Hping

- En un herramienta de creación de paquetes TCP/IP.
- Puede ser usado para crear paquetes IP que contienen cargas (payloads) de tipo TCP, UDP o ICMP.
- Todos los campos de encabezado pueden modificarse y controlarse a través de la línea de comandos.
- Se requiere un buen entendimiento de los protocolos IP, TCP y UDP para poder sacar el máximo provecho a esta herramienta.

Lámina 75 Dr. Roberto Gómez Cárdenas



Posibles usos

- Prueba de reglas del firewall
- Prueba desempeño de la red
- Fingerprint de Sistemas Operativos
- Auditoría stacks TCP/IP
- Verificar si un host esta arriba
- Un “ping” TCP que pueda atravesar firewalls, mientras que una petición ICMP no.

Lámina 76 Dr. Roberto Gómez Cárdenas



Sintaxis

- La sintaxis es

```
hping2 host [opciones]
```
- Algunas opciones interesantes

Opción	Significado
-c	Cantidad de peticiones a llevar a cabo
-i	Intervalo de espera (uX para X microsegundos) entre envío de paquetes.
-I	Nombre de la interface
-V	Verbose
-D	Información de depuración
-q	Silencioso, no se muestra nada, excepto las líneas de resumen al comenzar y al terminar.
-n	Sólo salida numérica, no se intentará la búsqueda de nombres simbólicos para direcciones de host.

Lámina 77
Dr. Roberto Gómez Cárdenas



Modos

- El modo por defecto es TCP
- Otros modos

Modo	Equivalente	Significado
-0	--rawip	Modo RAW IP
-1	--icmp	Modo ICMP
-2	--udp	Modo UDP
-8	--scan	Modo SCAN
-9	--listen	Modo escucha

Lámina 78
Dr. Roberto Gómez Cárdenas



Opciones modo IP

- Para paquetes IP es posible definir el valor de algunos campos
- Por ejemplo:

Opción	Equivalente	Significado
-a	--spooF	Dirección fuente destino
--rand-dest		Dirección destino aleatoria
--rand-source		Dirección fuente aleatoria
-t	-ttl	Valor TTL (64 por defecto)
-o	-tos	Type of service (0x00 por defecto)
-x	--morefrag	Activar bandera de fragmentación
-y	--dontfrag	Desactivar bandera fragmentación
-G	--rroute	Redirección
-H	--ipproto	Campo protocolo (solo para modo RAW IP)

Lámina 79
Dr. Roberto Gómez Cárdenas



Opciones modo ICMP

- Campos para protocolo ICMP

Opción	Significado	Type	Description
-C	Tipo de ICMP, echo request por defecto	0	echo-reply
		3	destination-unreachable
		4	source-quench
		5	redirect
		8	echo-request
-K	Código ICMP, 0 por defecto	11	time-exceeded
		12	parameter-problem
--force-icmp	Envía todos los tipos ICMP (solo los soportados)		
--icmp-gw	Establece dirección para ICMP redirect (0.0.0.0 por defecto)		
--icmp-ts	Alias para --icmp --icmptype 13		
--icmp-addr	Alias para --icmp --icmptype 17		
--icmp-help	Despliega ayuda para otras opciones ICMP		

Code	Description
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Destination network prohibited
10	Destination host prohibited

Lámina 80
Dr. Roberto Gómez Cárdenas



UDP/TCP

- Opciones

Opcion	Equivalente	Significado
-s	--baseport	Puerto base (random por defecto)
-p	--destport	Puerto destino
-k	--keep	Mantiene puerto destino
-M	--setseq	Establece número de secuencia
-L	--setack	Habilita ACK
-w	--win	Tamaño ventana (64 por defecto)
-O	--tcpoff	Asigna un valor offset falso
-Q	--seqnum	Muestra número de secuencia

Lámina 81
Dr. Roberto Gómez Cárdenas



Banderas paquetes TCP

- Posible especificar banderas a activar.

Parámetro	Bandera
-F --fin	Activa la bandera FIN
-S --syn	Activa la bandera SYN
-R --rst	Activa la bandera RST
-P --push	Activa la bandera PUSH
-A --ack	Activa la bandera ACK
-U --urg	Activa la bandera URG
-X --xmas	Activa la bandera X, bandera no usada (0x40)
-Y --ymas	Activa la bandera Y, bandera no usada (0x80)

Lámina 82
Dr. Roberto Gómez Cárdenas



Algunos ejemplos

- `hping toto.com -S -V`
 - Envía paquetes TCP SYN al puerto 0 del host toto.com
 - A notar que hping incrementará el puerto origen en 1 por cada paquete que genere.
- `hping toto.com -S -V -p 443`
 - Envía paquete TCP SYN al puerto 443 del host toto.com
- `hping toto.com --udp --spooof 18.1.1.15`
 - Envía paquetes UDP, con dirección origen 18.1.1.15 al host toto.com
- `hping toto.com -V --udp --file datos.txt --data 100`
 - Envía paquetes UDP con la porción de datos con 100 bytes de relleno, pero conteniendo el contenido de datos.txt al host toto.com
- `hping toto.com --udp --rand-source`
 - Envía paquetes con diferentes direcciones origen al hosto ~~toto.com~~ Dr. Roberto Gómez Cárdenas

Lámina 83



Otros ejemplos

- `hping -I eth0 -S 192.168.10.1 -p 80`
- `hping -I eth0 -S 192.168.10.1 -p ++79`
- `hping -M 3000 -SA 192.168.10.1 -p 80`
- `hping -SA 192.168.10.1`
- `hping -SA -r 192.168.10.1`
- `hping toto.com --icmp --icmp-ts -V`
- `hping toto.com --icmp -V`
- `hping toto.com --udp -V -p 111`
- `hping toto.com -S -p 443 -i u10000 -c 500`

Lámina 84

Dr. Roberto Gómez Cárdenas



Secuestro de sesiones

- Termino en inglés: hijacking
- Tipo de ataque en el que el atacante toma control de una comunicación tal y como un secuestrador de aviones tomo control del avión.
 - entre dos entidades y haciendo pasar por una de ellas
- En un tipo de ataque (man in the middle)
 - el atacante toma control de la conexión mientras esta se produce.
- El objetivo es robar una conexión generada por un aplicación de red iniciada por un cliente (p.e. telnet)
 - conseguir un programa en Internet
 - hacerlo manualmente

Lámina 85
Dr. Roberto Gómez Cárdenas



Encabezado TCP

0	3	9	15	18	23	31	
puerto fuente				puerto destino			
número de secuencia							
número de acknowledgement							
offset de datos	reservado	U R G	A C K	P R H	R S T	S S N	F I N
checksum				tamaño de la ventana			
checksum				apuntador urgente			
opciones						relleno	

Lámina 86
Dr. Roberto Gómez Cárdenas



Características TCP

- Transmission Control Protocol RFC 793
- Objetivo: protocolo altamente confiable entre host en redes switcheadas de paquetes.
- Debe recuperarse de datos dañados, perdidos, duplicados o entregados fuera de orden
 - asignación numero secuencia a cada paquete transmitido
 - se requiere un acuse de recibo (ACK) del receptor
 - si, después de un tiempo especificado, el ACK no es recibido el dato es retransmitido
 - el receptor usa números secuencia para ordenar los paquetes fuera de orden y eliminar duplicaciones
 - daño paquetes es manejado con un checksum en cada paquete

Lámina 87 Dr. Roberto Gómez Cárdenas



El numero de secuencia

- Cada paquete de datos enviado a través de una conexión TCP tiene un número de secuencia.
 - se tienen acuse recibo por cada paquete
- Sistema acuse recibo es acumulativo
 - el ack del numero secuencia X, indica que todos los paquetes hasta, pero incluyendo, X se han recibido
- Numeración es en base a los bytes del paquete
 - cada byte tiene un número de secuencia
 - primer dato que sigue al encabezado tiene el menor valor
 - los siguientes bytes son numerados secuencialmente
 - espacio numeración finito pero grande (0 a $2^{32} - 1$)

Lámina 88 Dr. Roberto Gómez Cárdenas



Secuestrando sesión telnet

- **Campo SEQ:** Los datos de este campo son usados para definir la secuencia de los paquetes enviados.
 - esta en hexadecimal y el servidor pondrá estos datos en el campo ACK del paquete que envíe al cliente
- El hijacking es básicamente predecir los datos de los campos SEQ y ACK para enviar paquetes falsos que serán aceptados por el servidor sin que note nada anormal.

Lámina 89

Dr. Roberto Gómez Cárdenas



Principios del ataque

- Una vez que el número de secuencia se ha establecido
 - todos los datos serán $ISN + 1$
- El truco no está en secuestrar la sesión
 - encontrar el ISN
- Tres requerimientos para secuestrar comunicación TCP
 - tráfico no debe estar encriptado
 - atacante debe ser capaz de reconocer los números de secuencia TCP y predecir el número siguiente
 - atacante debe “spoofear” direcciones MAC e IP para recibir comunicaciones no dirigidas a él.

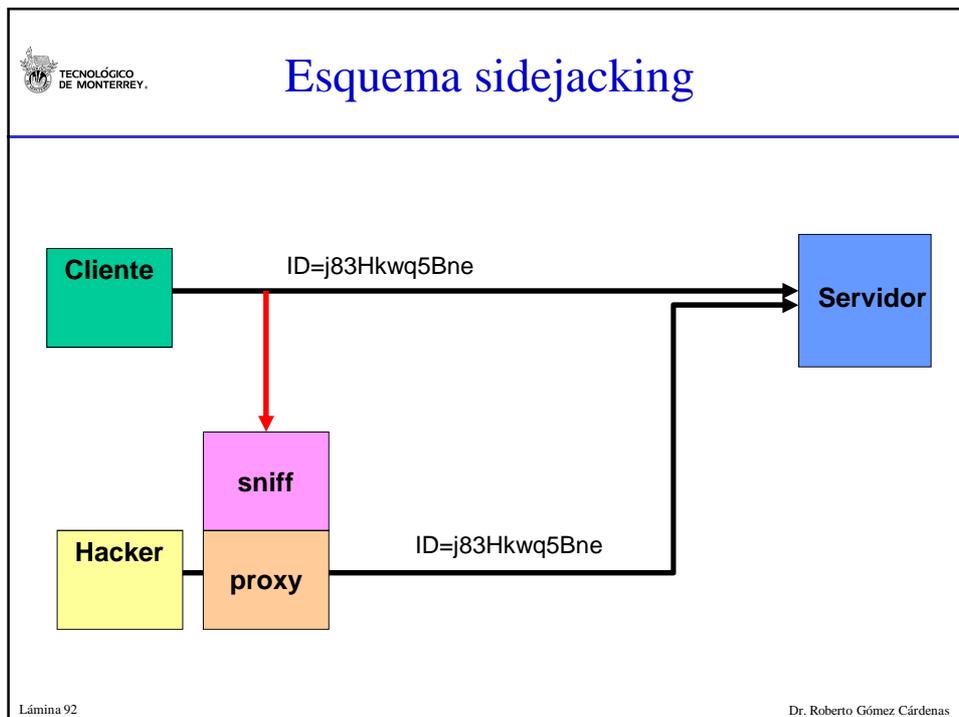
Lámina 90

Dr. Roberto Gómez Cárdenas

 **Sidejacking**

- Ataque a aplicaciones con Web/2.0
- Passwords cifrados para autenticación (login)
 - Posible con SSL
- Pero los datos no se encuentran cifrados
 - Cookies contienen
 - Cada petición HTTP envía
- No se trata de un ataque de hombre en medio.
- No se trata de un secuestro en si, sino más bien de una clonación.

Lámina 91 Dr. Roberto Gómez Cárdenas





La cookie buscada

- proto="HTTP", op="GET",
Host="farm1.static.flickr.com",
URL="/190/495273334_ccb75752c1_m.jpg",
cookie="cookie_epass=70fe73053a47f87eb
22a6373325b0db3; cookie_accid=365488;
**cookie_session=365488%3A70fe73053a47f
87eb22a6373325b0db3;**
use_master_until=1179009958"

Lámina 93 Dr. Roberto Gómez Cárdenas



Herramientas

- Dos herramientas para hacer lo anterior
 - Ferret: es un sniffer de línea de comandos que captura cookies.
 - Hamster: este actúa como un proxy transparente, basándose en las cookies o resultados capturados por Ferret.
- Las dos herramientas trabajan en conjunto.
- Observación:
 - Ferret está diseñado para tarjetas inalámbricas

Lámina 94 Dr. Roberto Gómez Cárdenas



Configurando el browser

C:\Archivos de programa\Mozilla Firefox\>set MOZ_NO_REMOTE=1
 C:\Archivos de programa\Mozilla Firefox\>Firefox -p

Firefox - Escoja perfil de usuario

Firefox guarda información sobre su configuración, preferencias y otros elementos en su perfil de usuario.

Trabajar sin conexión
 No preguntar al inicio

Configuración de conexión

Configurar proxies para el acceso a Internet

Conexión directa a Internet
 Autodetectar configuración del proxy para esta red
 Configuración manual del proxy

Proxy HTTP: 127.0.0.1 Puerto: 3128
 Usar el mismo proxy para todo

Proxy SSL: Puerto: 0
 Proxy ETP: Puerto: 0
 Proxy gopher: Puerto: 0
 Servidor SOCKS: Puerto: 0

SOCKS v4 SOCKS v5

No usar proxy para: localhost, 127.0.0.1
Ejemplo: mozilla.org, .net.nz

URL para la configuración automática del proxy:

Lámina 95

Dr. Roberto Gómez Cárdenas



Ferret

- Viendo los adaptadores
 - C:\Sidejacking\>ferret -w
- Suponiendo que se elige el i2
 - C:\Sidejacking\>Start ferret -i2

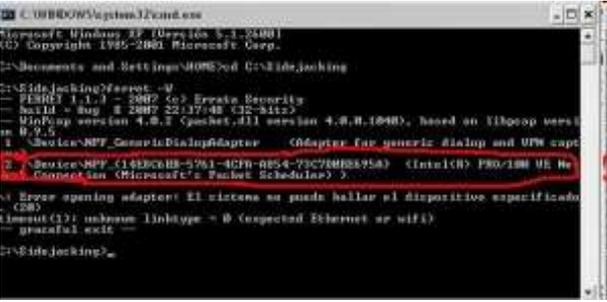


Lámina 96

Dr. Roberto Gómez Cárdenas



Accediendo a una cuenta

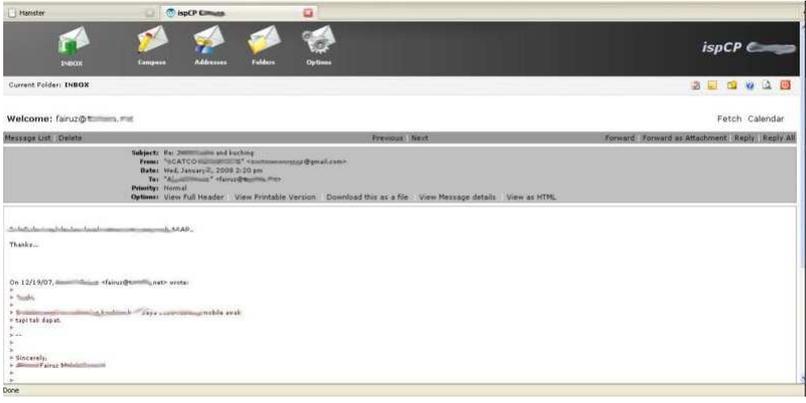


Lámina 99

Dr. Roberto Gómez Cárdenas



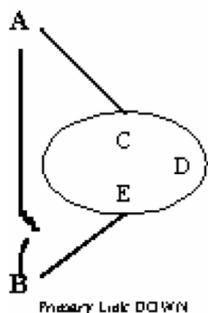
Source routing

- Opción IP: Source Routing
- Permite al host emisor especifique la ruta que el receptor debe usar para responderle.
- Un atacante puede tomar ventaja de esto especificando que una ruta no incluya al host real y que redirija la respuesta a una ruta que pueda monitorear (e.g. a sí mismo o una subred local).
- Ruteadores modernos tiran paquetes que traigan la opción habilitada.

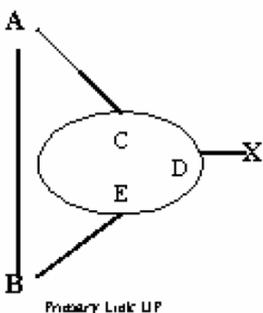
Lámina 100

Dr. Roberto Gómez Cárdenas


Esquema ataque source routing



Primary Link DOWN



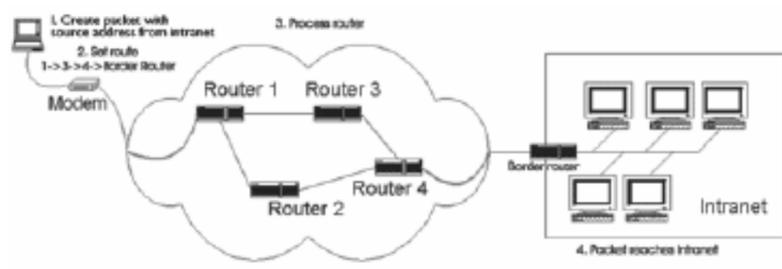
Primary Link UP

Legitimate:
B → A "reply via C,D,E"

Source Routing Attack:
B(X) → A "reply via C,D,X"

Lámina 101 Dr. Roberto Gómez Cárdenas


Otro esquema source routing



Un sistema fuera de la intranet puede hacerse pasar por un sistema dentro de la Internet usando este métodos, de tal forma que un ruteador mal implementado pueda Redirir el paquete no ruteable al destino sin detectar la direccion fuente spofeada.

Lámina 102 Dr. Roberto Gómez Cárdenas



Análisis de tráfico

- Terminó en inglés: Traffic Analysis
- El análisis de tráfico es una técnica complicada para inferir posibles sucesos a partir de la cantidad de información que circula en uno o varios segmentos de red.
- No es necesario que la información circule “en claro”.
- Usada por los americanos durante el inicio de la segunda guerra mundial

Lámina 103

Dr. Roberto Gómez Cárdenas



Replay Attacks

- Alicia autoriza una transferencia de fondos de una cuenta a otra
 - encripta la petición de transferencia con una llave de firma que solo ella conoce
 - envía petición a una máquina que verifica la firma y lleva a cabo la transacción
- Un intruso, Eva, desea contar con la misma transacción repetida sin la autorización de Ana
 - no necesita producir la petición encriptada por ella misma
 - asumiendo que puede adivinar o deducir que mensaje corresponde a la transferencia solo necesita tomar el mensaje y enviarlo después

Lámina 104

Dr. Roberto Gómez Cárdenas



Generalizando

- En general se asume “replay” o “repetición”
 - capturar un mensaje o una parte de un mensaje que es usado tiempo después
- Esto incluye los dos casos
 - el mensaje pasa sin impedimento alguno
 - el mensaje es verificado para que pueda pasar
- Es bueno preocuparse por este tipo de ataques.
 - aparte de contar con un buen algoritmo de encriptación

Lámina 105

Dr. Roberto Gómez Cárdenas



Protección perimetral

Definiendo y protegiendo el fuerte

Lámina 106

Dr. Roberto Gómez Cárdenas



¿Qué es el perímetro?

- Es una frontera fortificada que puede incluir lo siguiente
 - Ruteadores
 - Firewalls
 - IDSs
 - Dispositivos VPNs
 - Software
 - DMZs y subredes screened

Lámina 107 Dr. Roberto Gómez Cárdenas



Los principales 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 108 Dr. Roberto Gómez Cárdenas

 **Filtrado de información**



Lámina 109 Dr. 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.

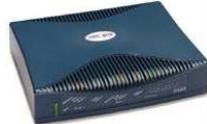
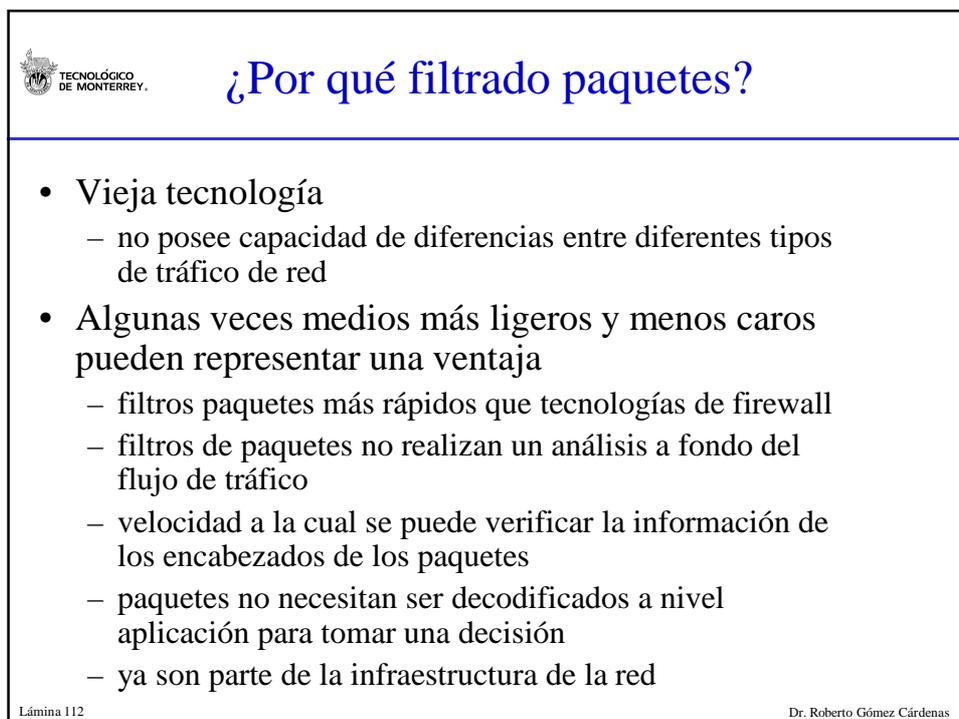
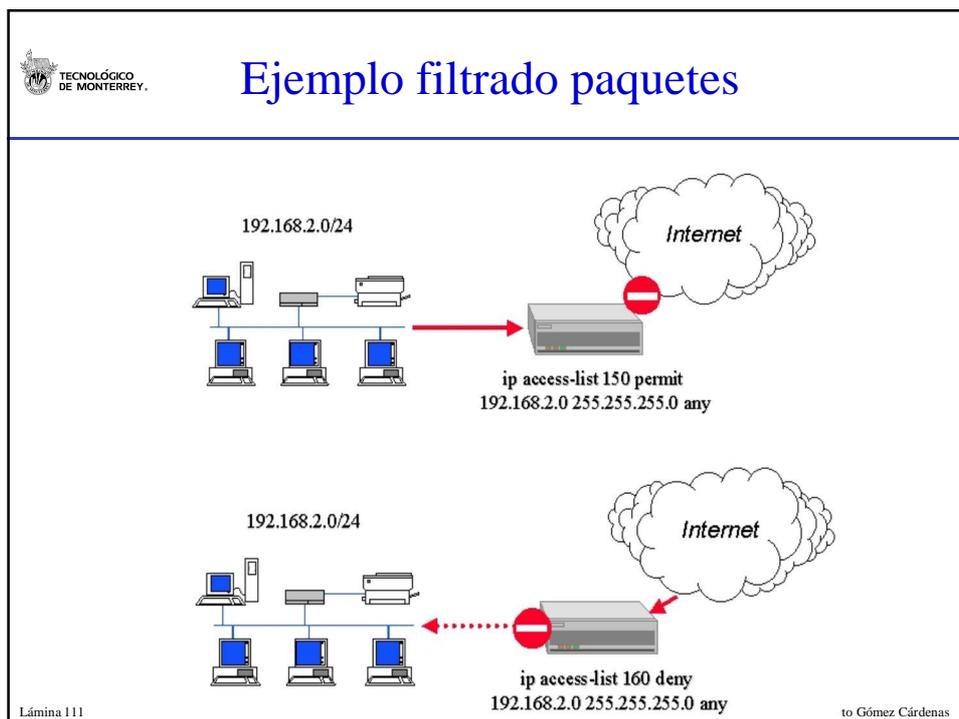


Lámina 110





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 113 Dr. 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 114 Dr. 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 115 Dr. 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 116 Dr. Roberto Gómez Cárdenas



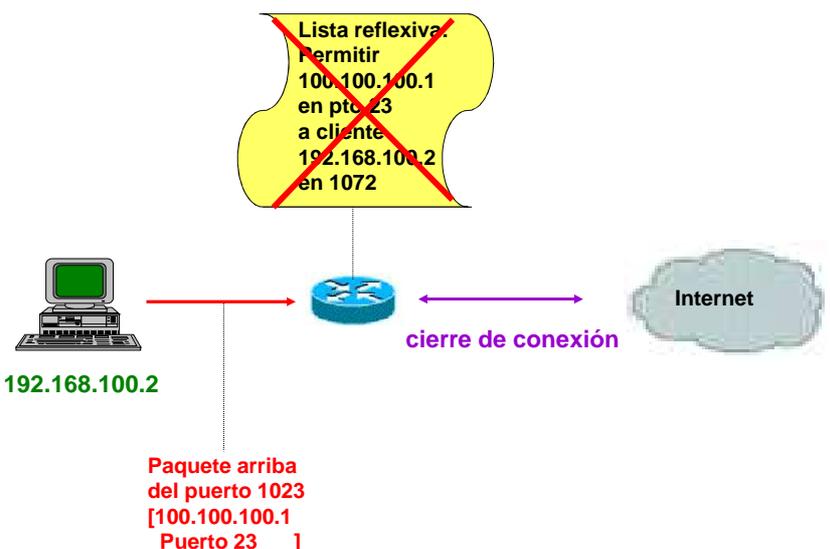
ACL reflexivas

- 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 117
Dr. Roberto Gómez Cárdenas



Ejemplo ACL reflexiva



Lista reflexiva
~~Permitir
 100.100.100.1
 en pto 23
 a cliente
 192.168.100.2
 en 1072~~

192.168.100.2

Paquete arriba
 del puerto 1023
 [100.100.100.1
 Puerto 23]

Internet

cierre de conexión

Lámina 118
Dr. 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 proxye.
- 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

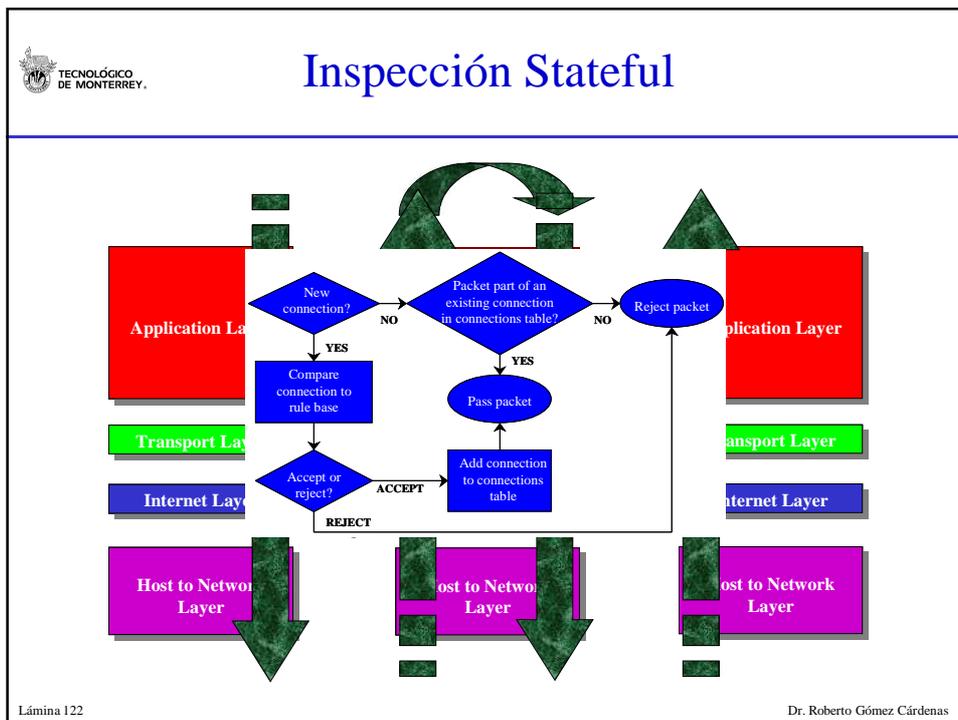
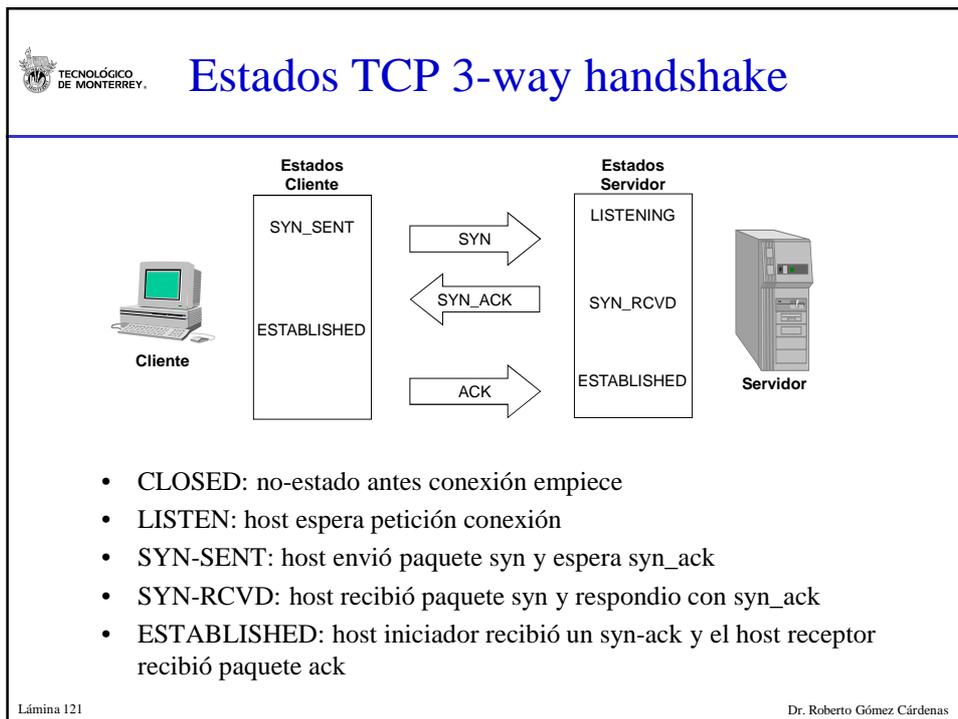
Lámina 119 Dr. Roberto Gómez Cárdenas



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 120 Dr. Roberto Gómez Cárdenas



TECNOLÓGICO DE MONTERREY.

Ejemplos firewall statefull

Web Server Firewall Allow only http - tcp 80

PC Firewall Only allows reply packets for requests made out Blocks other unregistered traffic

Client 192.168.51.50 Server 172.16.3.4

Dynamic Packet Filter

Filter remembers this information

Matches outgoing, so allowed in

No match, so not allowed in

SP = source port
SA = source address
DP = destination port
DA = destination address

Funcionamiento con protocolos orientados conexión

Funcionamiento con protocolos orientados no conexión

Lámina 123

Dr. Roberto Gómez Cárdenas

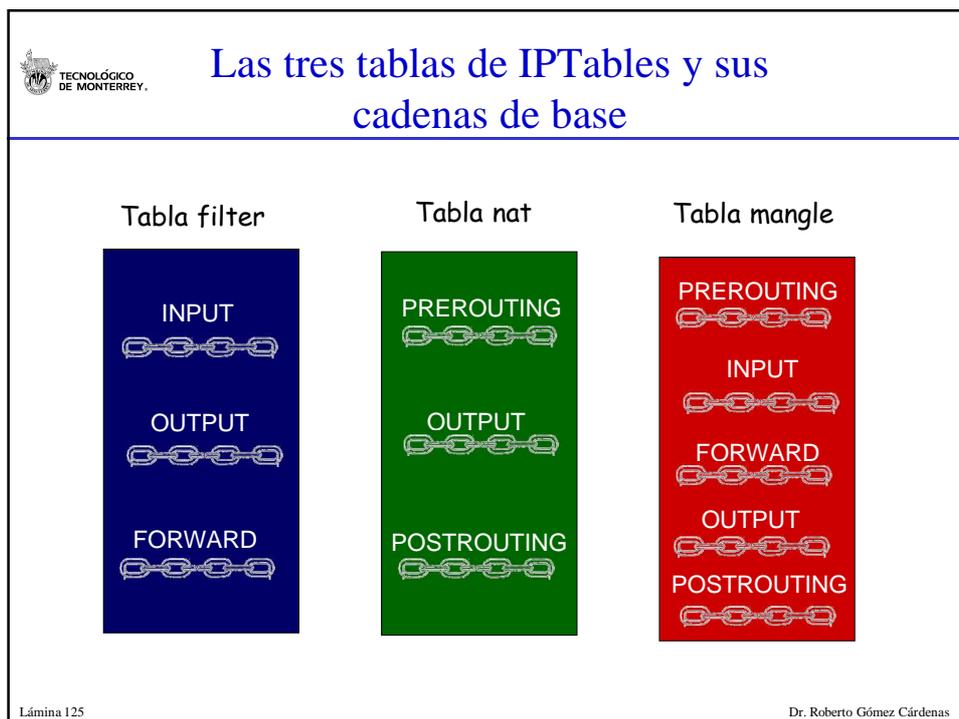
TECNOLÓGICO DE MONTERREY.

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 tráfico se deben seguir.
 - cuando empieza conexión con protocolos IPTables añade una entrada de estado para la conexión en cuestión

Lámina 124

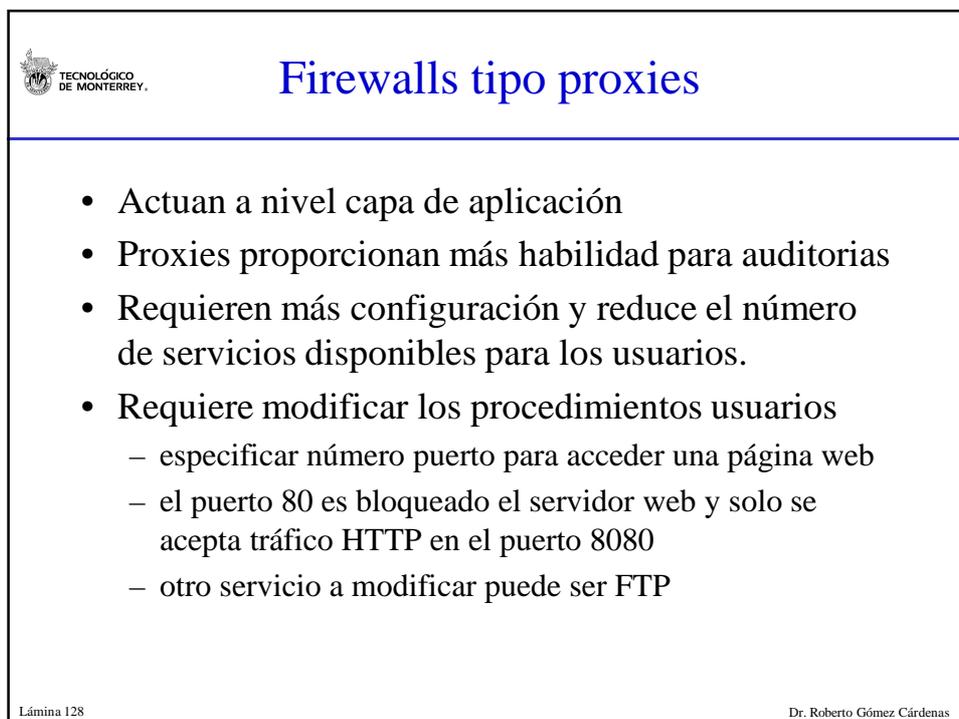
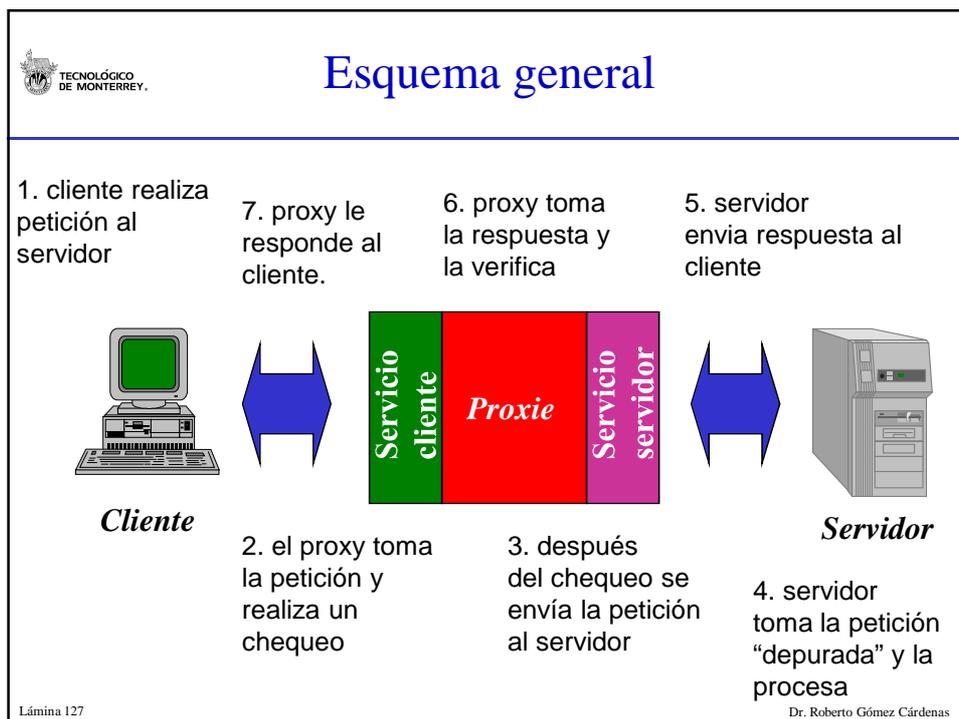
Dr. Roberto Gómez Cárdenas




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 126 Dr. 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 129 Dr. Roberto Gómez Cárdenas



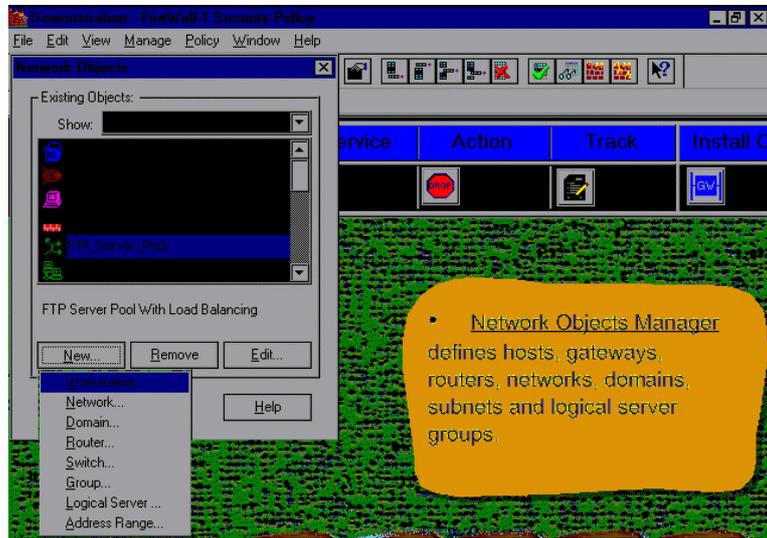
Chequeo paquetes en Checkpoint

- 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 escrutinio 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 130 Dr. Roberto Gómez Cárdenas



Los objetos de Checkpoint



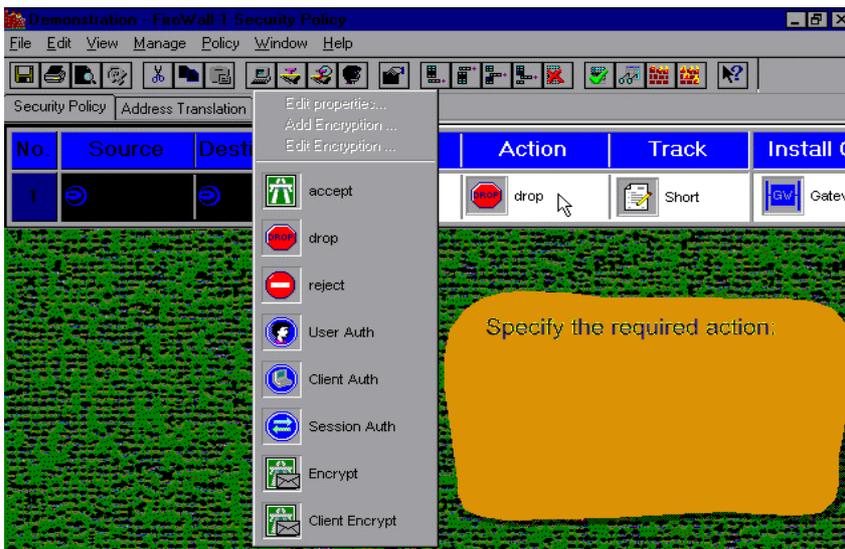
• Network Objects Manager defines hosts, gateways, routers, networks, domains, subnets and logical server groups.

Lámina 131

Dr. Roberto Gómez Cárdenas



Las acciones en Checkpoint



Specify the required action:

Lámina 132

Dr. Roberto Gómez Cárdenas



Ejemplos reglas

No.	Source	Destination	Service	Action	Track	Install C
1	Any	Web_Server	http	accept	Short	GV Gatew
2	Local_Net	Any	Any	accept	Short	GV Gatew
3	Any	Any	Any	drop	Alert	GV Gatew

With three simple rules, you have implemented access control for your network.

Lámina 133

Dr. Roberto Gómez Cárdenas



Autenticación en Checkpoint

Authentication Scheme: RADIUS

- Undefined
- S/Key
- SecurID
- FireWall-1 Password
- OS Password
- RADIUS
- AssureNet Pathways Delender
- RADIUS_SERVER

FireWall-1's open platform supports numerous authentication schemes, including SecurID cards and the industry-standard RADIUS protocol.

Lámina 134

Dr. Roberto Gómez Cárdenas



Encriptación en Checkpoint

No.	Source	Destination	Service	Action	Track	Insta
1	Any	Web_Server	http	accept	Short	[GW]
2	Sales@Any	SQL_Server	sqlnet2	Session Auth	Long	[GW]
3	Local_Net Remote_Net	Remote_Net Local_Net	Encrypted_Services	Encrypt	Long	[GW]
4	Local_Net	Any	Any			
5	Any	Any	Any			

The VPN between the corporate network and the remote office is specified by choosing the local and remote network as the source and destination criteria... and selecting the encryption action.

Lámina 135

Dr. Roberto Gómez Cárdenas



NAT en Checkpoint

No.	Original Packet			Translated Packet	
	Source	Destination	Service	Source	Destination
Address Translation is part of the object definition process in Firewall-1.					

Lámina 136

Dr. Roberto Gómez Cárdenas

Balaceo de carga en checkpoint

FireWall-1 can distribute client requests using one of the five predefined load balancing algorithms.

Lámina 137 Dr. Roberto Gómez Cárdenas

Ejemplo bitácoras generadas por checkpoint

Log shows the complete logging history of the Firewall.

No	Time	Inter.	Type	Action	Servi.	Proto.	Rule	SrcKeyID
9137	5:17:12	daemon	log	encrypt	http	tcp	11	f60c2d90c
9138				reject	ident	tcp	22	
9139				encrypt	http	tcp	11	f60c2d90c
9140				encrypt	ident	tcp	11	932b6f113
9141				encrypt	http	tcp	11	f60c2d90c
9142				encrypt	ident	tcp	11	932b6f113
9143				encrypt	http	tcp	11	f60c2d90c
9144				encrypt	http	tcp	11	f60c2d90c
9145				encrypt	http	tcp	11	f60c2d90c
9146				reject	ident	tcp	22	
9147	5:21:46	le0	log	accept	smtp	tcp	23	
9148	5:17:17	qe2	log	accept	smtp	tcp	23	
9149	5:21:47	le0	log	accept	smtp	tcp	23	
9150	5:17:19	daemon	log	encrypt	smtp	tcp	6	f60c2d90c
9151	5:21:49	le0	log	accept	smtp	tcp	23	
9152	5:24:35	daemon	log	decrypt	smtp	tcp	6	f60c2d90c
9153	5:21:49	daemon						

Lámina 138 Dr. Roberto Gómez Cárdenas



Ventajas/Desventajas Firewalls Proxy

- **Ventajas**
 - 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.

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

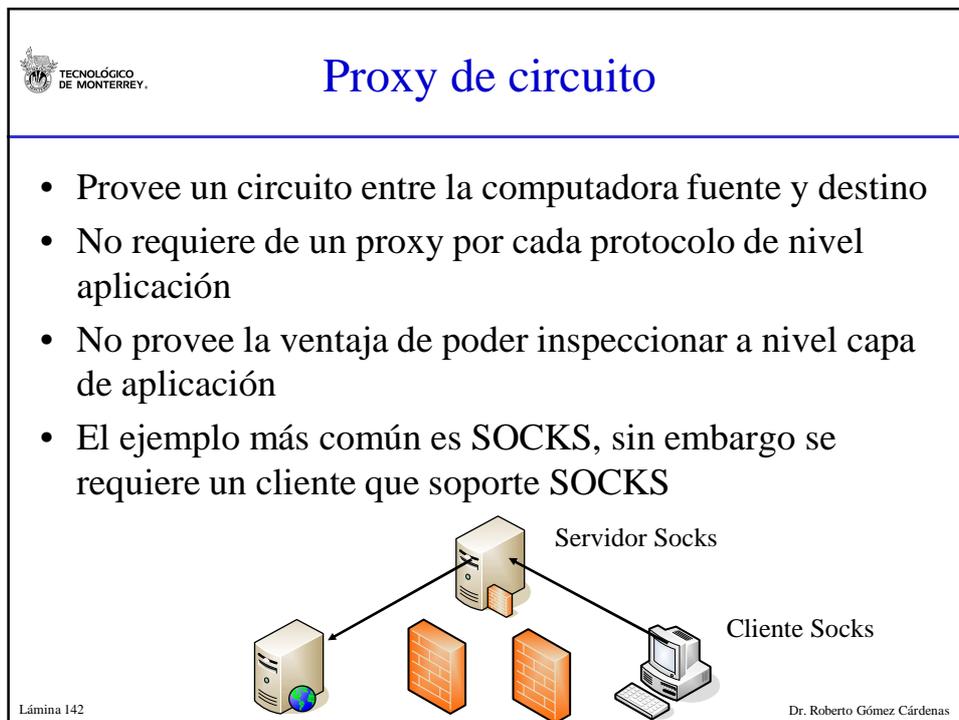
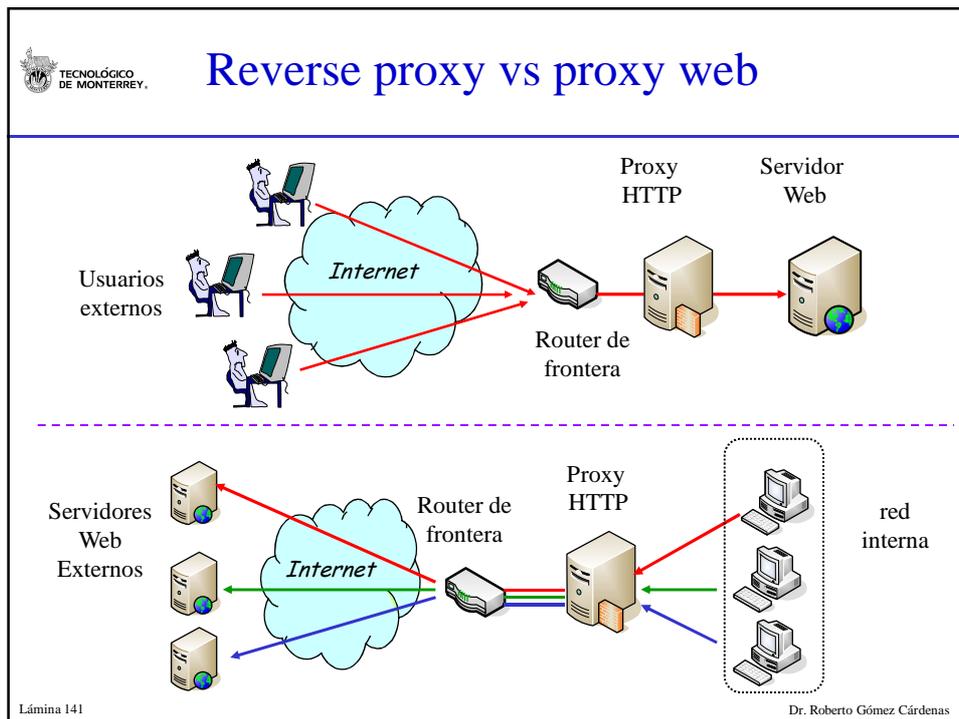
Lámina 139 Dr. Roberto Gómez Cárdenas



Reverse proxy

- Mismo principio que un proxy, excepto que en lugar de entregar páginas a usuarios internos, las entrega a usuarios externos.
- Puede ser usado para encargarse de alguna carga de los servidores web y proporcionar una capa adicional de protección.
- Posible aplicación: servidor con información sensible
 - configurar proxy afuera firewall como si fuera el propio servidor web
 - cuando clientes externos intentan acceder al servidor son dirigidos al proxy
 - contenido real reside en el servidor real más seguro atrás del firewall

Lámina 140 Dr. 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.

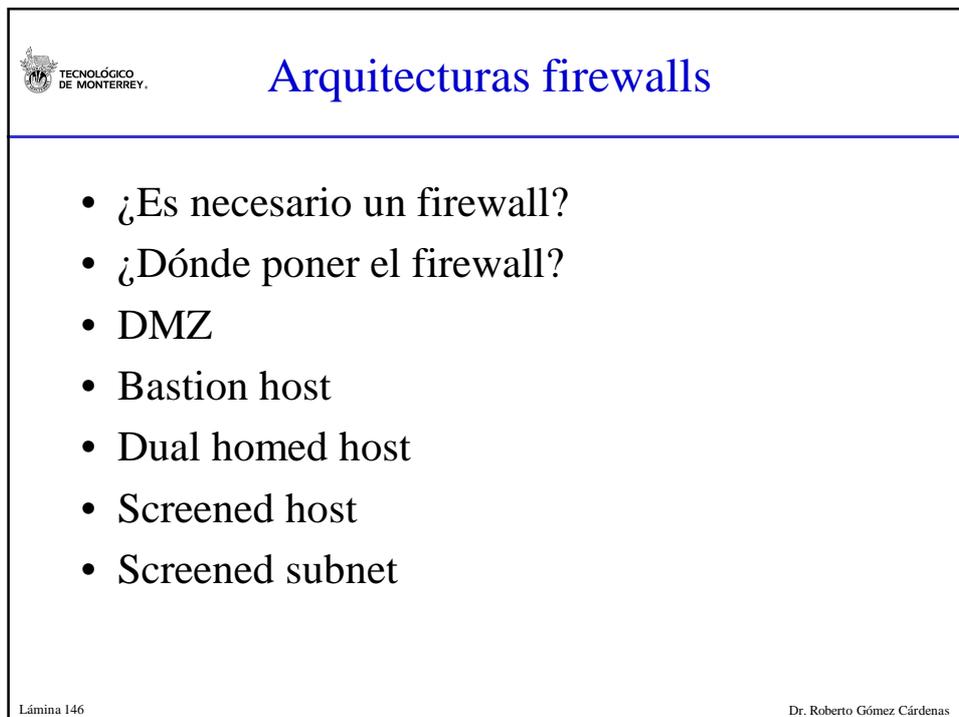
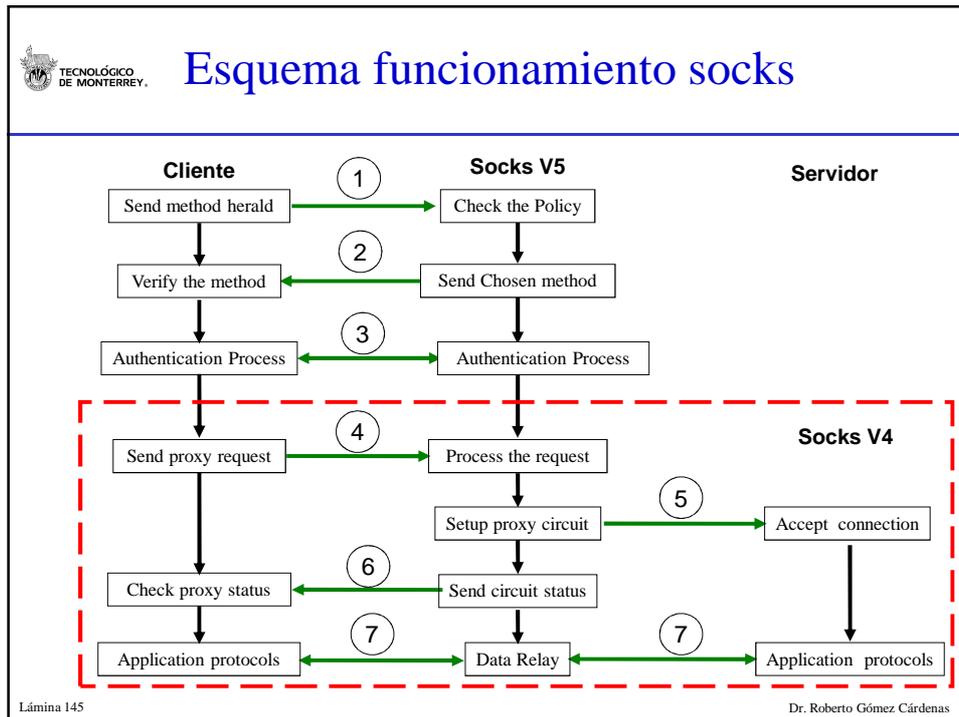
Lámina 143 Dr. Roberto Gómez Cárdenas

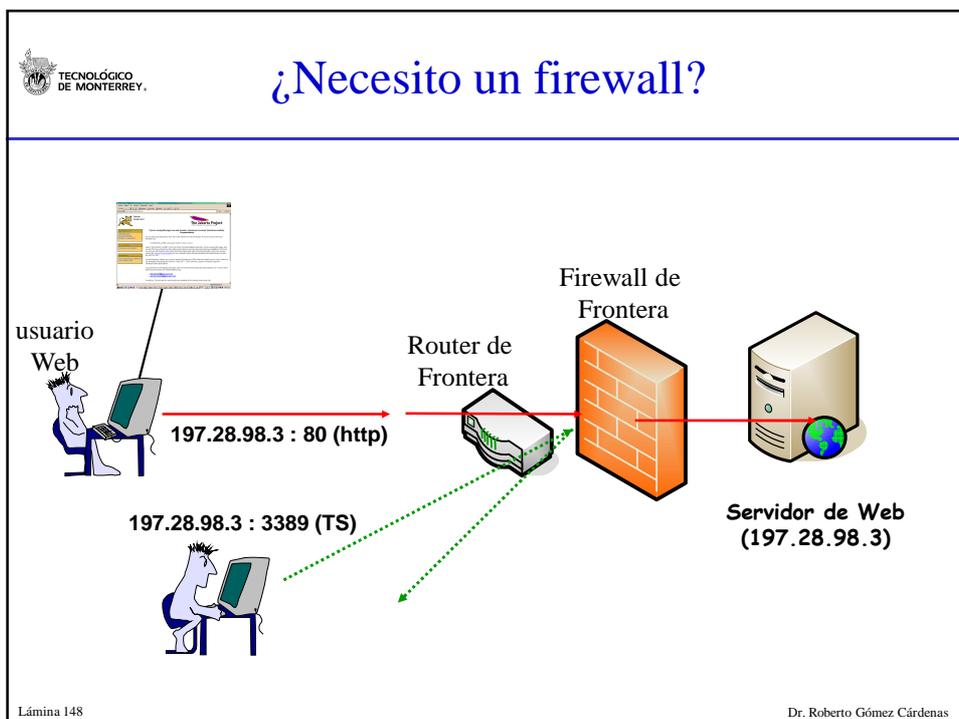
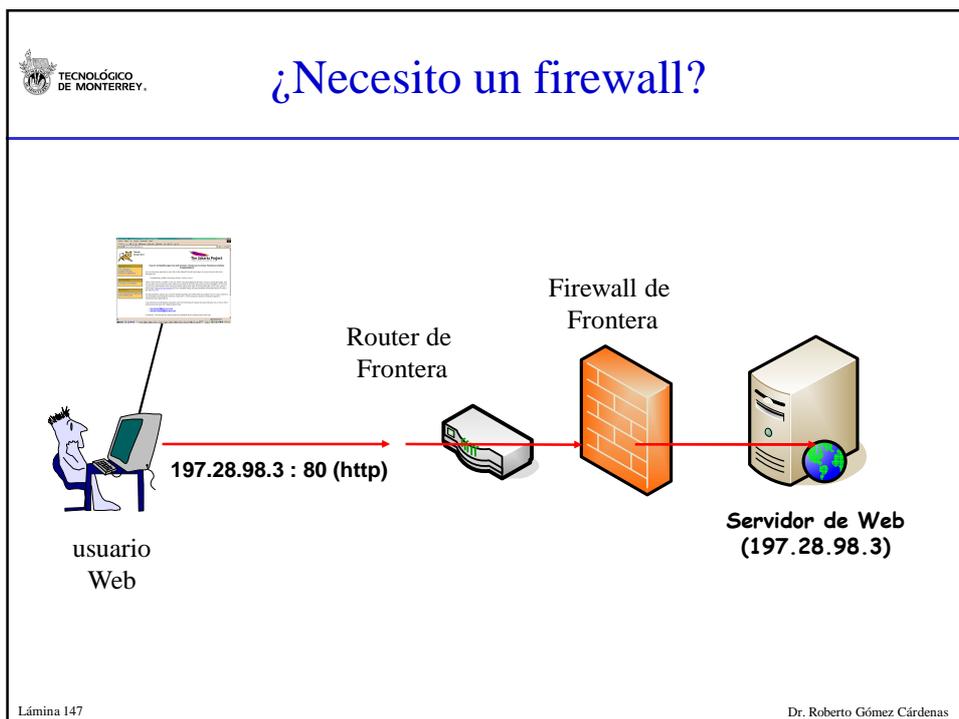


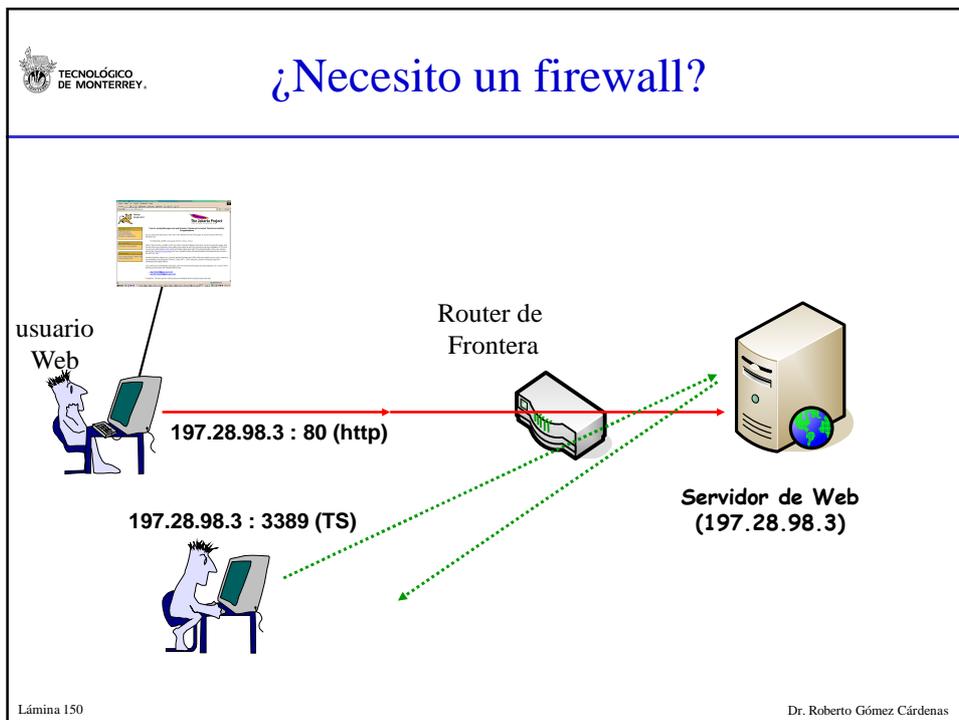
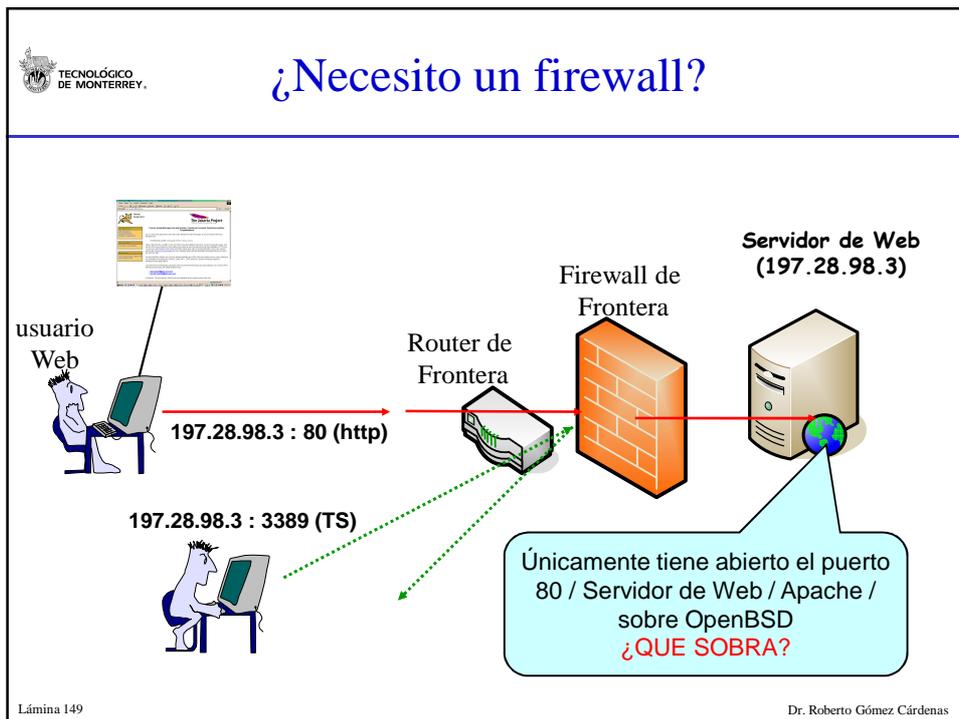
Características socks

- 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 144 Dr. Roberto Gómez Cárdenas









¿Es esto el mundo real?

- Pero hoy día es poco probable encontrarnos una Compañía que solo requiera un servidor de web. Sin embargo, este ejemplo nos deja ver claramente cual es la funcionalidad de un firewall.
- Pasemos a un ejemplo con una arquitectura más compleja

Lámina 151

Dr. Roberto Gómez Cárdenas



Un ambiente más real

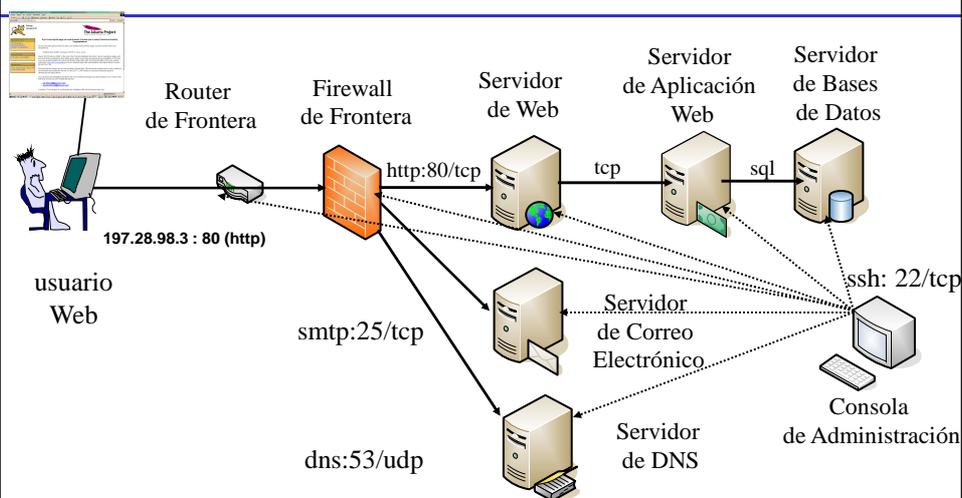
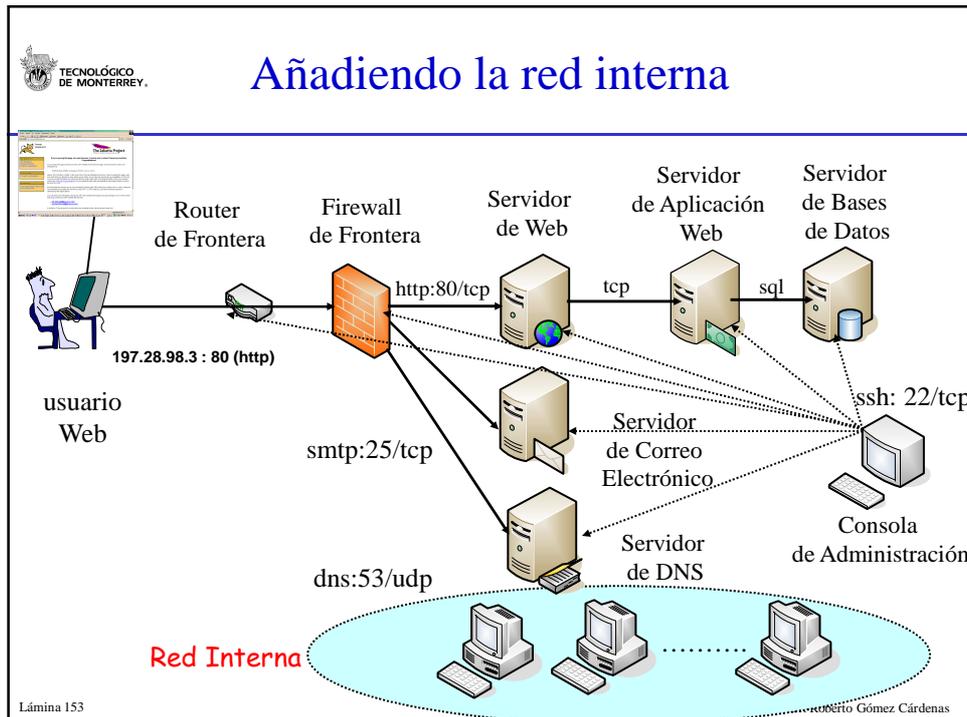


Lámina 152

Dr. Roberto Gómez Cárdenas



TECNOLÓGICO DE MONTERREY.

¿Y si falla?

- Lo que empezó con un simple router, firewall y servidor de web se complicó de manera importante.
- Adicionalmente, el esquema anterior solo está protegiendo la red interna del exterior (Internet), **pero no está protegiendo a los servidores críticos de la red interna.**
- ¿Qué pasaría, con el esquema anterior, si un atacante logra tomar control de servidor de correo electrónico?

Lámina 154

Dr. Roberto Gómez Cárdenas


Defense in Depth

- Proveer a nuestra estrategia de seguridad de varios niveles de seguridad de tal manera que si uno falla, podremos contener el ataque y contaremos con un siguiente nivel de protección.

Internet



Zona A



Zona B

Ataque exitoso

Internet



Zona A



Zona B

Zona A comprometida, pero no Zona B

Lámina 155 Dr. Roberto Gómez Cárdenas


Aplicando concepto a nuestro esquema

Base de Datos – Transacciones en línea



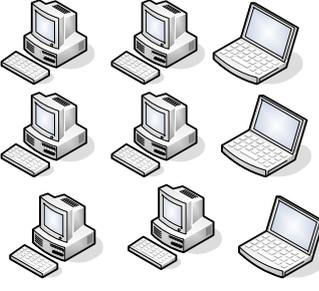
Dividiendo zonas por la criticidad y sensibilidad de la información contenida en ellas

Internet

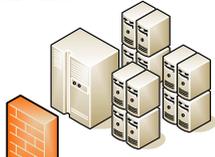




DMZ



LAN

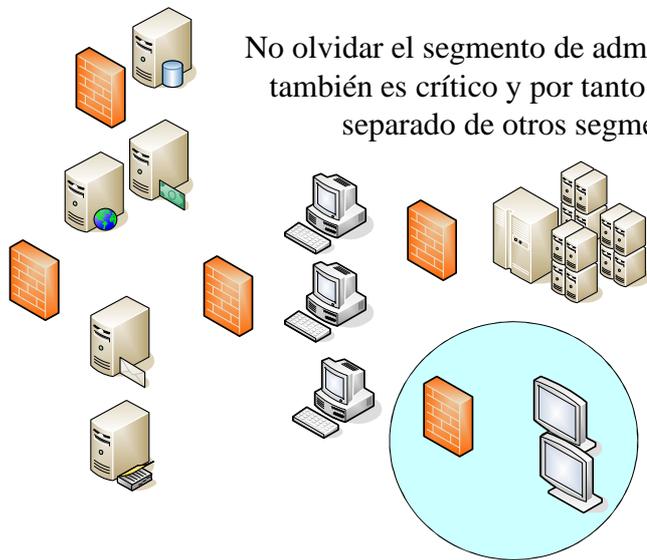


SERVIDORES CRITICOS

Lámina 156 Dr. Roberto Gómez Cárdenas



¿Y el segmento de administración?



No olvidar el segmento de administración – también es crítico y por tanto debe estar separado de otros segmentos

Lámina 157 Dr. Roberto Gómez Cárdenas



Bastion host

- Comúnmente un sistema fuertemente endurecido,
- No tiene servicios innecesarios activos, no tiene binarios innecesarios, vulnerabilidades parchadas, cuentas de usuario reducidas al mínimo, no tiene puertos TCP/UDP innecesarios, en ocasiones no tiene ningún puerto TCP/UDP activo.
- Son utilizados como base para instalación de firewalls, detectores de intrusos, servidores expuestos (dns, smtp, pop3, http, etc.)

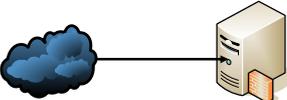


Lámina 158 Dr. Roberto Gómez Cárdenas



Dual homed hosts

- Dual homed gateway
 - bastion host con un sistema con dos interfaces de red
 - una de ellas protege la red interna
 - la otra para la red externa
 - soporta uno o más protocolos de internet

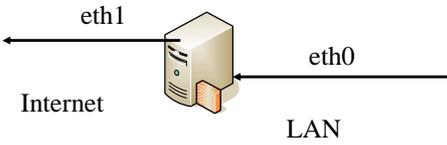


Lámina 159
Dr. Roberto Gómez Cárdenas



Screened Host

- El router solo puede enviar tráfico al Bastion-Host no puede enviar tráfico a los demás equipos.
- El Bastion-Host se encargará de realizar una tarea de filtrado adicional a la ya realizada por el router, doble línea de defensa – tanto router de frontera como bastion host.
- Esquema utilizado para redes pequeñas que no requieren dar servicios públicos hacia Internet

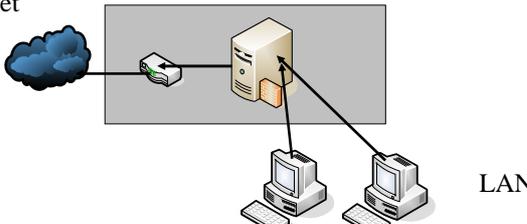
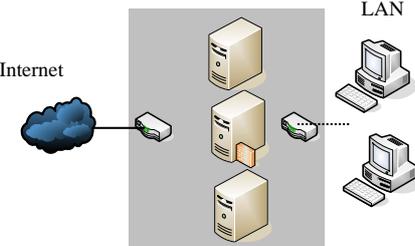


Lámina 160
Dr. Roberto Gómez Cárdenas



Screened Subnet



- Esquema muy utilizado cuando el presupuesto es bajo pero se requieren tener sistemas expuestos a Internet para dar servicios públicos como servidores de web, correo electrónico, etc.
- Su nivel de seguridad es medio
- No es muy recomendable para protección de infraestructuras críticas.
- La ventaja es que provee un segundo router que bien configurado puede contener ataques hacia el interior de la red LAN.

Lámina 161

Dr. Roberto Gómez Cárdenas

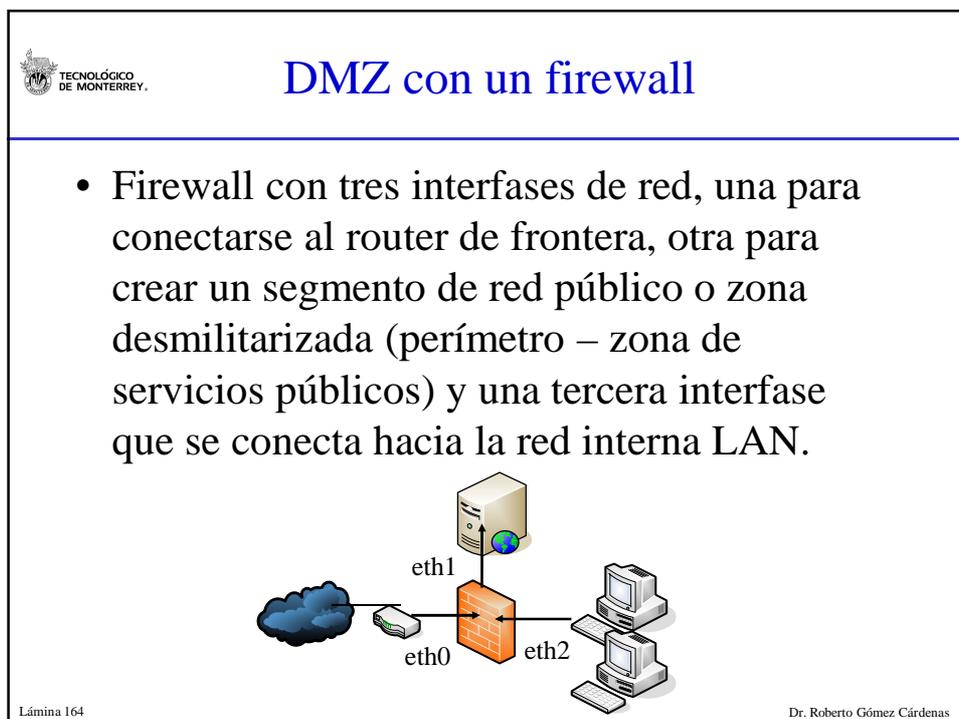
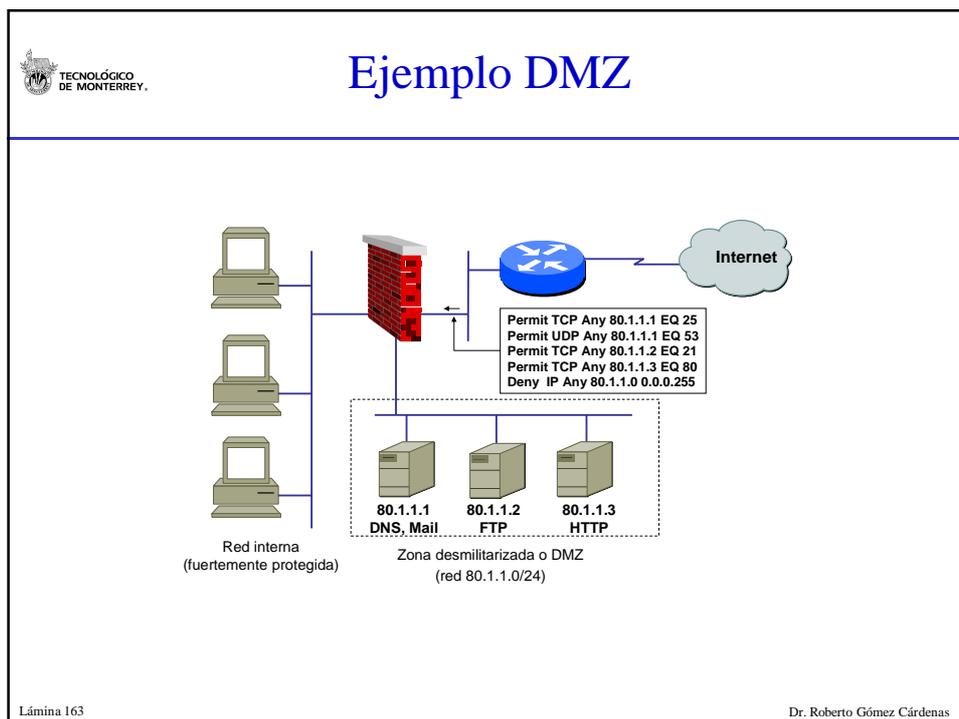


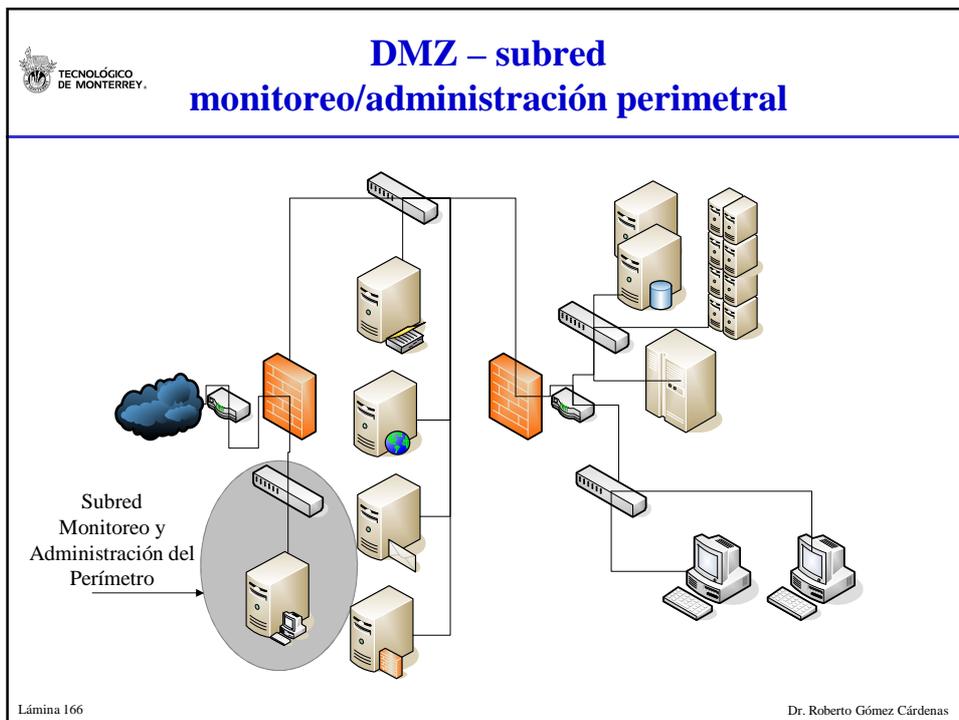
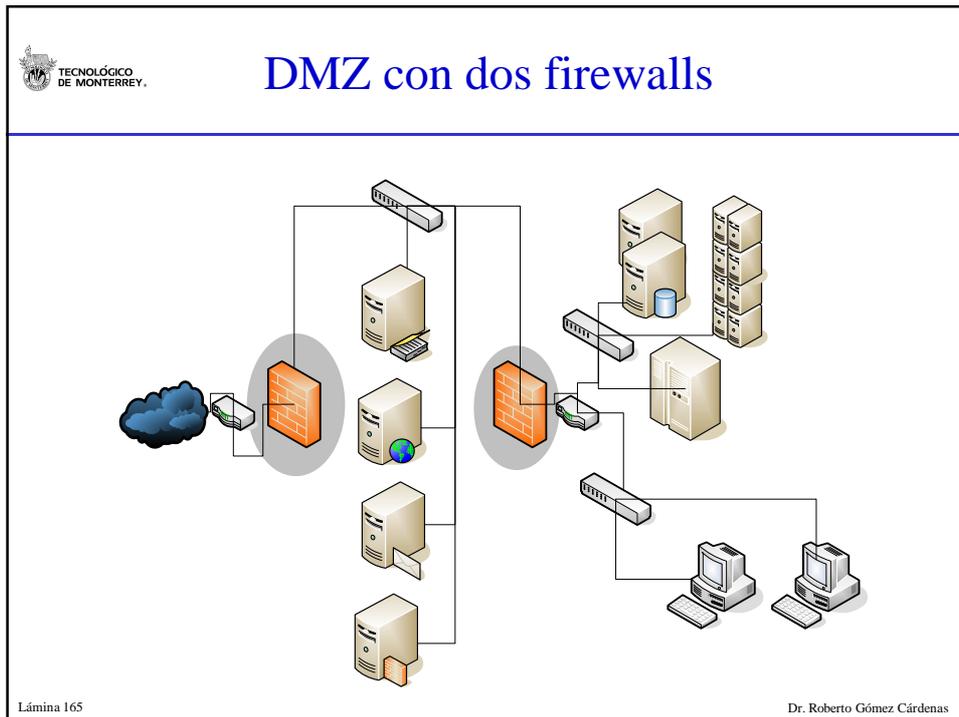
DMZ

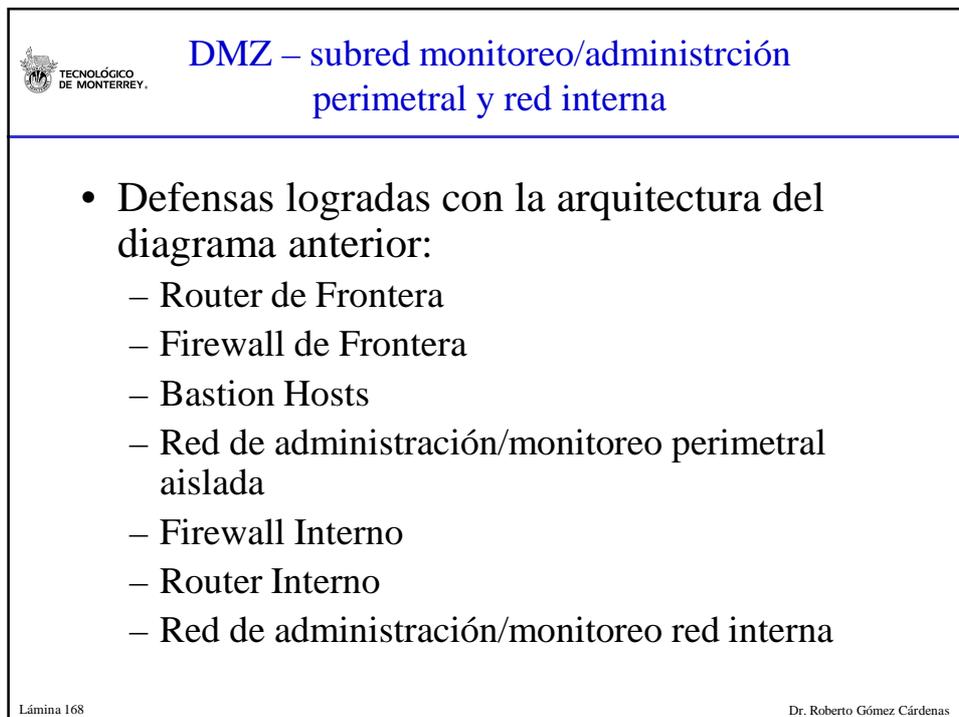
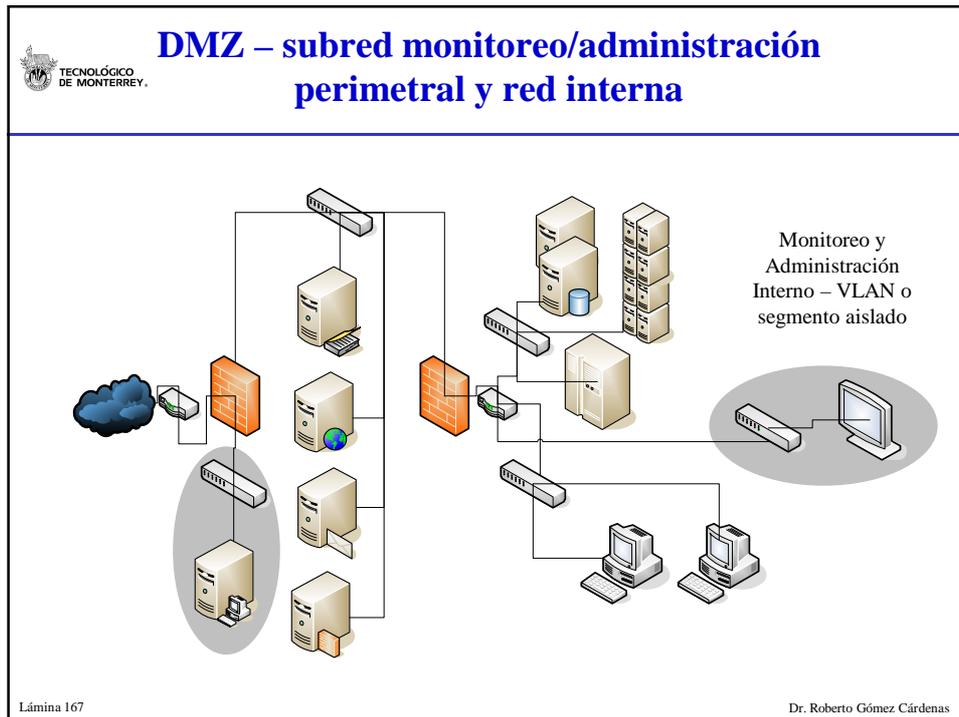
- **DMZ: Zona Desmilitarizada**
 - termino guerra Corea
 - área insegura entre áreas seguras
 - aplicado a hosts localizados fuera del firewall
- Normalmente la red de una empresa tiene un conjunto de servidores que deben estar accesibles desde el exterior, por ejemplo servidor Web, FTP, etc.
- Hacen referencia a una pequeña red que contiene servicios públicos conectados directamente a una protección ofrecida por el firewall o cualquier dispositivo de filtrado.

Lámina 162

Dr. Roberto Gómez Cárdenas









Firewalls Personales

- Es un producto que tiene más de siete años en el mercado.
- Son instalados en computadoras personales de usuarios principiantes y expertos
- Útiles para gente que pasa horas o días conectada a internet desde su casa
- Posibilidad de que alguien robe información o que use la máquina para atacar a otros

Lámina 169

Dr. Roberto Gómez Cárdenas



Ventajas Firewalls Personales

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

Lámina 170

Dr. Roberto Gómez Cárdenas



Firewalls personales

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

Lámina 171 Dr. 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 172 Dr. 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

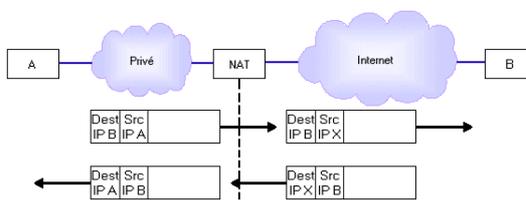


Lámina 173

 **Direcciones homologadas**

- Debido a la gran demanda de direcciones IP públicas y homologadas, (i.e. identificadas en el resto de Internet) 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 174 Dr. 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 175

Dr. Roberto Gómez Cárdenas



Ejemplo traducción NAT

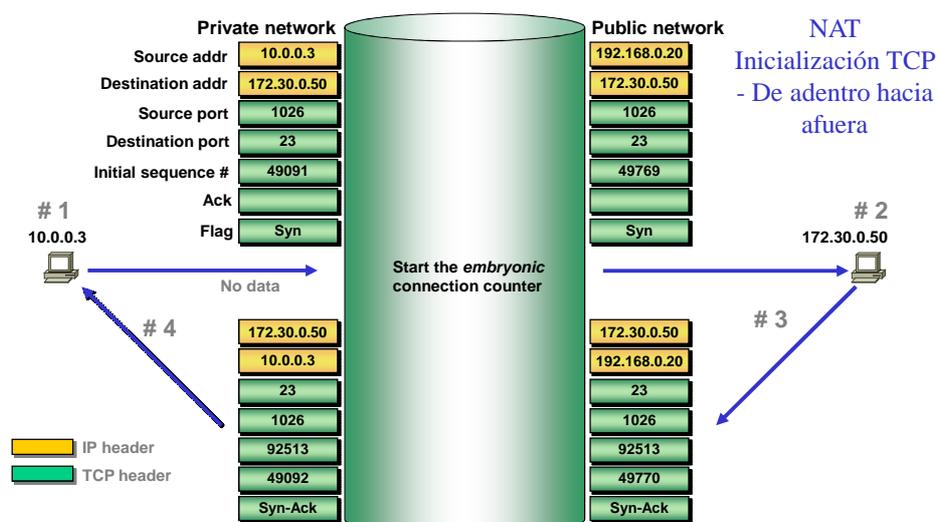


Lámina 176

Dr. Roberto Gómez Cárdenas



PAT

- También conocido como NAPT
 - o single address NAT
- Mapea varias direcciones internas en una dirección 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 “efímero” 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 177
Dr. 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/port	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 178
Dr. Roberto Gómez Cárdenas

 TECNOLÓGICO DE MONTERREY.

Transferencia de zonas

obteniendo la arquitectura de la red

Lámina 179 Dr. Roberto Gómez Cárdenas

 TECNOLÓGICO DE MONTERREY.

Transferencia de zona

- Para distribuir la carga de DNS
 - varios servidores DNS pueden usarse
 - cada uno cuenta con una copia de su respectiva zona
- Transferencia de zona
 - proceso copia zona de maestro a esclavo



Lámina 180 Dr. Roberto Gómez Cárdenas



El peligro de la transferencia de zonas

- Posible obtener información crítica obtenida mediante "transferencia de zona" de servidores DNS mal configurados.
- Algunas veces nos encontramos con servidores DNS configurados de manera insegura y que pueden permitirnos entrar en la llamada zona de transferencia de DNS, aun siendo usuarios de internet no autorizados.
- Posible intentarlo utilizando la instrucción nslookup

Lámina 181 Dr. Roberto Gómez Cárdenas



Usando nslookup

```
$ whois toto.com
Domain Name:TOTO.COM
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS1.TOTO.COM
Name Server: NS2.TOTO.COM
Status: ACTIVE
Updated Date: 08-oct-2003
Creation Date: 25-oct-1994
Expiration Date: 24-oct-2006
$ nslookup
Default Server: servidor.itesm.mx
Address: 192.12.15.2
$ server ns1.toto.com
$ set type=any
$ ls -d > listahost
$
```

Lámina 182 Dr. Roberto Gómez Cárdenas



¿Y que se hizo?

- Definir el tipo de registro como cualquiera
- (any) con lo que es posible recuperar los registros DNS disponibles.
- Luego los listamos y redirigimos a "listahost" para consultarlo mas adelante.
- Si todo funciona bien, al leer "listahost", se encontraran diversas entradas con varios registros

Lámina 183

Dr. Roberto Gómez Cárdenas



Ejemplo de información

```

> server 195.57.10.2
Default Server: sigrid.sodefesa.es
Address: 195.57.10.2
> ls sodefesa.es
[sigrid.sodefesa.es]
sodefesa.es. NS server = sigrid1.sodefesa.es
sodefesa.es. NS server = sigrid.sodefesa.es
ftp A 195.57.10.25
news A 194.179.3.124
poseidon A 195.57.10.25
private A 195.57.10.7
prometeus A 195.57.10.29
sigr1 A 195.57.10.53
sigrid A 195.57.10.2
sigrid1 A 195.57.10.3
www A 195.57.10.25
:
:

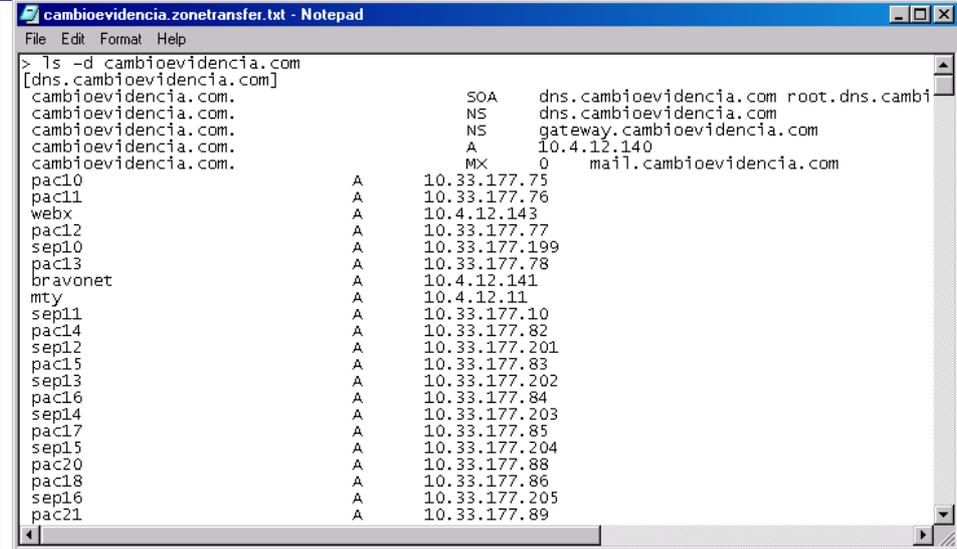
```

Lámina 184

Dr. Roberto Gómez Cárdenas

TECNOLÓGICO DE MONTERREY.

Un ultimo ejemplo



```

cambioevidencia.zonetransfer.txt - Notepad
File Edit Format Help
> ls -d cambioevidencia.com
[dns.cambioevidencia.com]
cambioevidencia.com.      SOA      dns.cambioevidencia.com root.dns.cambi
cambioevidencia.com.      NS       dns.cambioevidencia.com
cambioevidencia.com.      NS       gateway.cambioevidencia.com
cambioevidencia.com.      A       10.4.12.140
cambioevidencia.com.      MX       0      mail.cambioevidencia.com
pac10                      A       10.33.177.75
pac11                      A       10.33.177.76
webx                       A       10.4.12.143
pac12                      A       10.33.177.77
sep10                      A       10.33.177.199
pac13                      A       10.33.177.78
bravonet                   A       10.4.12.141
mty                       A       10.4.12.11
sep11                      A       10.33.177.10
pac14                      A       10.33.177.82
sep12                      A       10.33.177.201
pac15                      A       10.33.177.83
sep13                      A       10.33.177.202
pac16                      A       10.33.177.84
sep14                      A       10.33.177.203
pac17                      A       10.33.177.85
sep15                      A       10.33.177.204
pac20                      A       10.33.177.88
pac18                      A       10.33.177.86
sep16                      A       10.33.177.205
pac21                      A       10.33.177.89

```

Lámina 185 Dr. Roberto Gómez Cárdenas

TECNOLÓGICO DE MONTERREY.

Detalle sobre nslookup

- Linux RedHat 7.3
 - Note: nslookup is deprecated and may be removed from future releases. Consider using the `dig` or `host` programs instead. Run nslookup with the `-sil[ent]` option to prevent this message from appearing.
- Otras opciones y/o herramientas
 - Sam Spad
 - AXFR
 - ghba.c.
 - dig →
 - dig
 - host

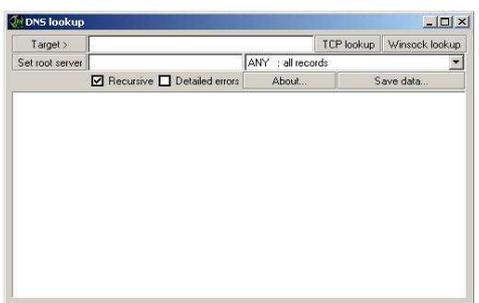


Lámina 186 Dr. Roberto Gómez Cárdenas



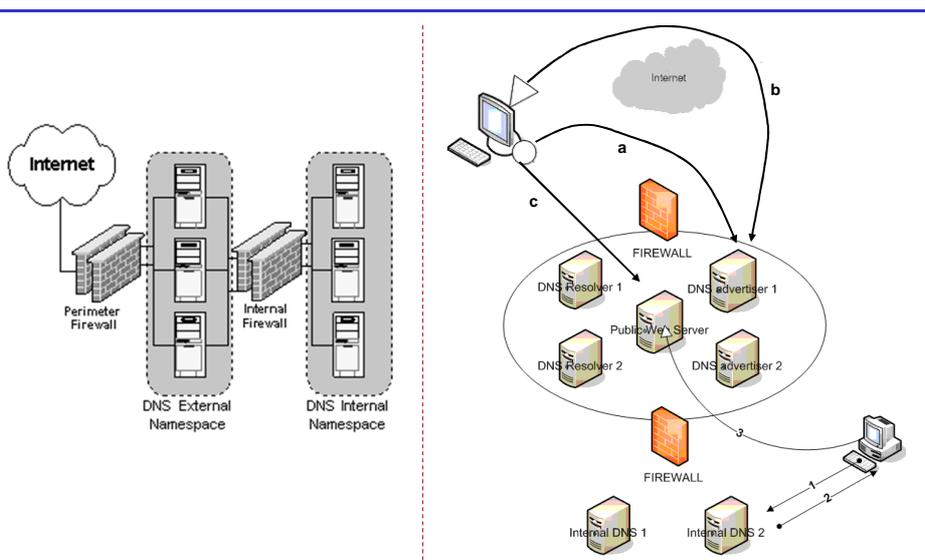
Solución: split DNS

- Problema anterior:
 - los mismos servidores DNS son usados tanto para la red interna como para la parte internet de la red
- Alternativa
 - configurar dos DNS independientes que son actualizados por separados
 - el servidor interno contiene una base de datos de de todos los nombres DNS dentro de la organización.
 - el servidor externo solo puede resolver nombres relacionados con los hosts externos (i.e. e-mail forwarders y web servers)
- Variante: Split-Split DNS Design

Lámina 187 Dr. Roberto Gómez Cárdenas



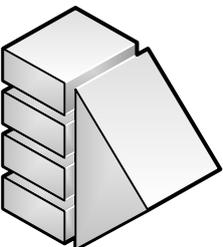
split DNS vs split-split DNS



The diagram illustrates two DNS architectures. On the left, 'split DNS' shows a network with a 'Perimeter Firewall' and an 'Internal Firewall'. The 'Perimeter Firewall' separates the 'Internet' from the 'DNS External Namespace'. The 'Internal Firewall' separates the 'DNS External Namespace' from the 'DNS Internal Namespace'. On the right, 'split-split DNS' shows a network with a 'Public Web Server', 'DNS Resolver 1', 'DNS Resolver 2', 'DNS advertiser 1', and 'DNS advertiser 2' behind a 'FIREWALL'. Below this, 'Internal DNS 1' and 'Internal DNS 2' are shown. Arrows 'a', 'b', and 'c' indicate traffic flow: 'a' from Internet to Public Web Server, 'b' from Internet to DNS advertiser 1, and 'c' from Internet to DNS Resolver 1. Arrows 1 and 2 show traffic from Internal DNS 1 and 2 to the Public Web Server.

Lámina 188 Dr. Roberto Gómez Cárdenas

 **Accesos remotos**



RADIUS y TACACS

Lámina 189 Dr. Roberto Gómez Cárdenas

 **RADIUS y TACACS**

- 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 190 Dr. Roberto Gómez Cárdenas



RADIUS

- Remote Authentication Dial-In User Service
- Sistema de autenticación y accounting usado por varios proveedores de internet (ISPs)
- Cuando un usuario se conecta a su ISP, este debe proporcionar su username y password.
- Esta información se pasa al 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

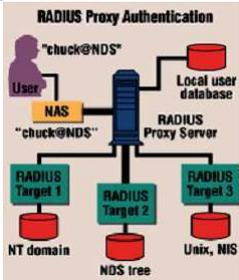


Lámina 191
Dr. Roberto Gómez Cárdenas



TACACS

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

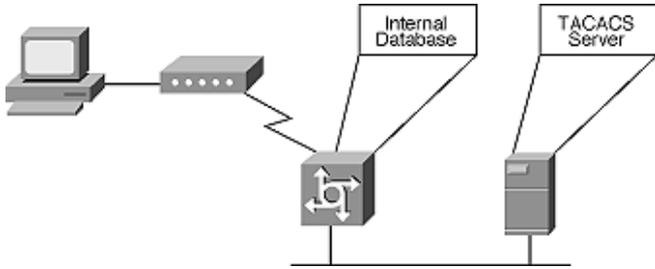


Lámina 192
Dr. Roberto Gómez Cárdenas



IDS, IPS, HONEYPOTS

- IDS: Software específicamente diseñado para reconocer los patrones de un comportamiento no deseado.
- IPS: Dispositivo (hardware o software) que tiene la habilidad de detectar ataques tanto conocidos como desconocidos y reaccionar a esos para impedir su éxito

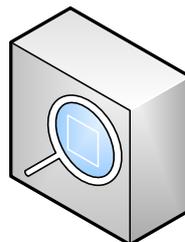


Lámina 193

Dr. Roberto Gómez Cárdenas



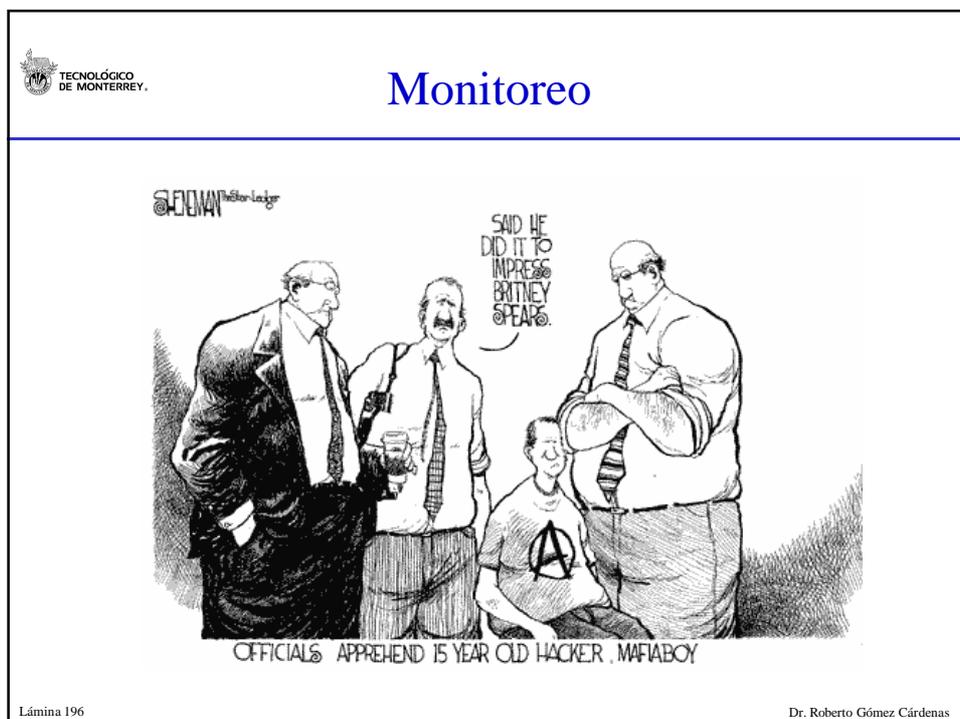
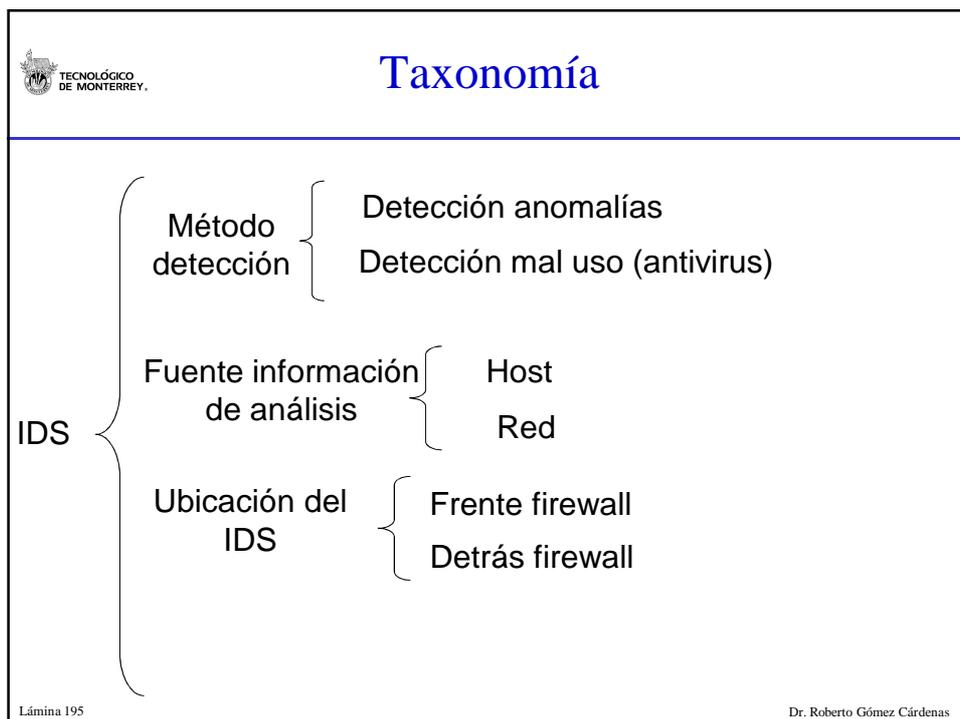
Objetivos: Exactitud

- 100% de exactitud y 0% de falsos positivos.
 - Un falso positivo ocurre cuando el sistema genera una falsa alarma.
 - O lo que es lo mismo el síndrome de Juanito y el Lobo...
 - Generar un 0% de falsos positivos es trivial:
 - No detectar nada.
 - Generar un 0% de falsos negativos es un objetivo adicional:
 - No permitir que ningún ataque pase desapercibido.



Lámina 194

Dr. Roberto Gómez Cárdenas

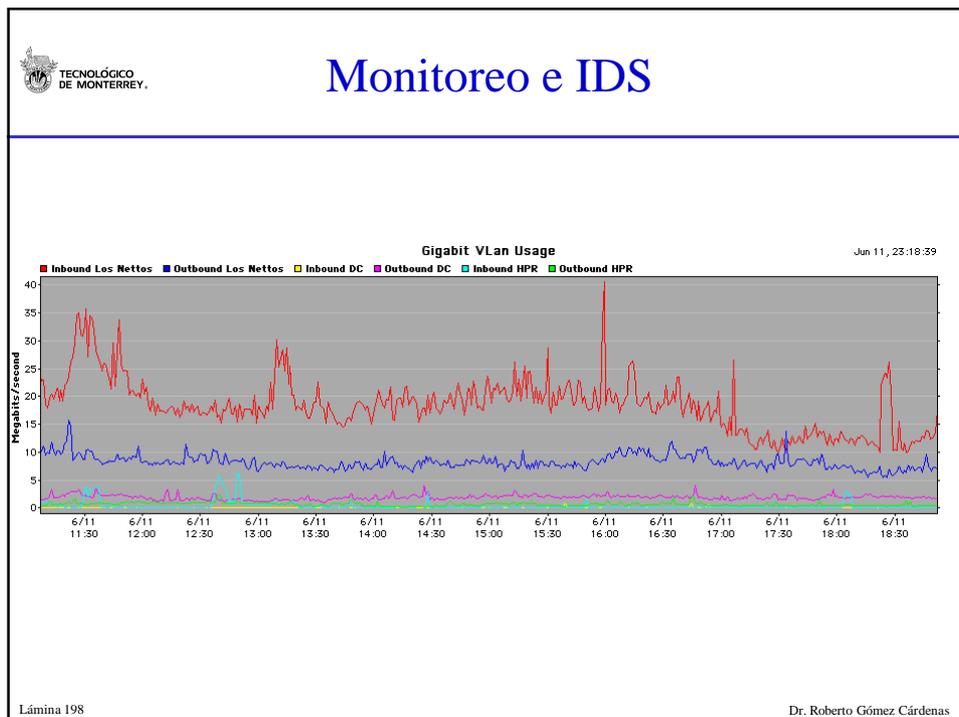




Monitoreo e IDS

- Es de suma importancia monitorear los signos vitales de nuestra red
 - Tráfico de entrada
 - Tráfico de salida
 - Tráfico interno
- Comúnmente el tráfico de una red es normalizado, es decir, tiene patrones constantes, cuando existe un pico seguramente es porque hay un problema (ej.: worms, dispositivos nuevos mal configurados, etc.)

Lámina 197
Dr. Roberto Gómez Cárdenas




Solo tengo dos IDS/Monitores
¿dónde los colocarían?

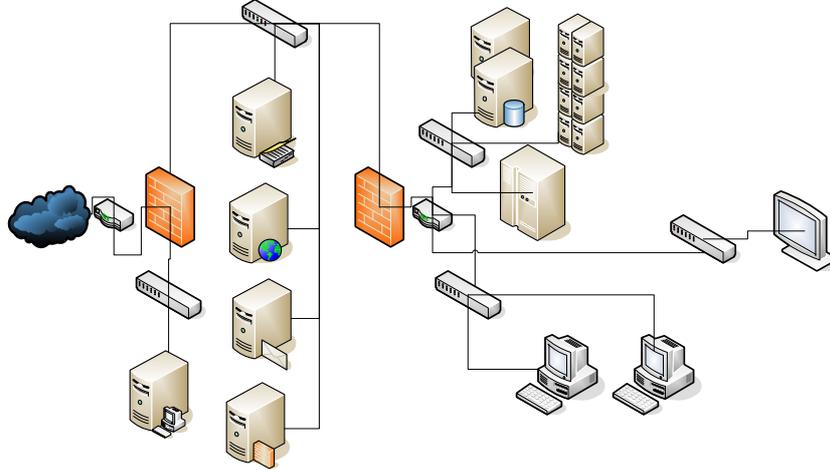


Lámina 199 Dr. Roberto Gómez Cárdenas


Una opción, pero hay muchas
dependerá del Análisis de Riesgos

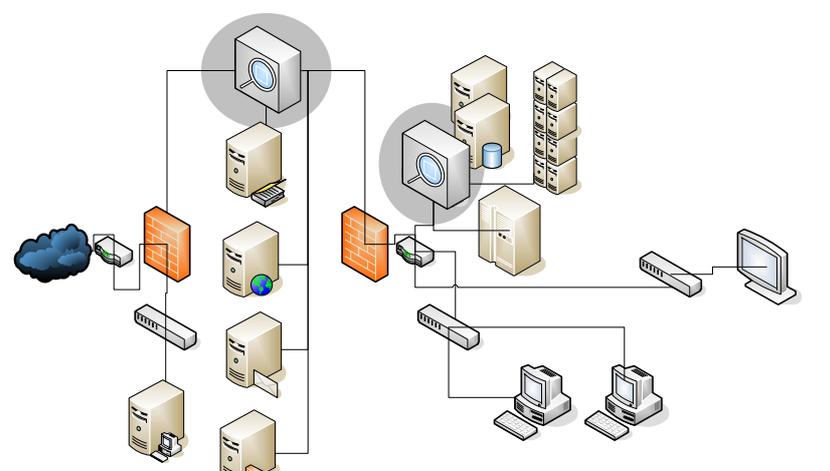


Lámina 200 Dr. Roberto Gómez Cárdenas

