Allied Telesyn Internacional

Curso de Certificación

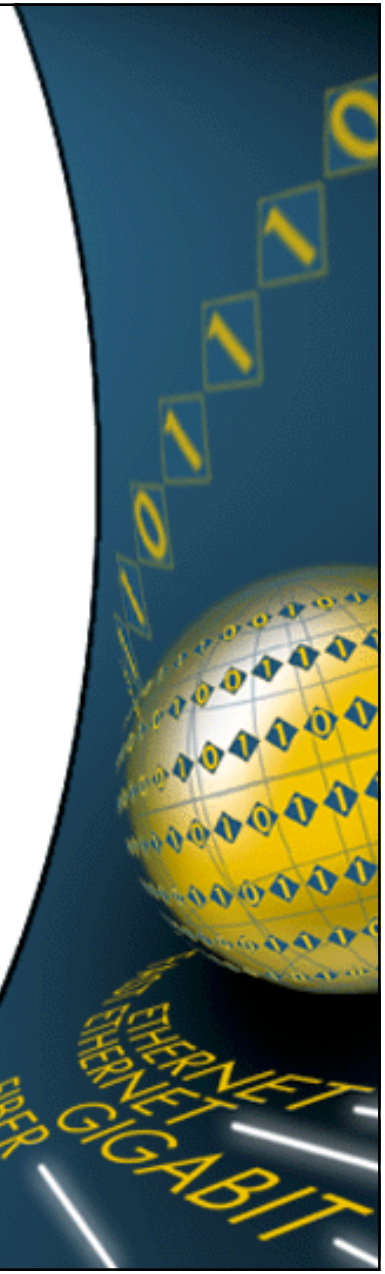
Firewall y VPN's

Rev. Sep-2000

Allied Telesyn SIMPLY CONNECTING THE WORLD

Protege tus recursos

Firewall



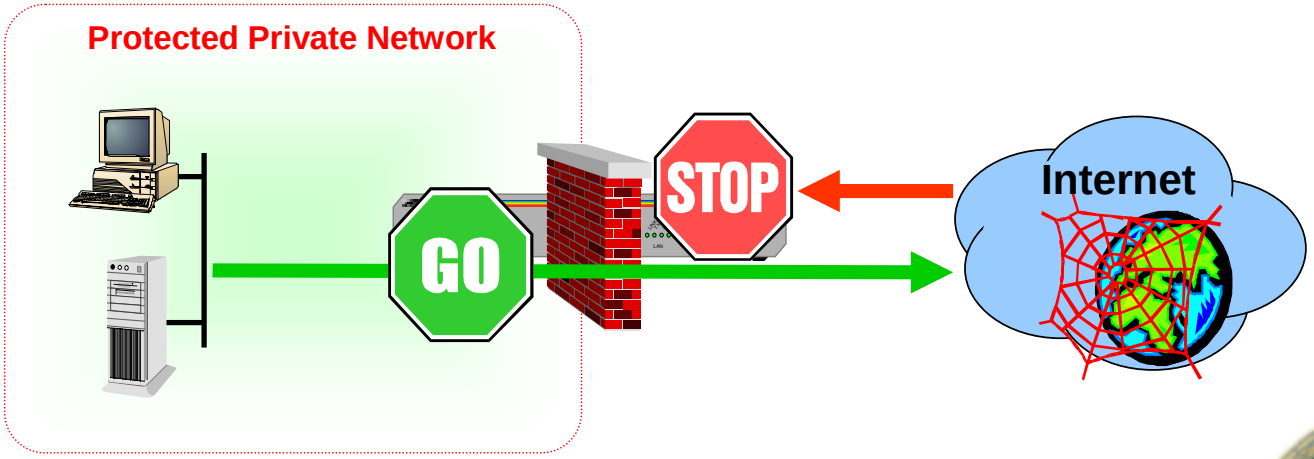
Allied Telesyn SIMPLY CONNECTING THE WORLD

¿Que es un firewall?

- Un centinela en la puerta de tu red
- Un firewall es un dispositivo de seguridad diseñado para permitir un acceso seguro a Internet

¿Que es un firewall?

Un firewall permite o deniega accesos basándose en políticas y reglas



Tipos comunes de ataques

- Intrusiones
  - Para poner en duda o desafiar
  - Vandalismo
  - Uso del sistema para distribuir material sospechoso o ilegal
  - Robar información

Buscando Debilidades

- Descubriendo hosts (ordenadores) en las redes privadas
  - Host Scans
- Descubriendo debilidades en hosts, firewalls y routers.
  - Port Scans

Tipos comunes de ataques

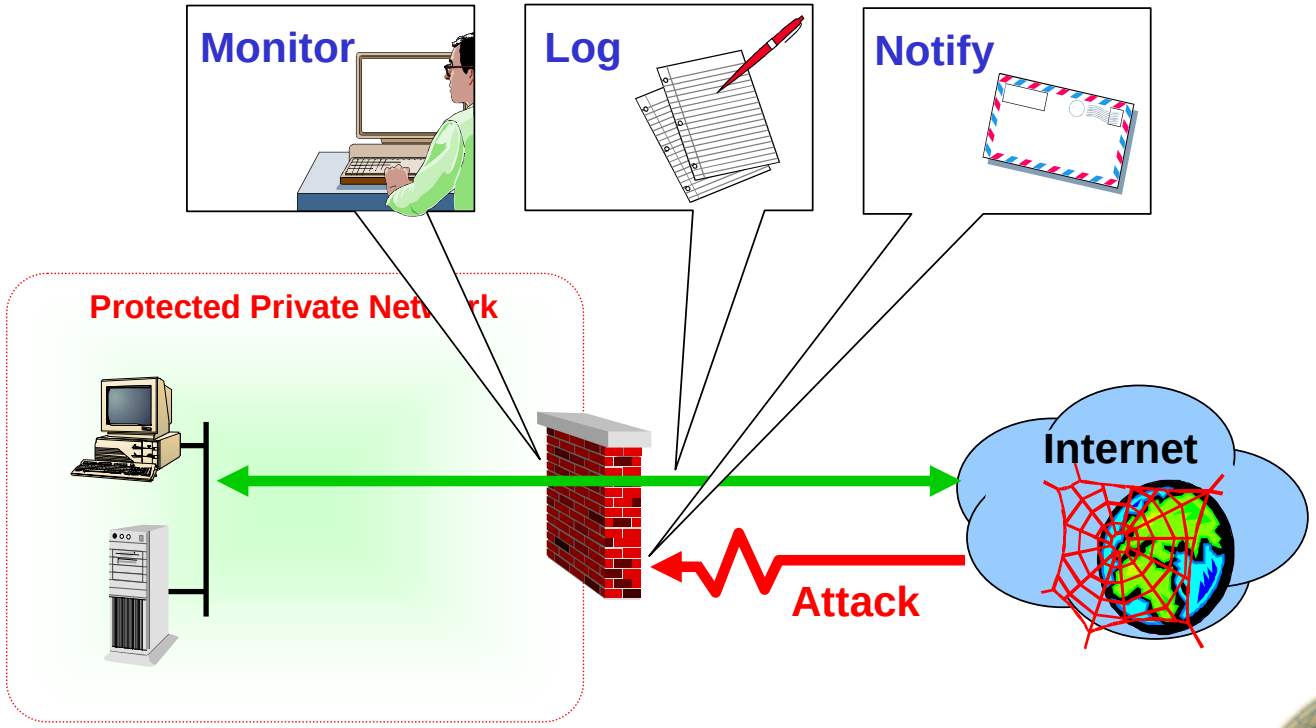
- Denegación de Servicio (DOS)
  - Intentando impedir el uso legítimo de un sistema de red
  - Incapacidad de servicios comerciales
  - Sobrecarga o cuelgue de routers de acceso, redes, firewalls o hosts
  - Bypass de firewalls basados en server

Ataques de denegación de servicio

- Algunos ejemplos de Denegación de Servicio
  - Fragmentation Attack
  - Smurf Attack
  - SYN Flooding

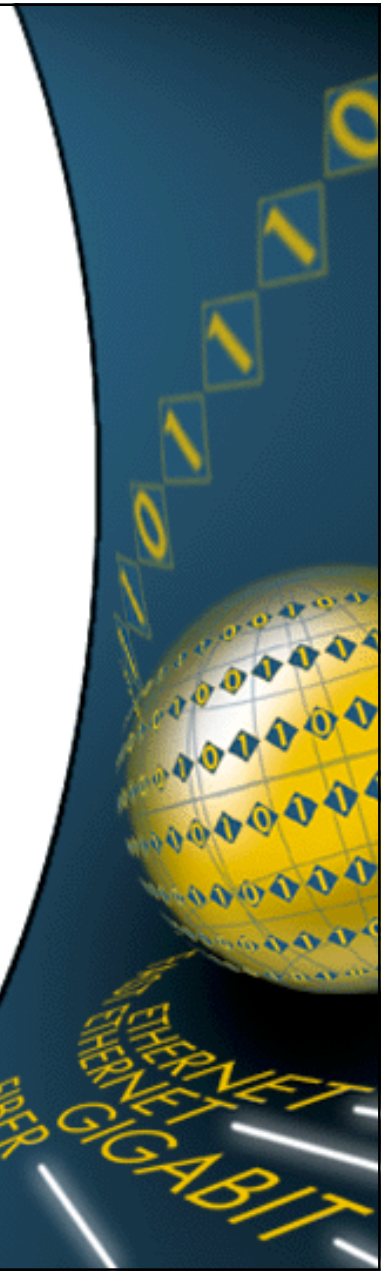
Allied Telesyn SIMPLY CONNECTING THE WORLD

Vigilando para ataques



Seguridad en Internet

Tecnologías de Firewall



Allied Telesyn SIMPLY CONNECTING THE WORLD

Tres tecnologias de firewall

- La National Computer Security Association clasifica los firewalls en tres categorias:
  - Packet Filtering Firewall
  - Application Gateway Firewall
  - Stateful Inspection Firewall

Allied Telesyn SIMPLY CONNECTING THE WORLD

The Internet protocol stack

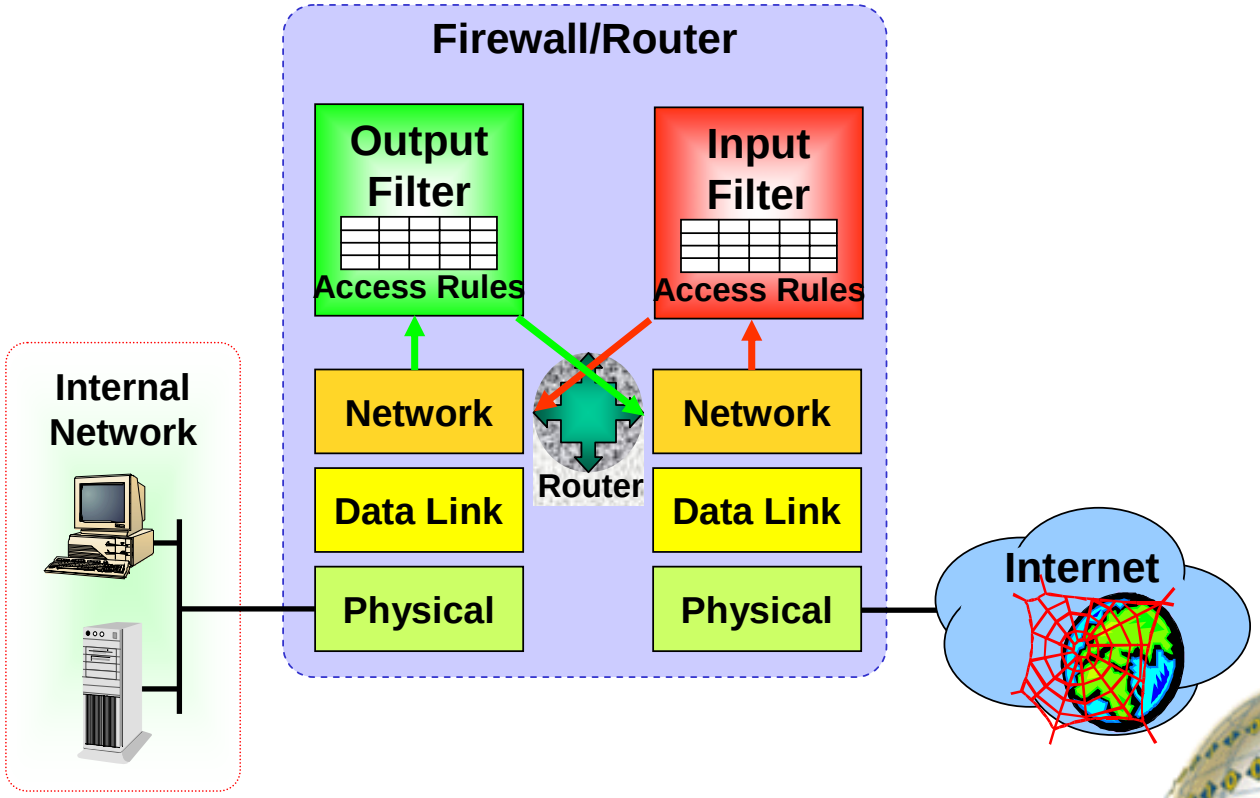
	Application	
TCP, UDP . . .	Transport	TCP, UDP . . .
IP	Network	IP
PPP, Frame Relay . . .	Data Link	Drivers, MAC Address
Leased Line, ISDN, xDSL . . .	Physical	LAN Interface Card

Packet Filtering firewall

- El firewall original
- Aplica filtros de paquetes basado en reglas de acceso:
  - Dirección de origen
  - Dirección de destino
  - Aplicación o protocolo
  - Puerto de origen
  - Puerto de destino

Allied Telesyn SIMPLY CONNECTING THE WORLD

Packet Filtering firewall



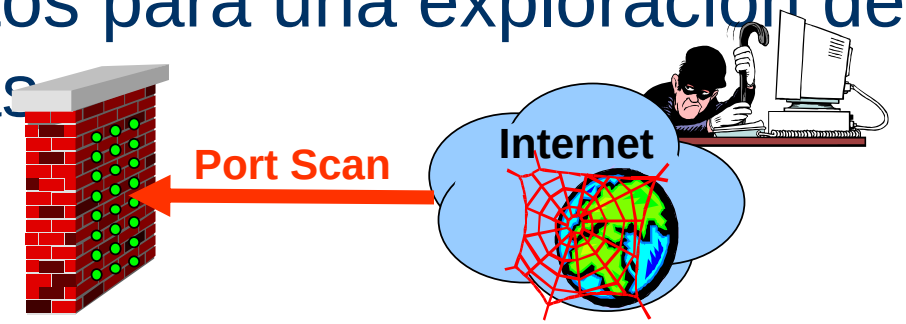
Packet Filtering firewall - Ventajas

- Bajo coste
- Baja sobrecarga de CPU

Allied Telesyn SIMPLY CONNECTING THE WORLD

Packet Filtering firewall - Desventajas

- Se basa sólo en la información de la capa de Red y Transporte
- Configuración estática, lo que significa que los puertos TCP o UDP están abiertos para una exploración de los piratas

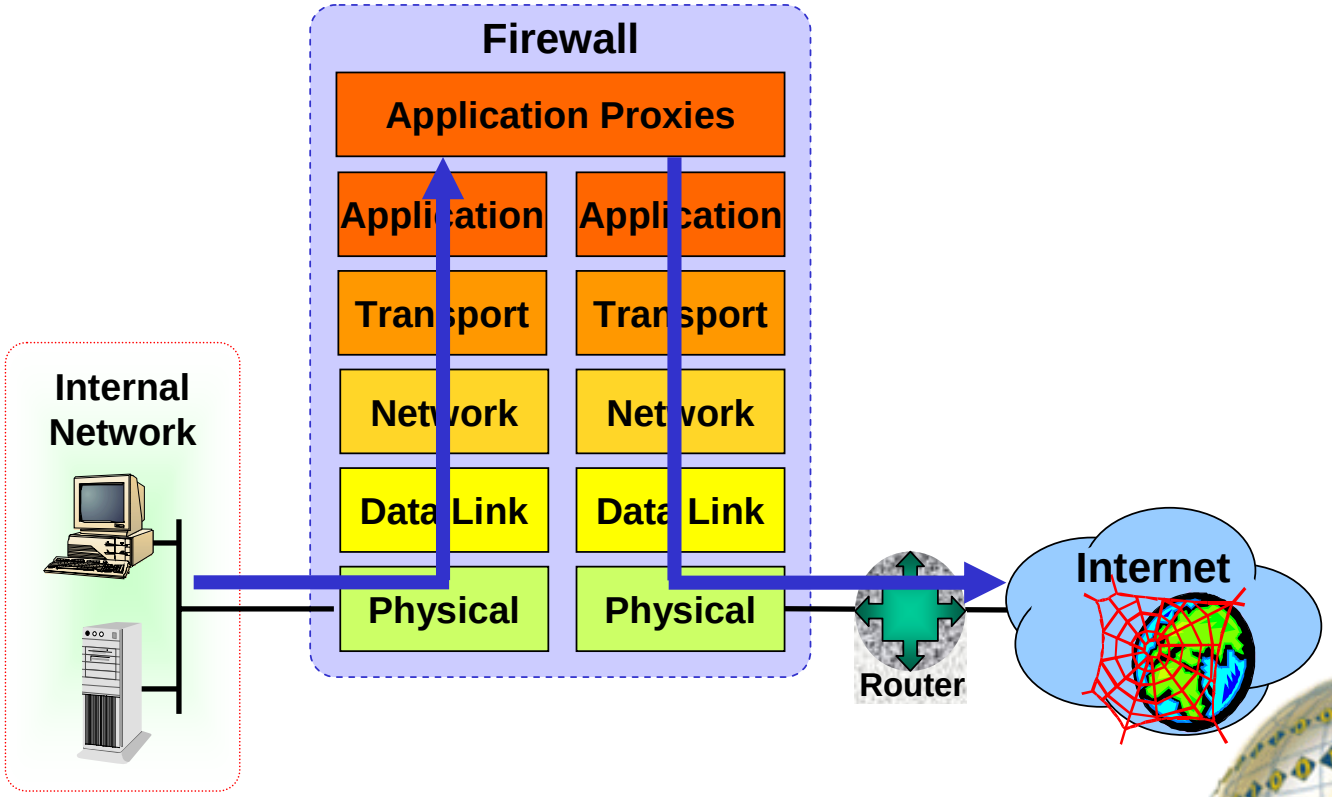


Application Gateway firewall

- Una aproximación a la tecnologia de firewall
  - Cada conexión entre dos redes es realizada via una aplicación programada llamada proxy
  - Proxies son aplicaciones o protocolos específicos
  - Sólo los protocolos que tienen específicos proxies configurados están permitidos para atravesar el firewall, todo el resto de tráfico es rechazado

Allied Telesyn SIMPLY CONNECTING THE WORLD

Application Gateway Firewall



Application Gateway - Ventajas

- Muy seguro si es usado en conjunción con un firewall inteligente de filtrado de paquetes
- Un buen diseño de los proxies provee una excelente seguridad

Allied Telesyn SIMPLY CONNECTING THE WORLD

Application Gateway - Desventajas

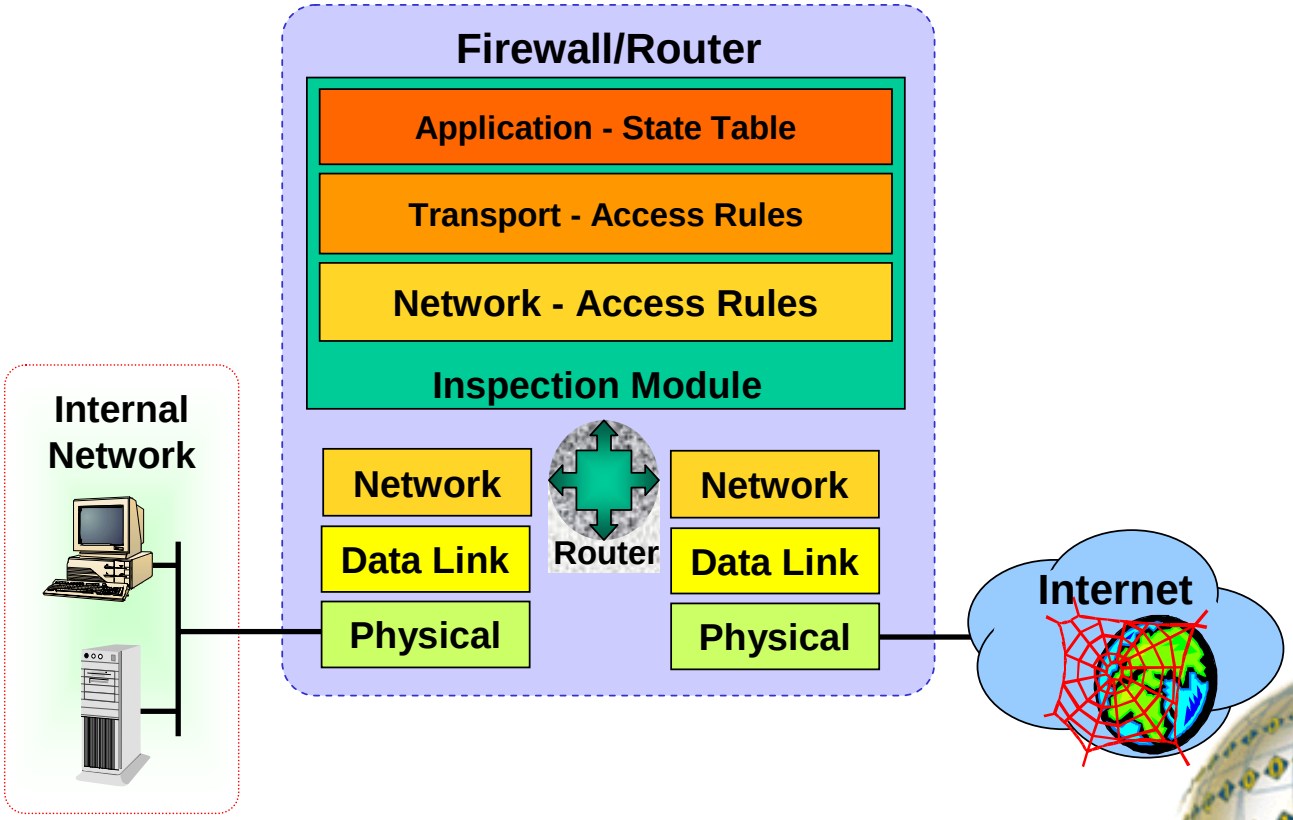
- Mucha carga de la CPU
- Requiere altas prestaciones en el ordenador donde reside
- El sistema operativo del ordenador está sujeto a ataques
- Muchos proxies no son transparentes para la aplicación
- No es transparente para los usuarios
- Caro

Stateful Inspection firewall

- Tercera generación de la tecnologia de firewall, con frecuencia referido como filtrado de paquetes dinámico (dynamic packet filtering)
- Entiende los datos de los paquetes desde la capa de Red (cabecera IP) hasta la capa de aplicación
- Sigue la pista del estado de la comunicación

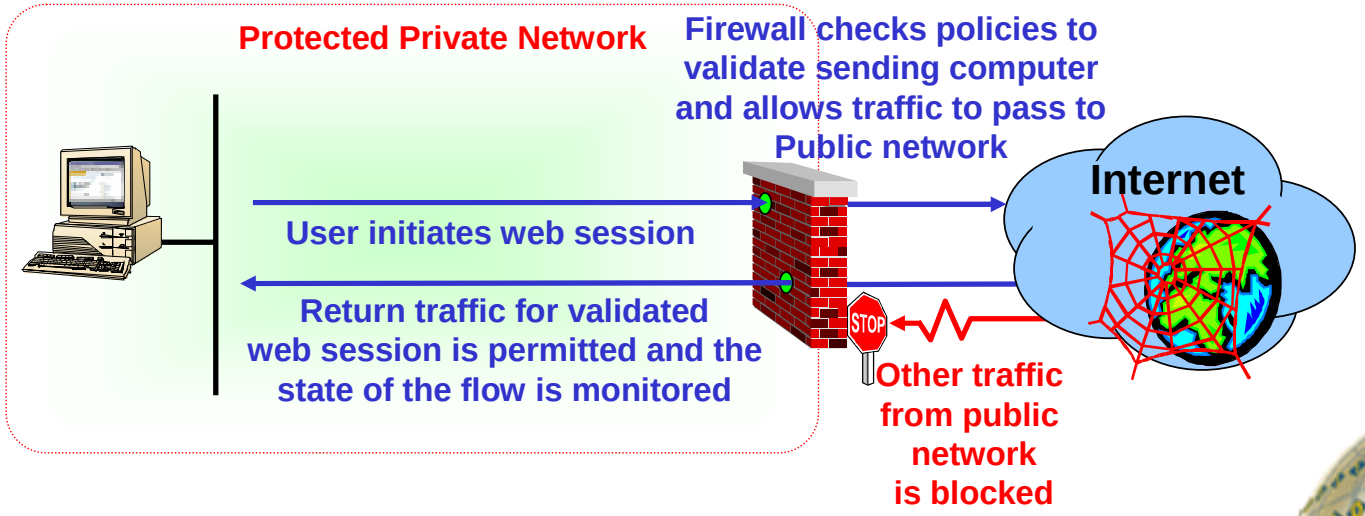
Allied Telesyn SIMPLY CONNECTING THE WORLD

Stateful Inspection firewall



Filtro dinámico

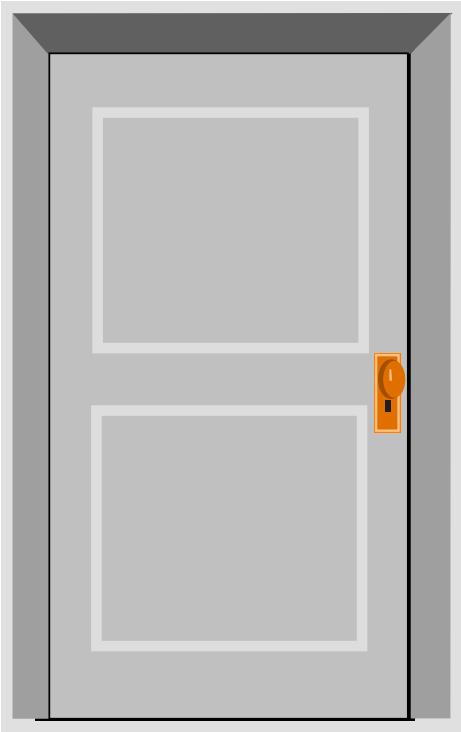
Stateful Inspection firewall dinamicamente abre y cierra puertos (puntos de conexión específicos de aplicación) basándose en políticas de acceso.



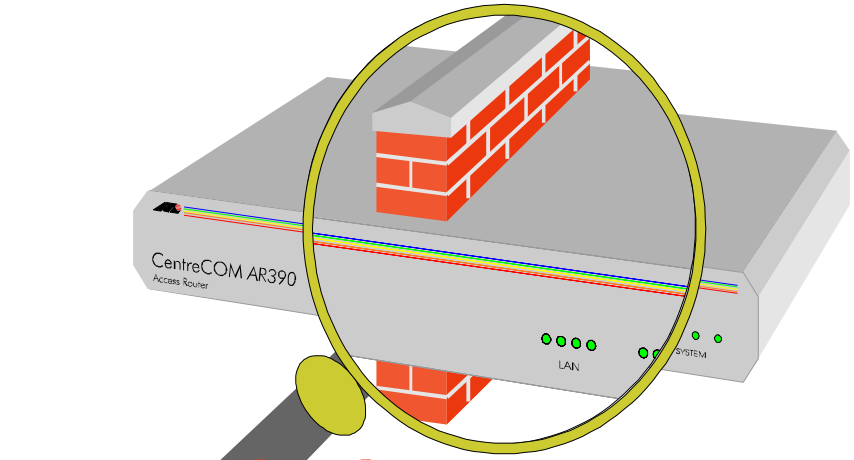
Stateful Inspection - Ventajas

- Monitoriza el estado del flujo de todos los datos
- Dinamicamente adapta filtros basados en políticas y reglas definidas
- Facilmente adaptable a las nuevas aplicaciones de Internet
- Transparente para los usuarios
- Baja carga de CPU

Requerimientos esenciales de seguridad



- Un firewall es la construcción de un conjunto de fundamentos para implementar una red segura
- Cierra primero la puerta



NEMESIS FIREWALL

Redefining Network Security

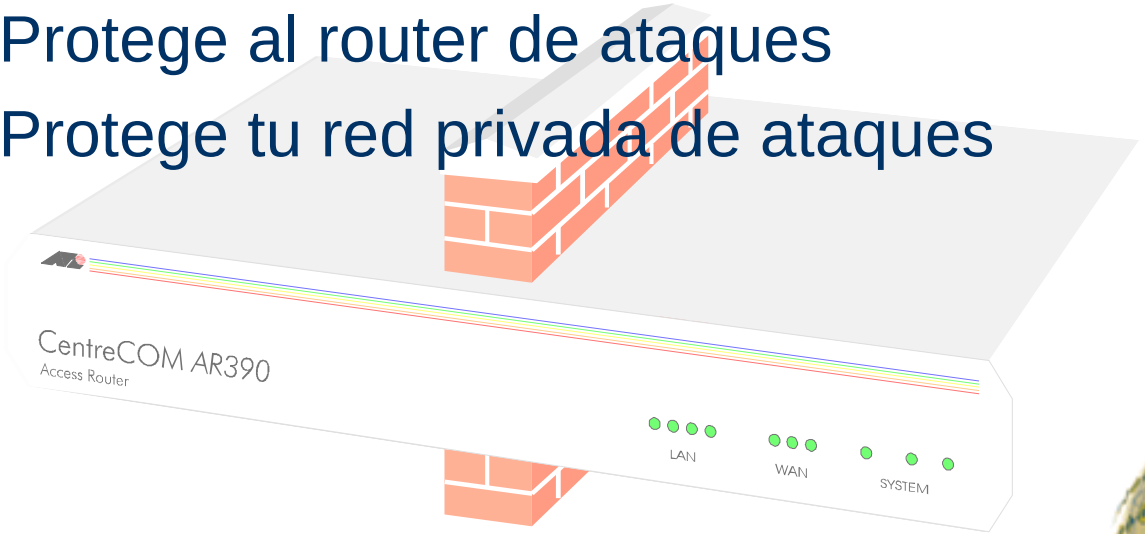
Allied Telesyn SIMPLY CONNECTING THE WORLD

Nemesis firewall

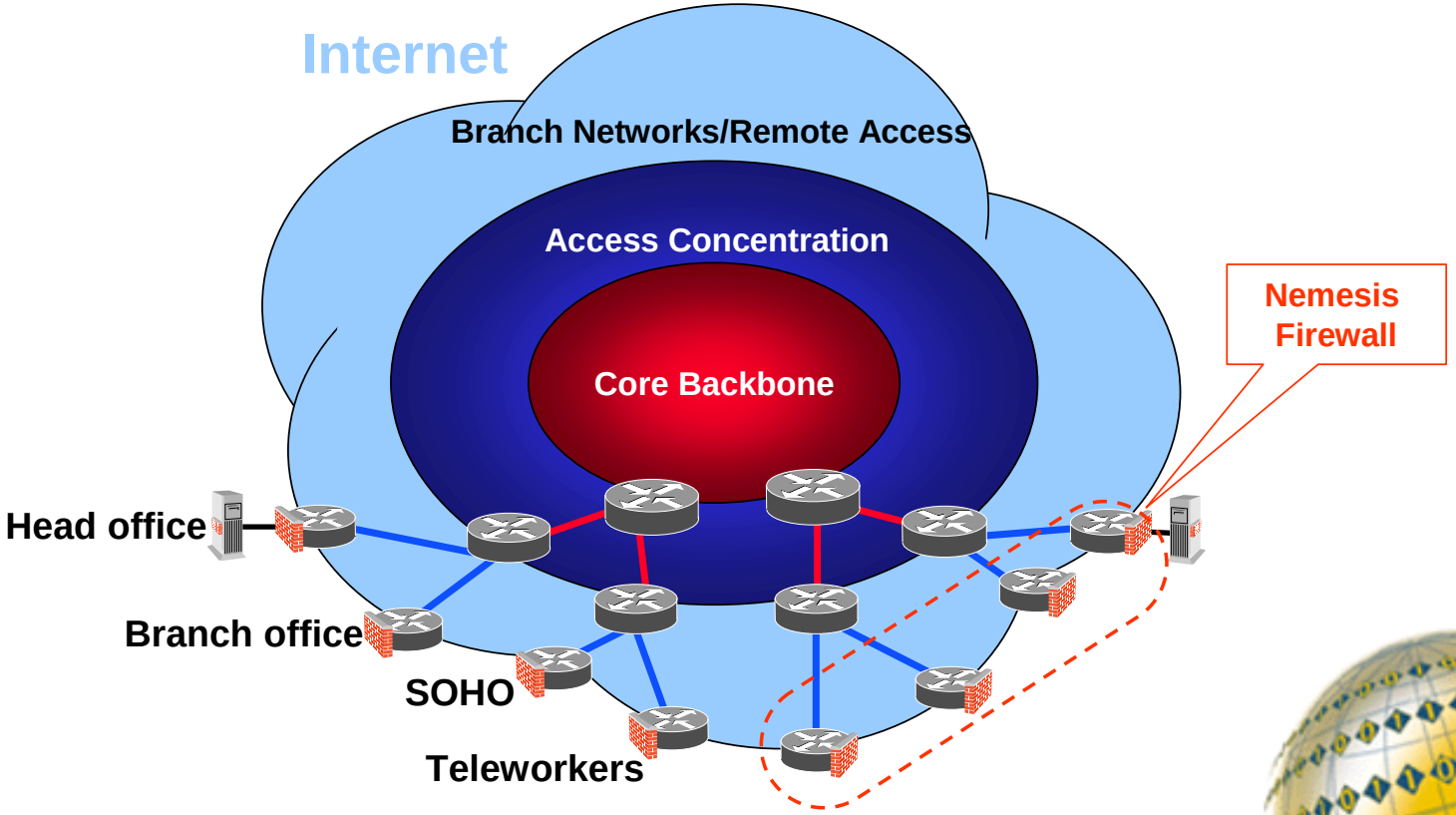
Un centinela en la puerta de tu red, combinando la potencia de multiples tecnologias para aportar un potente perímetro de seguridad

Router/Firewall Integrado

- Los routers de la serie AR proporcionan la plataforma para Nemesis
  - Protege los puntos de acceso de tu red
  - Protege al router de ataques
  - Protege tu red privada de ataques



Posicionamiento de Nemesis

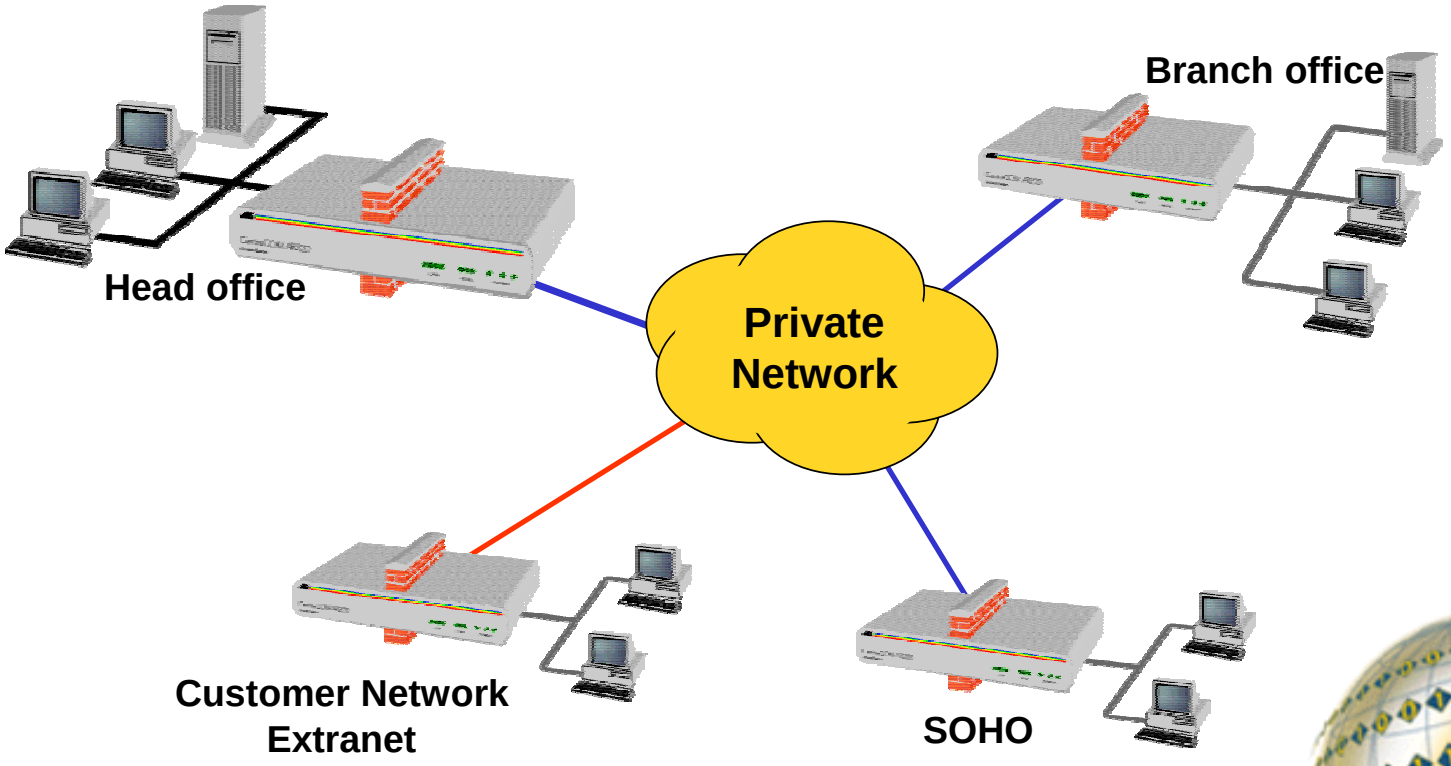


Allied Telesyn SIMPLY CONNECTING THE WORLD

¿Quien se beneficia de la Protección Nemesis?

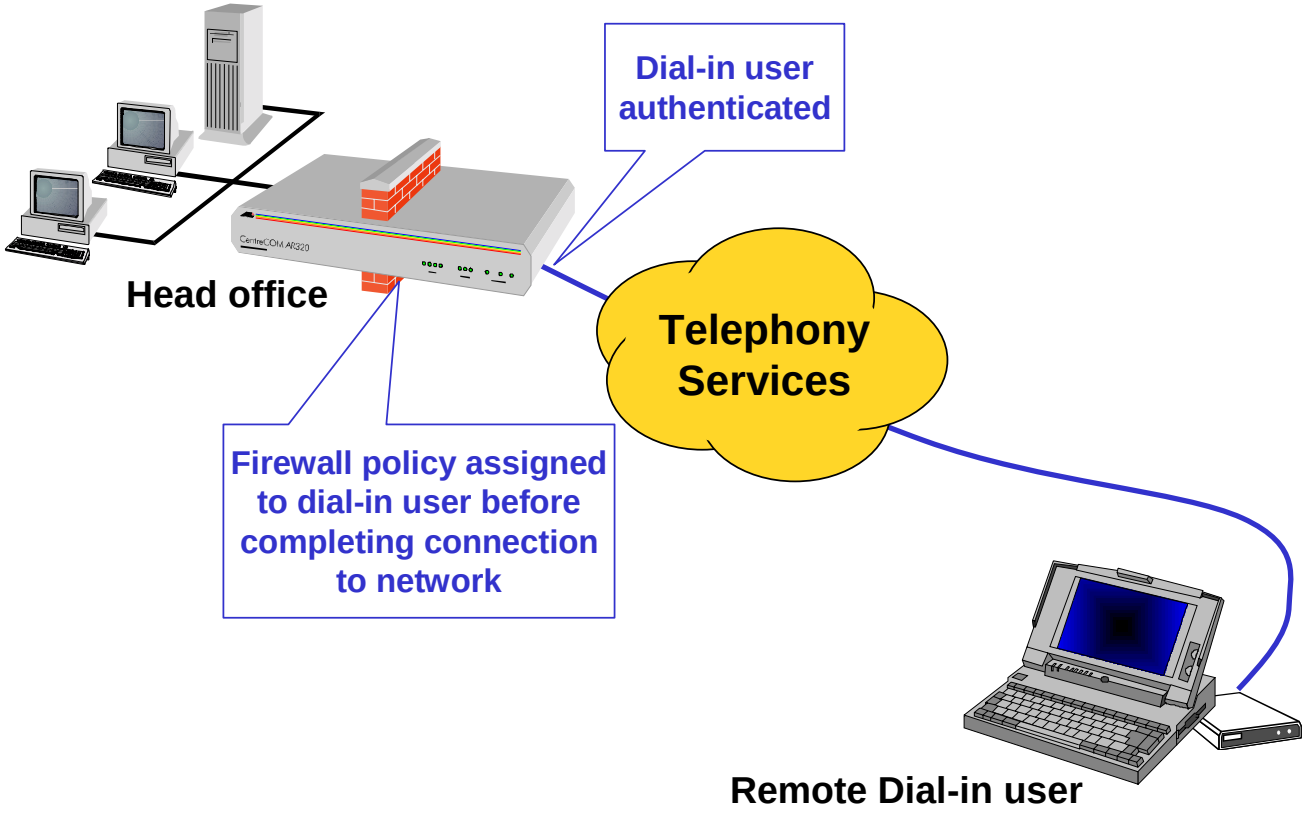
- Nemesis proporciona alto nivel de protección a un bajo nivel de coste
- Delegaciones de Corporaciones
- Pequeños y medianos negocios
- Localizaciones remotas
- Teletrabajadores

Seguridad Interoficinas Nemesis



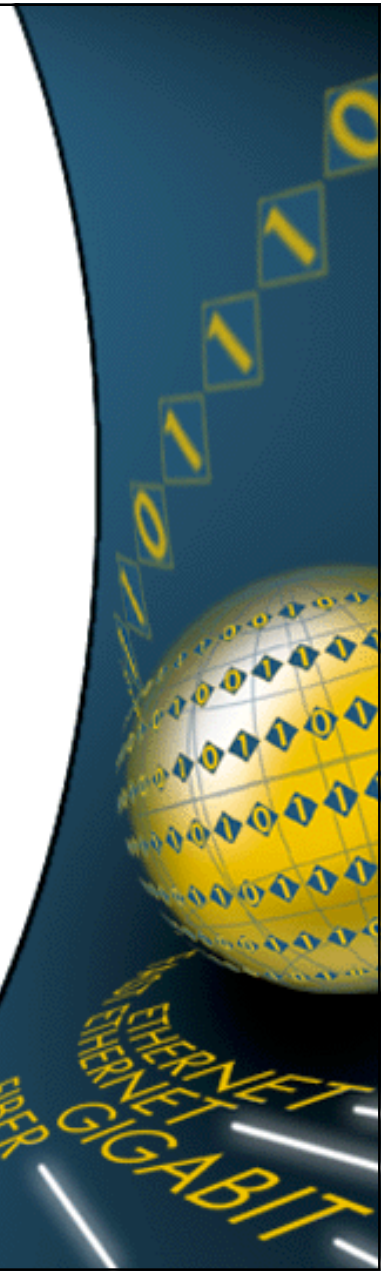
Allied Telesyn SIMPLY CONNECTING THE WORLD

Seguridad para acceso remoto Nemesis



Firewall Nemesis

Tecnología

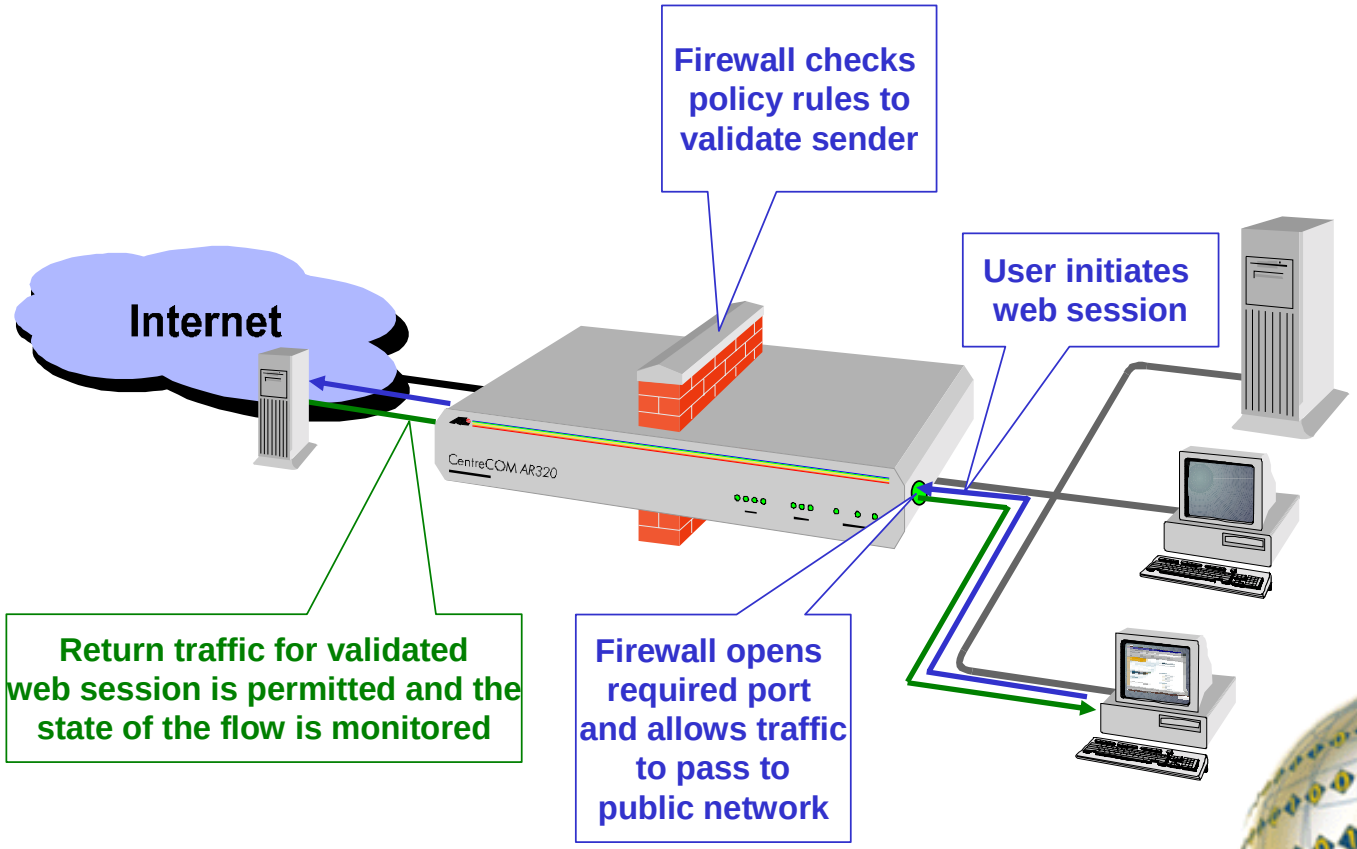


Allied Telesyn SIMPLY CONNECTING THE WORLD

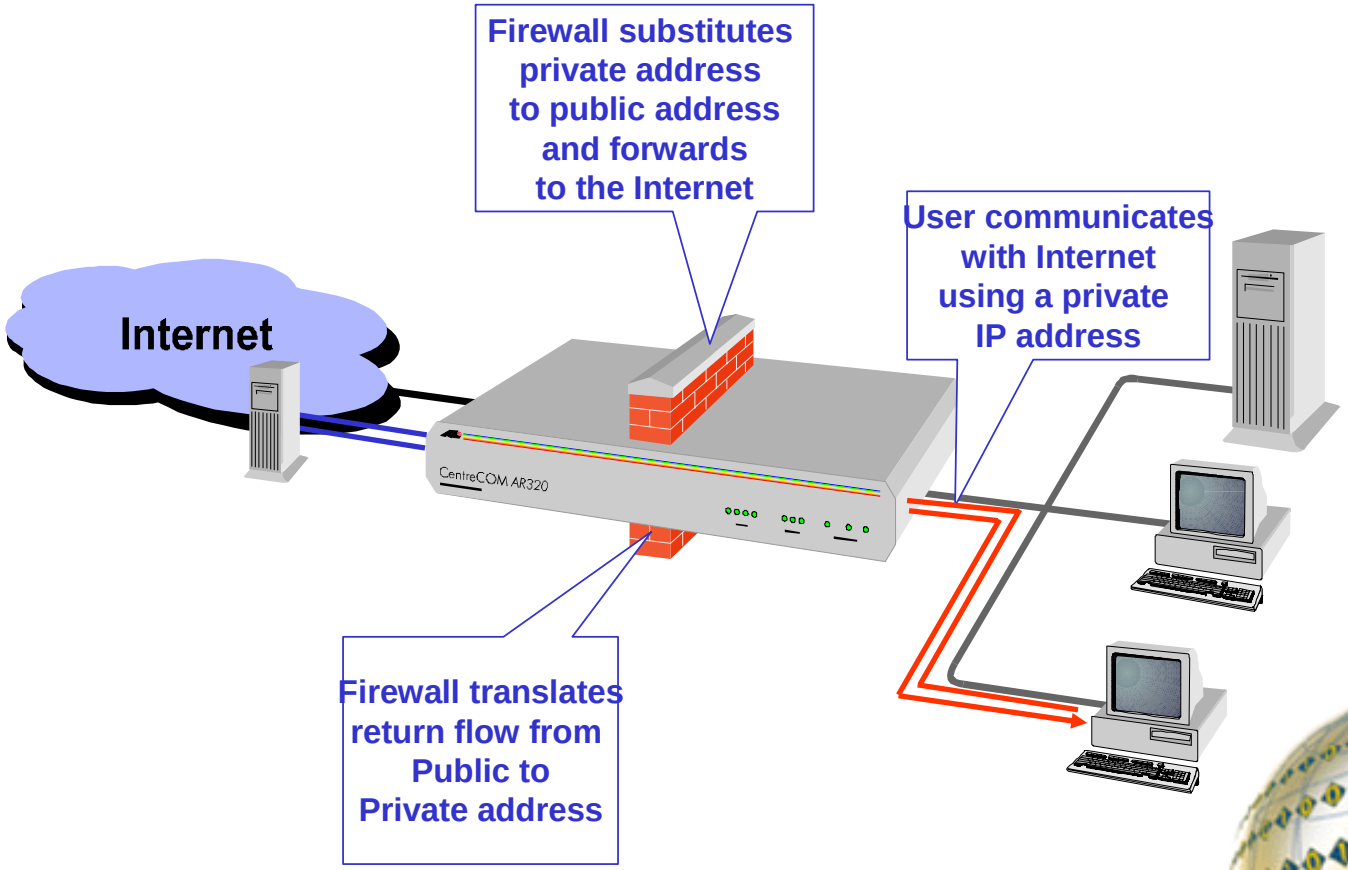
Firewall Nemesis

Combinando la potencia de la tecnologia Stateful Inspection firewall, Network Address Translation (NAT) y Application Level Gateways (ALG) garantiza la potencia del perímetro de seguridad

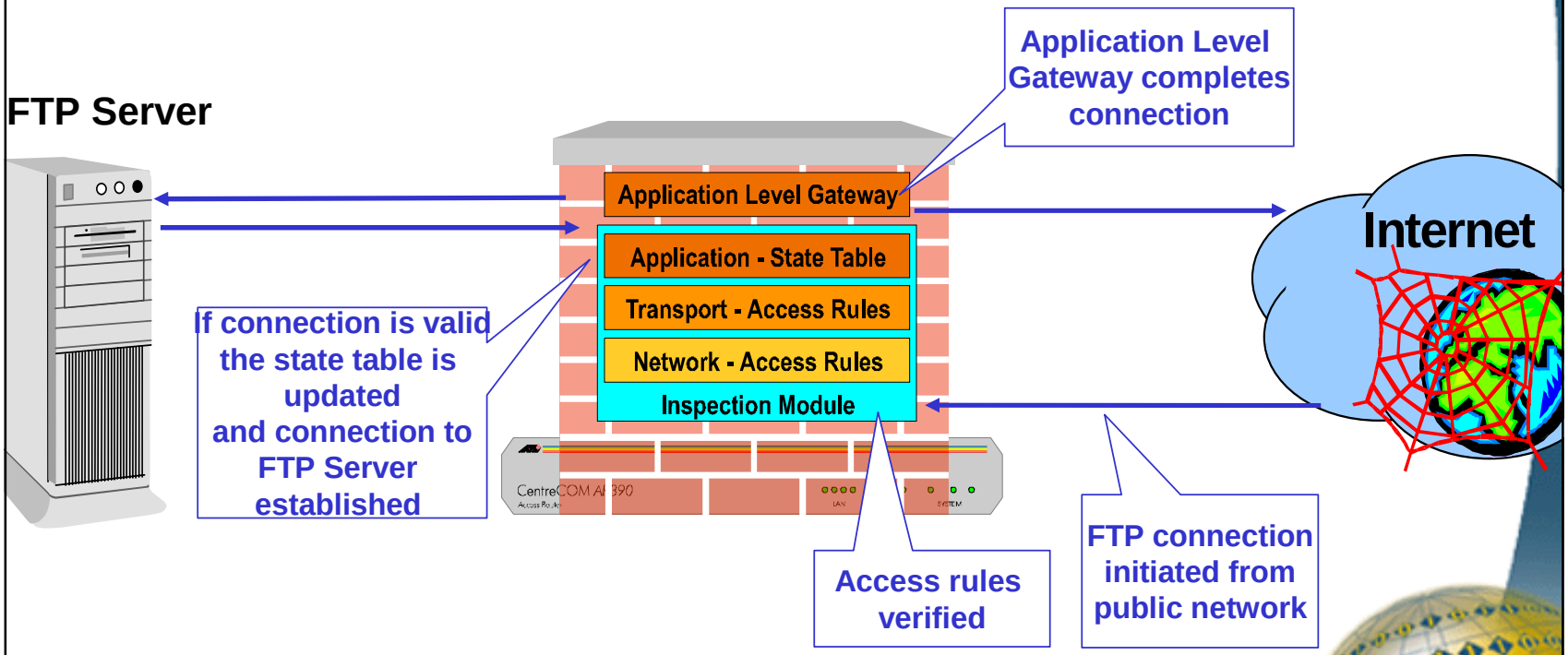
Nemesis - Stateful Inspection



Network Address Translation



Ejemplo de ALG Nemesis

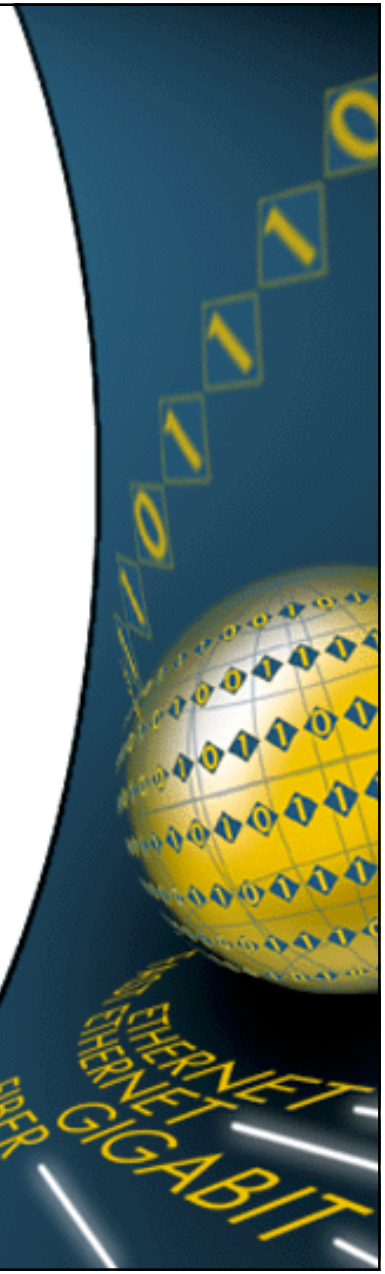


Firewall Nemesis - Protocolos soportados

- El firewall soporta protocolos como:
  - FTP, Progressive Networks’ RealAudio, Xing Technologies' Streamworks, White Pines' CuSeeMe, VDOnet's VDOLine, Microsoft's NetShow, NETBIOS, GRE, OSPF, PPTP, RSVP. . . . . .

Firewall Nemesis

Características



Allied Telesyn SIMPLY CONNECTING THE WORLD

Firewall Nemesis

- Aporta seguridad protegiendo las redes privadas contra las técnicas de los piratas incluyendo:
  - Ataques de Denegación de Servicio
    - SYN flooding, Fragmentation, Smurf and DDoS attacks
  - Scaneos
    - host scans y port scans

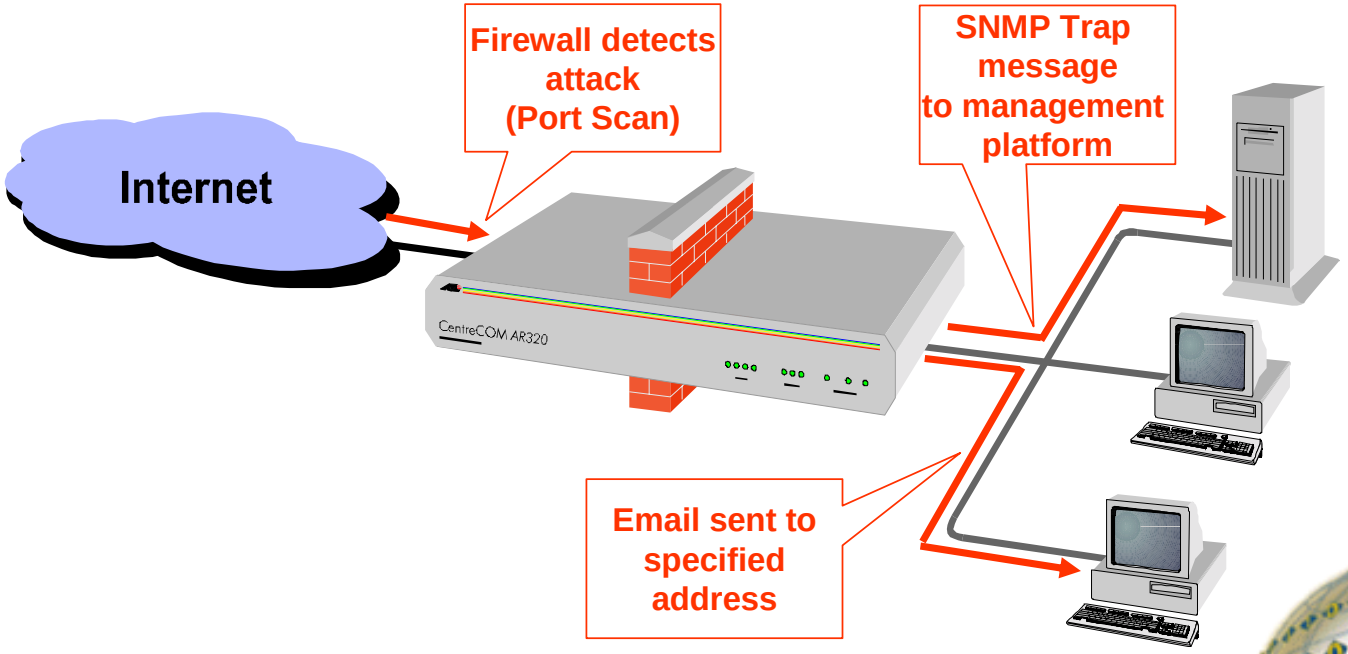
Firewall Nemesis - Reporting

- Todos los eventos del firewall pueden ser selectivamente registrados
  - Nemesis detecta y registra ataques de denegación de servicio y scaneos
  - Una contabilidad facilita datos grabados del flujo de tráfico por sesiones individuales
  - Las opciones de notificación de Nemesis dan una alarma inmediata de los ataques

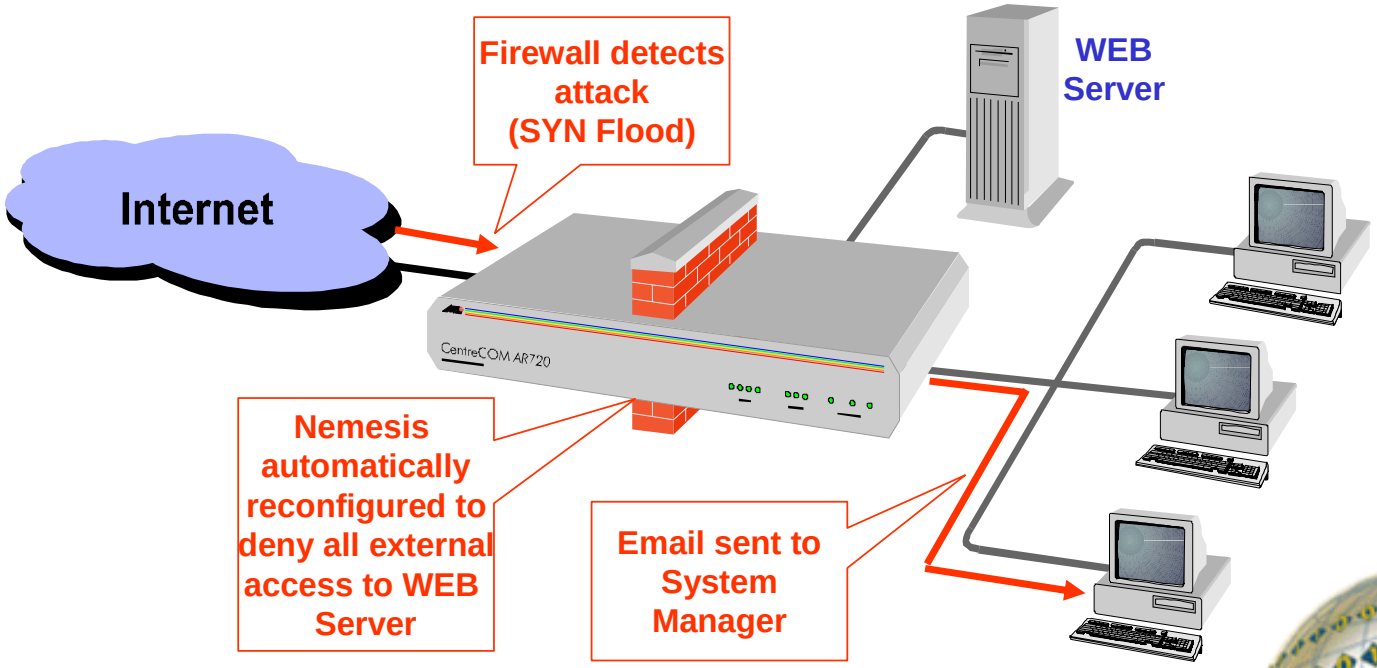
Registros

- El firewall puede ser configurado para que registre un extenso rango de eventos incluyendo:
  - Todos los paquetes denegados
  - Todos los paquetes permitidos
  - Una selección de tipos de paquetes permitidos y denegados

Notificación



Notificación y reconfiguración



Gestión segura

- Gestión remota segura con encriptación y autentificación
  - Secure Shell “SSH”
  - Encriptación RSA con claves de 512 - 2048 bits
  - DES y Triple DES encriptación para sesiones SSH
  - Puede limitar el acceso a direcciones de usuarios específicas

RADIUS

- Remote Authentication Dial-In User Services
  - Una única base de datos de seguridad central para todos los usuarios del sistema
  - Gestión centralizada de listas de acceso

Allied Telesyn SIMPLY CONNECTING THE WORLD

Integración de VPN

- Total integración con las soluciones VPN y VPDN de Allied Telesyn
  - IPsec, L2TP, encriptación DES y 3DES
- Combina redes seguras con bajo coste del ancho de banda global

Nemesis - Resumen

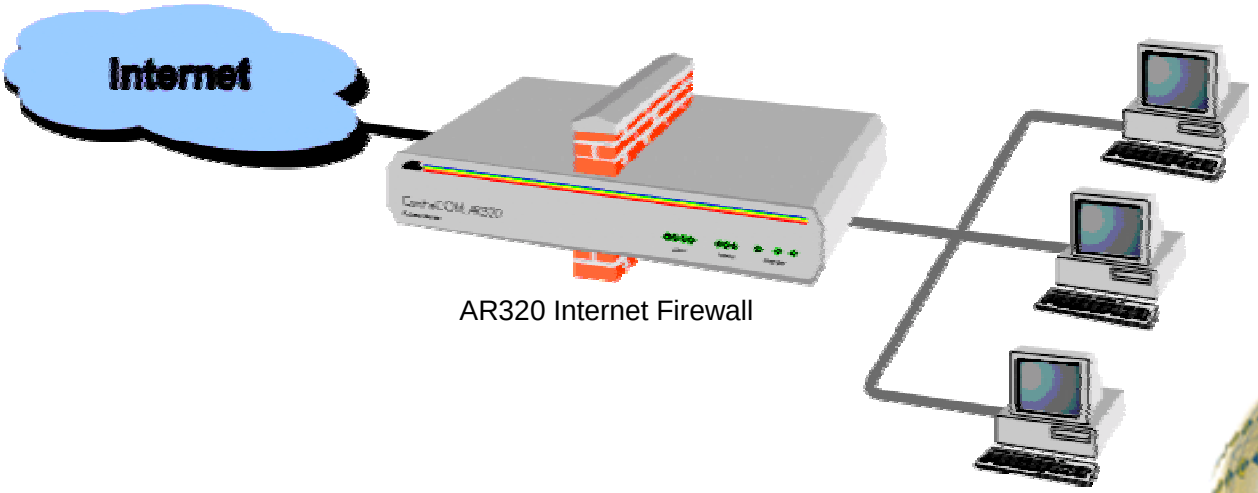
- Alto nivel de seguridad en la red a un bajo nivel de precio
- Total protección de acceso a delegaciones, pequeñas oficinas, teletrabajadores, etc.
- Protección de perímetro para Oficinas Centrales Corporativas

Plataformas Nemesis

- Puede ser implementada en todos los routers de las series AR3XX y AR7XX
  - Opcional en los modelos:
    - AR300L AR300, AR310, AR350, AR390, AR395 y AR720
  - Tres modelos con firewall como estandar
    - AR320, AR330 y AR720 DMZ

AR320

- Dos interfaces Ethernet para conexiones a Internet via xDSL o cable modems

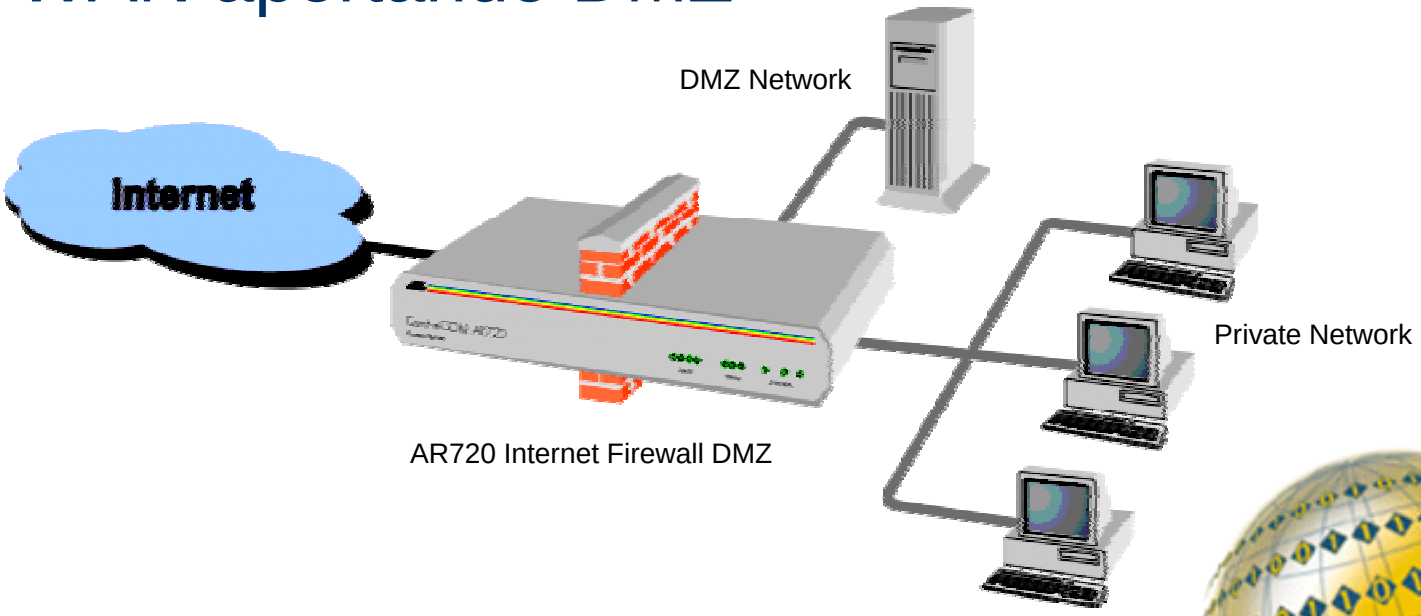


AR 320

- Interfaces
  - 2 x 10Mbps Ethernet ports
  - 2 x Async Ports
- WAN protocols supported
  - PPPoE (client & access concentrator)
  - DHCP (server & client)
  - Fixed IP address

AR330

- Dos interfaces Ethernet y un interface WAN aportando DMZ

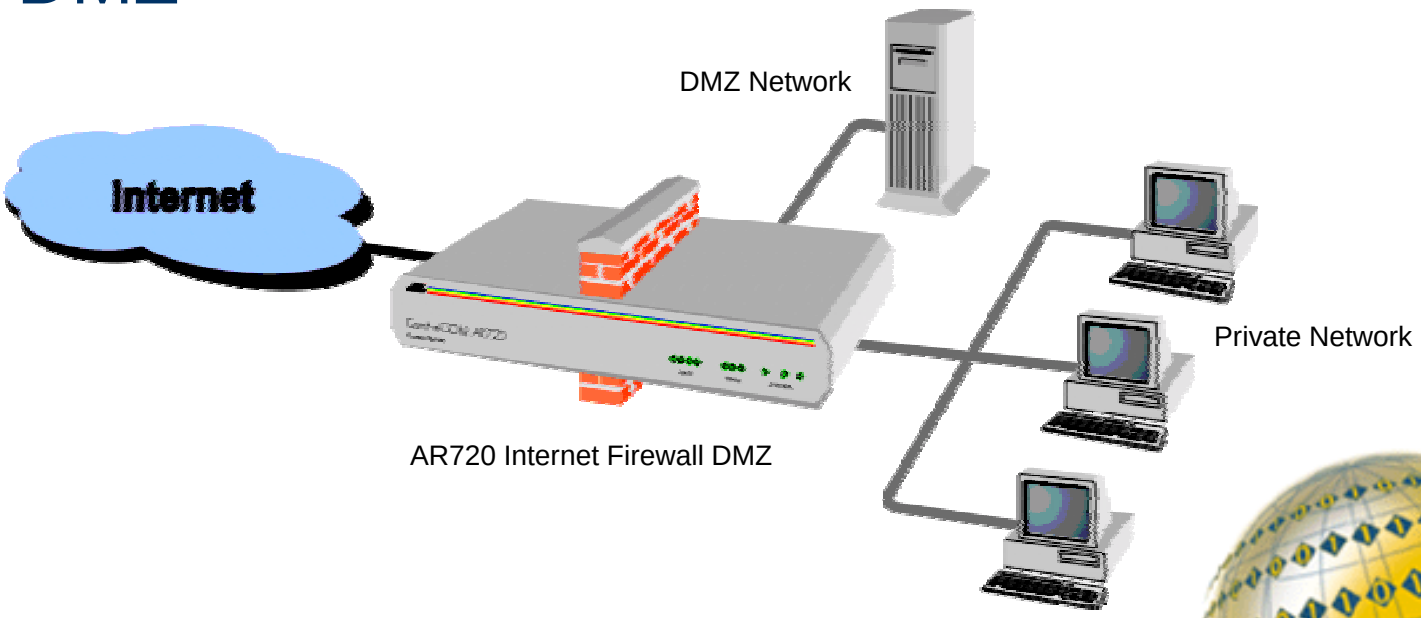


AR 330

- Interfaces
  - 2 x 10Mbps Ethernet ports
  - 2 x Async Ports
  - 1 x Sync WAN (X.21, V.35, V.24)
- WAN protocols supported
  - PPPoE (client & access concentrator)
  - Frame Relay
  - X.25

AR720 DMZ

- Tres interfaces Ethernet posibilidad de DMZ

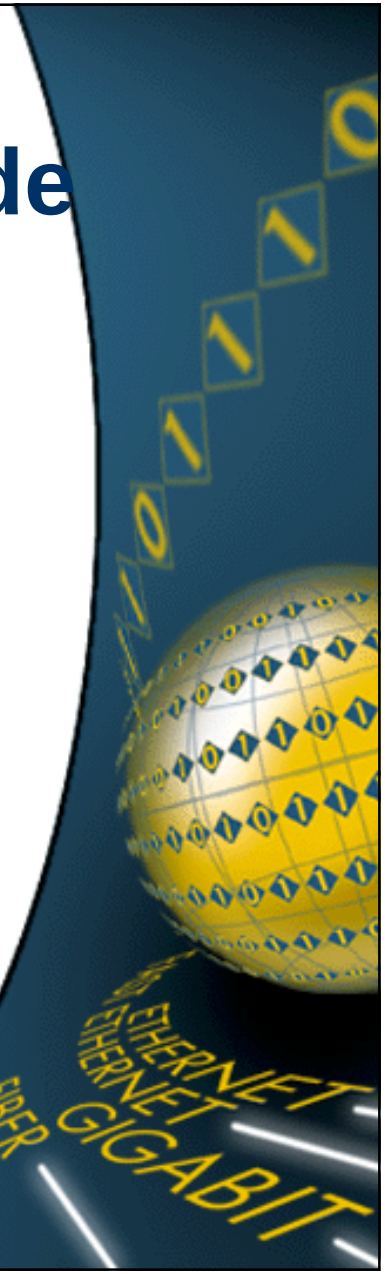


AR 720 DMZ

- Interfaces
  - 1 x 10/100Mbps Ethernet port
  - 2 x 10Mbps Ethernet ports
  - 2 x Async Ports
- WAN protocols supported
  - PPPoE (client & access concentrator)
  - DHCP (server & client)
  - Fixed IP address

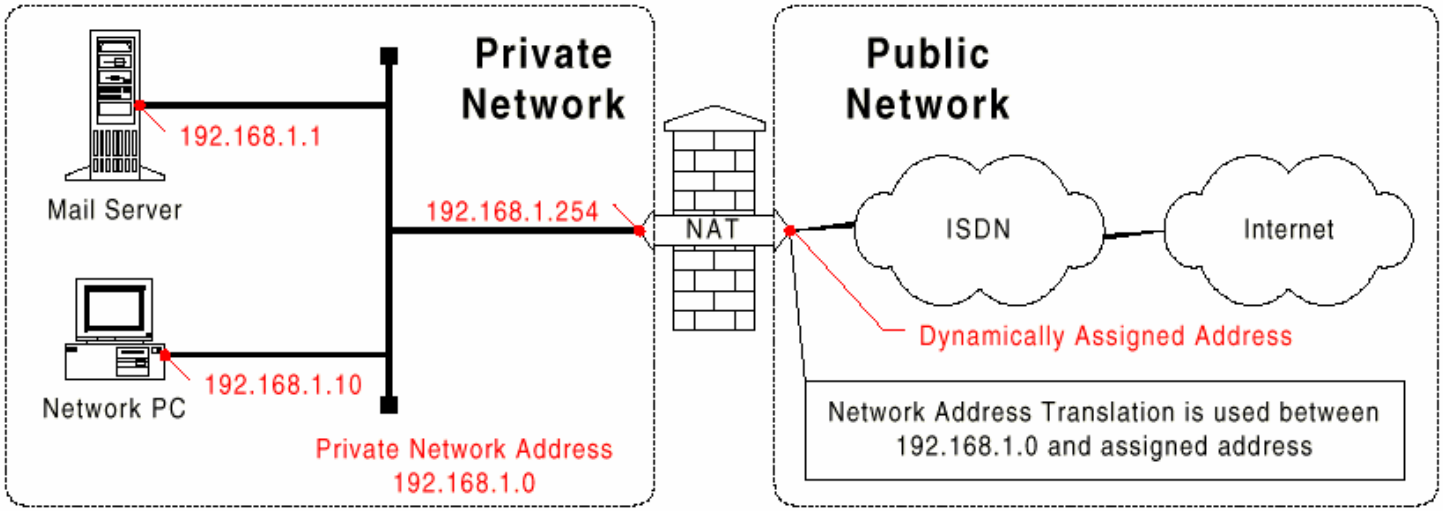
Ejemplos de configuración de Redes

¿Cómo podemos aplicar Nemesis?



Allied Telesyn SIMPLY CONNECTING THE WORLD

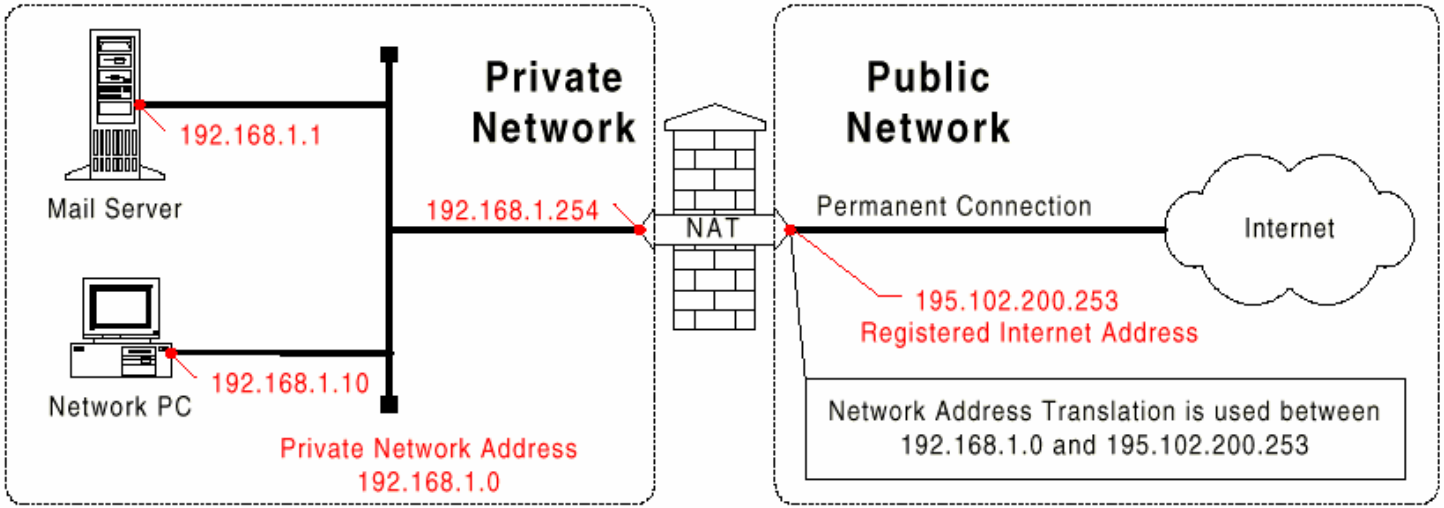
Configuraciones Firewall



Configuraciones Firewall

- SET Q931=0 PROF=ETB NUM1=12345
- ADD ISDN CALL=INTERNET NUMBER=0121345678 PREC=OUT DIRECTION=OUT
- CREATE PPP=0 IDLE=30 OVER=ISDN-INTERNET IPREQUEST=ON
- SET PPP=0 OVER=ISDN-INTERNET USERNAME="USER1" PASSWORD="LET-ME-IN" LQR=OFF
- ENABLE IP
- ENABLE IP REMOTE
- ADD IP INT=ETH0 IP=192.168.1.254
- ADD IP INT=PPP0 IP=0.0.0.0
- ADD IP ROU=0.0.0.0 MASK=0.0.0.0 INT=PPP0 NEXT=0.0.0.0
- ENABLE FIREWALL
- CREATE FIREWALL POLICY="OFFICE"
- ADD FIREWALL POLICY="OFFICE" INT=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY="OFFICE" INT=PPP0 TYPE=PUBLIC
- ADD FIREWALL POLICY=OFFICE NAT=ENHANCED INT=ETH0 GBLINT=PPP0

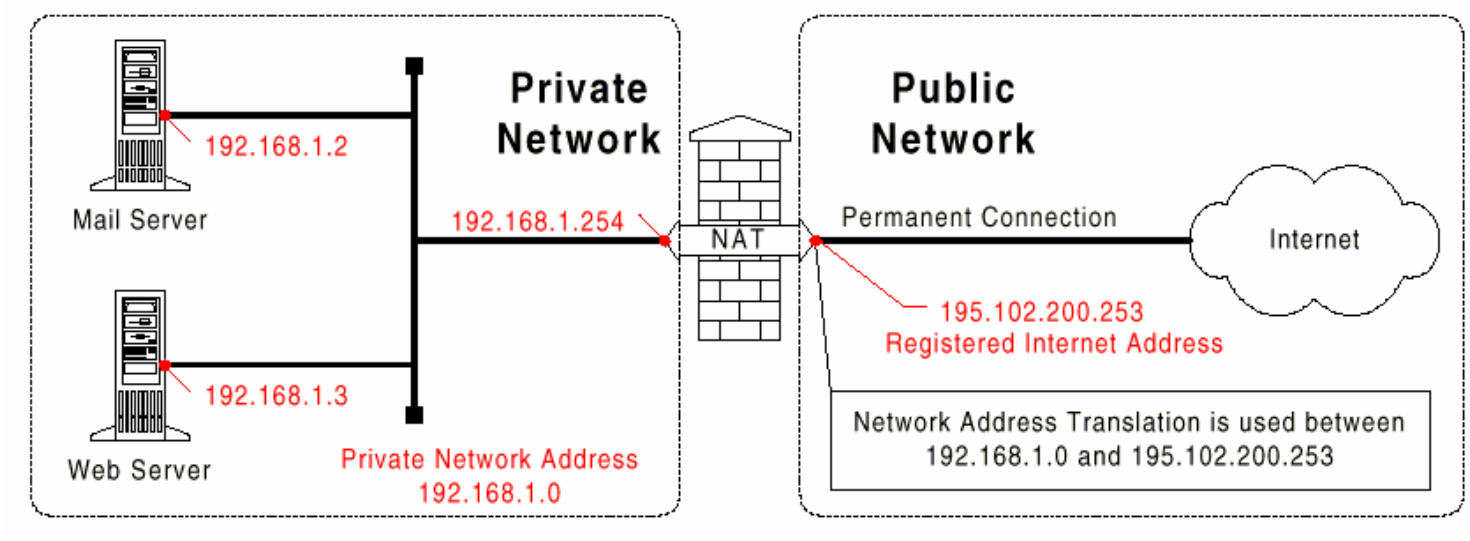
Configuraciones Firewall



Configuraciones Firewall

- SET Q931=0 PROF=ETB NUM1=12345
- ADD ISDN CALL=INTERNET NUMBER=0121345678 PREC=OUT DIRECTION=OUT
- CREATE PPP=0 IDLE=30 OVER=ISDN-INTERNET IPREQUEST=ON
- SET PPP=0 OVER=ISDN-INTERNET USERNAME="USER1" PASSWORD="LET-ME-IN" LQR=OFF
- ENABLE IP
- ENABLE IP REMOTE
- ADD IP INT=ETH0 IP=192.168.1.254
- ADD IP INT=PPP0 IP=195.102.200.253
- ADD IP ROU=0.0.0.0 MASK=0.0.0.0 INT=PPP0 NEXT=0.0.0.0
- ENABLE FIREWALL
- CREATE FIREWALL POLICY="OFFICE"
- ADD FIREWALL POLICY="OFFICE" INT=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY="OFFICE" INT=PPP0 TYPE=PUBLIC
- ADD FIREWALL POLICY=OFFICE NAT=ENHANCED INTERFACE=ETH0 GBLINTERFACE=PPP0 GBLIP=195.102.200.253

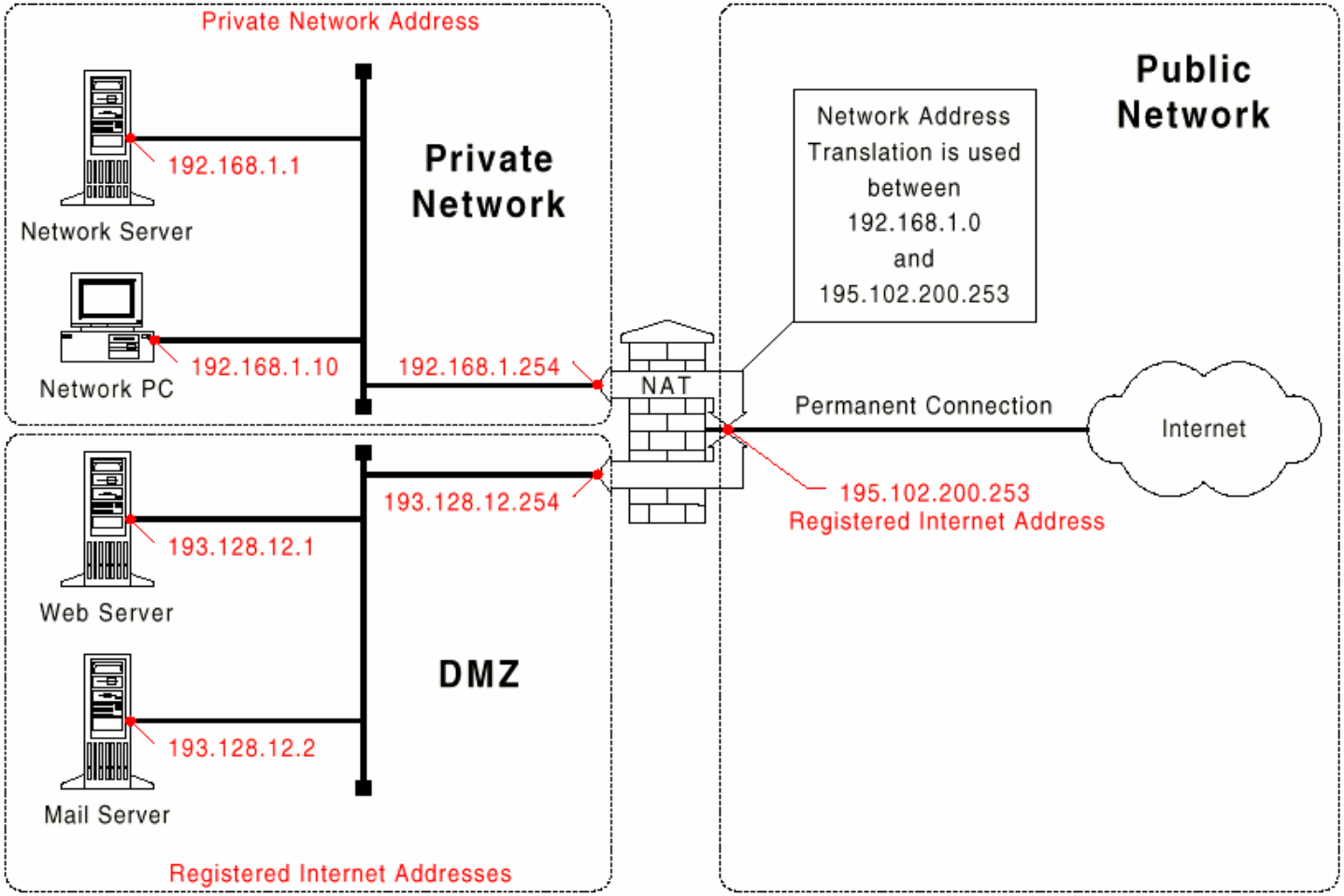
Configuraciones Firewall



Configuraciones Firewall

- SET Q931=0 PROF=ETB NUM1=12345
- ADD ISDN CALL=INTERNET NUMBER=0121345678 PREC=OUT DIRECTION=OUT
- CREATE PPP=0 IDLE=30 OVER=ISDN-INTERNET IPREQUEST=ON
- SET PPP=0 OVER=ISDN-INTERNET USERNAME="USER1" PASSWORD="LET-ME-IN" LQR=OFF
- ENABLE IP
- ENABLE IP REMOTE
- ADD IP INT=ETH0 IP=192.168.1.254
- ADD IP INT=PPP0 IP=195.102.200.253
- ADD IP ROU=0.0.0.0 MASK=0.0.0.0 INT=PPP0 NEXT=0.0.0.0
- ENABLE FIREWALL
- CREATE FIREWALL POLICY="OFFICE"
- ADD FIREWALL POLICY="OFFICE" INT=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY="OFFICE" INT=PPP0 TYPE=PUBLIC
- ADD FIREWALL POLICY=OFFICE NAT=ENHANCED INTERFACE=ETH0 GBLINTERFACE=PPP0 GBLIP=195.102.200.253
- ADD FIREWALL POLICY=OFFICE RULE=1 ACTION=ALLOW INT=PPP0 PROT=TCP PORT=25 IP=192.168.1.2 GBLIP=195.102.200.253 GBLPORT=25
- ADD FIREWALL POLICY=OFFICE RULE=2 ACTION=ALLOW INT=PPP0 PROT=TCP PORT=HTTP IP=192.168.1.3 GBLIP=195.102.200.253 GBLPORT=HTTP

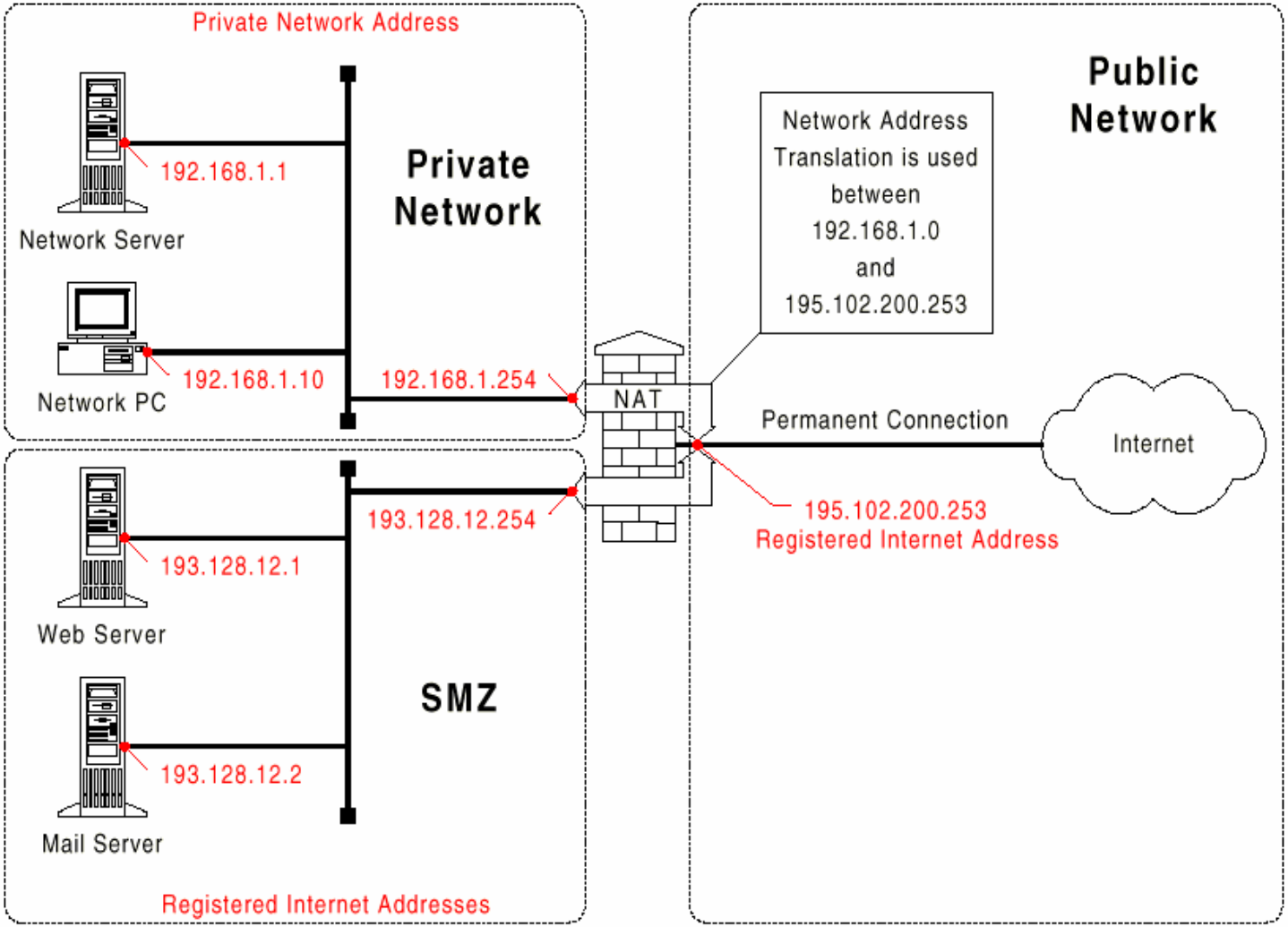
Configuraciones Firewall



Configuraciones Firewall

- SET Q931=0 PROF=ETB NUM1=12345
- ADD ISDN CALL=INTERNET NUMBER=0121345678 PREC=OUT DIRECTION=OUT
- CREATE PPP=0 IDLE=30 OVER=ISDN-INTERNET IPREQUEST=ON
- SET PPP=0 OVER=ISDN-INTERNET USERNAME="USER1" PASSWORD="LET-ME-IN" LQR=OFF
- ENABLE IP
- ENABLE IP REMOTE
- ADD IP INT=ETH0 IP=192.168.1.254
- ADD IP INT=PPP0 IP=195.102.200.253
- ADD IP INT=ETH1 IP=193.128.12.254
- ADD IP ROU=0.0.0.0 MASK=0.0.0.0 INT=PPP0 NEXT=0.0.0.0
- ENABLE FIREWALL
- CREATE FIREWALL POLICY="OFFICE"
- ADD FIREWALL POLICY="OFFICE" INT=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY="OFFICE" INT=PPP0 TYPE=PUBLIC
- ADD FIREWALL POLICY="OFFICE" INT=ETH1 TYPE=PUBLIC
- ADD FIREWALL POLICY=OFFICE NAT=ENHANCED INTERFACE=ETH0 GBLINTERFACE=PPP0 GBLIP=195.102.200.253

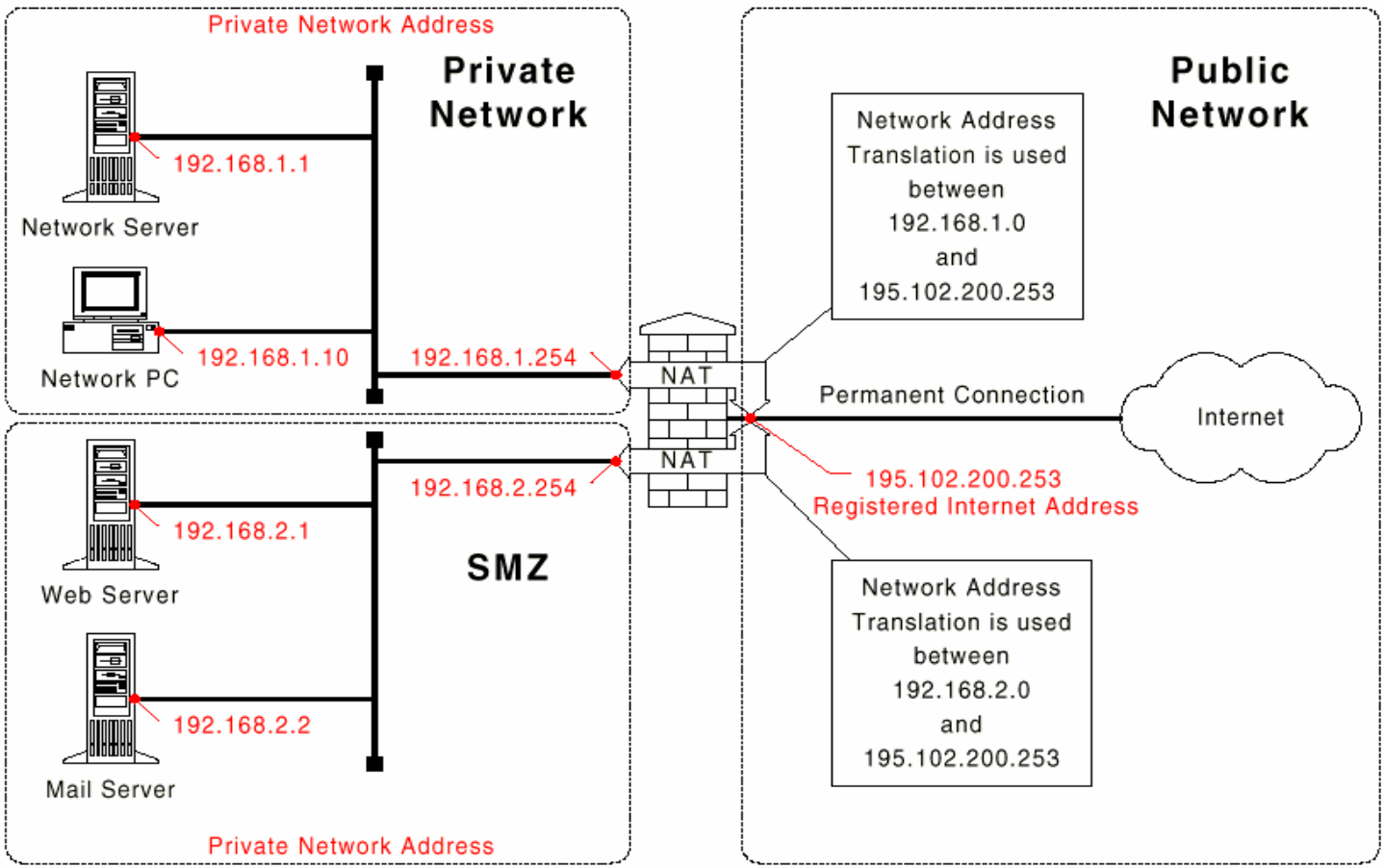
Configuraciones Firewall



Configuraciones Firewall

- SET Q931=0 PROF=ETB NUM1=12345
- ADD ISDN CALL=INTERNET NUMBER=0121345678 PREC=OUT DIRECTION=OUT
- CREATE PPP=0 IDLE=30 OVER=ISDN-INTERNET IPREQUEST=ON
- SET PPP=0 OVER=ISDN-INTERNET USERNAME="USER1" PASSWORD="LET-ME-IN" LQR=OFF
- ENABLE IP
- ENABLE IP REMOTE
- ADD IP INT=ETH0 IP=192.168.1.254
- ADD IP INT=PPP0 IP=195.102.200.253
- ADD IP INT=ETH1 IP=193.128.12.254
- ADD IP ROU=0.0.0.0 MASK=0.0.0.0 INT=PPP0 NEXT=0.0.0.0
- ENABLE FIREWALL
- CREATE FIREWALL POLICY="OFFICE"
- CREATE FIREWALL POLICY="SMZ"
- ADD FIREWALL POLICY="OFFICE" INT=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY="OFFICE" INT=PPP0 TYPE=PUBLIC
- ADD FIREWALL POLICY="OFFICE" INT=ETH1 TYPE=PRIVATE
- ADD FIREWALL POLICY=OFFICE NAT=ENHANCED INTERFACE=ETH0 GBLINTERFACE=PPP0 GBLIP=195.102.200.253
- ADD FIREWALL POLICY=OFFICE RULE=1 ACTION=ALLOW INT=PPP0 PROT=TCP PORT=25 IP=193.128.12.2
- ADD FIREWALL POLICY="OFFICE" RULE=2 ACTION=ALLOW INT=PPP0 PROTOCOL=TCP PORT=80 IP=193.128.12.3

Configuraciones Firewall



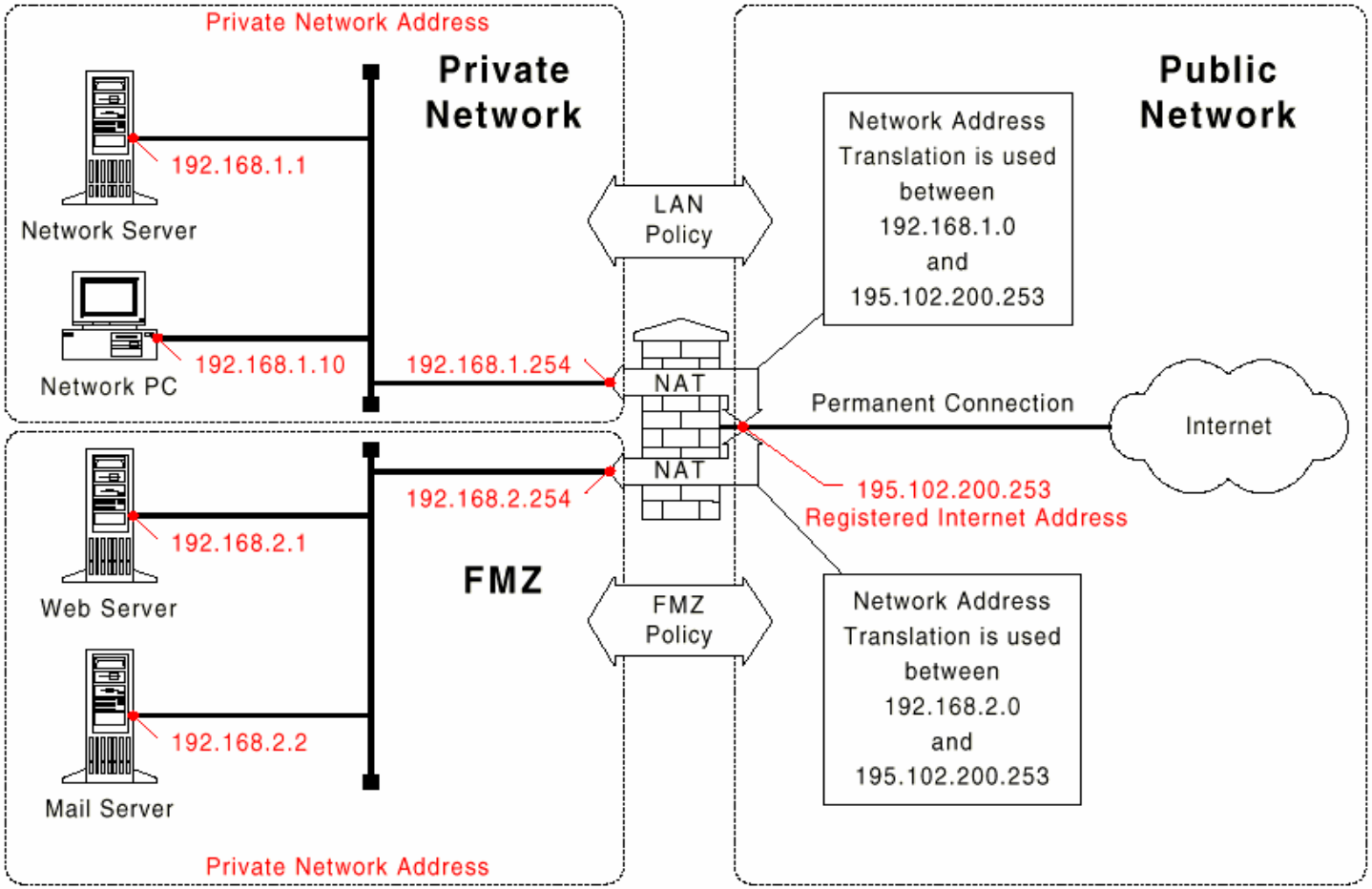
Configuraciones Firewall

- SET Q931=0 PROF=ETB NUM1=12345
- ADD ISDN CALL=INTERNET NUMBER=0121345678 PREC=OUT DIRECTION=OUT
- CREATE PPP=0 IDLE=30 OVER=ISDN-INTERNET IPREQUEST=ON
- SET PPP=0 OVER=ISDN-INTERNET USERNAME="USER1" PASSWORD="LET-ME-IN" LQR=OFF
- ENABLE IP
- ENABLE IP REMOTE
- ADD IP INT=ETH0 IP=192.168.1.254
- ADD IP INT=PPP0 IP=195.102.200.253
- ADD IP INT=ETH1 IP=192.168.2.254
- ADD IP ROU=0.0.0.0 MASK=0.0.0.0 INT=PPP0 NEXT=0.0.0.0
- ENABLE FIREWALL
- CREATE FIREWALL POLICY="OFFICE"
- ADD FIREWALL POLICY="OFFICE" INT=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY="OFFICE" INT=PPP0 TYPE=PUBLIC
- ADD FIREWALL POLICY="OFFICE" INT=ETH1 TYPE=PRIVATE
- ADD FIREWALL POLICY=OFFICE NAT=ENHANCED INTERFACE=ETH0 GBLINTERFACE=PPP0 GBLIP=195.102.200.253
- ADD FIREWALL POLICY="OFFICE" NAT=ENHANCED INT=ETH1 GBLINT=PPP0 GBLIP=195.102.200.253

Configuraciones Firewall

- ADD FIREWALL POLICY=OFFICE RULE=1 ACTION=ALLOW INT=PPP0 PROT=TCP PORT=25 IP=192.168.2.2 gblip=195.102.200.253 gblport=80
- ADD FIREWALL POLICY="OFFICE" RULE=2 ACTION=ALLOW INT=PPP0 PROTOCOL=TCP PORT=80 IP=192.168.2.3 gblip=195.102.200.253 gblport=80

Configuraciones Firewall



Configuraciones Firewall

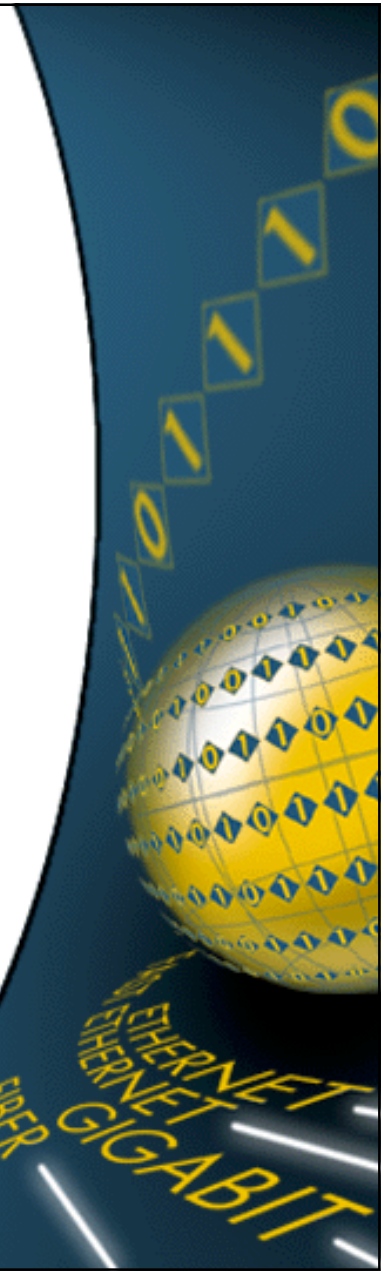
- SET Q931=0 PROF=ETB NUM1=12345
- ADD ISDN CALL=INTERNET NUMBER=0121345678 PREC=OUT DIRECTION=OUT
- CREATE PPP=0 IDLE=30 OVER=ISDN-INTERNET IPREQUEST=ON
- SET PPP=0 OVER=ISDN-INTERNET USERNAME="USER1" PASSWORD="LET-ME-IN" LQR=OFF
- ENABLE IP
- ENABLE IP REMOTE
- ADD IP INT=ETH0 IP=192.168.1.254
- ADD IP INT=PPP0 IP=195.102.200.253
- ADD IP INT=ETH1 IP=192.168.2.254
- ADD IP ROU=0.0.0.0 MASK=0.0.0.0 INT=PPP0 NEXT=0.0.0.0
- ENABLE FIREWALL
- CREATE FIREWALL POLICY="OFFICE"
- CREATE FIREWALL POLICY="SMZ"
- ADD FIREWALL POLICY=OFFICE INTERFACE=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY=OFFICE INTERFACE=PPP0 TYPE=PUBLIC
- ADD FIREWALL POLICY=SMZ INTERFACE=ETH0 TYPE=PRIVATE
- ADD FIREWALL POLICY=SMZ INTERFACE=PPP0 TYPE=PUBLIC

Configuraciones Firewall

- ADD FIREWALL POLICY="OFFICE" NAT=ENHANCED INT=ETH0 GBLINT=PPP0 GBLIP=195.102.200.253
- ADD FIREWALL POLICY="SMZ" NAT=ENHANCED INT=ETH1 GBLINT=PPP0 GBLIP=195.102.200.253
- ADD FIREWALL POLICY=SMZ RULE=1 ACTION=ALLOW INT=PPP0 PROT=TCP PORT=25 IP=192.168.2.2 gblip=195.102.200.253 gblport=80
- ADD FIREWALL POLICY="SMZ" RULE=2 ACTION=ALLOW INT=PPP0 PROTOCOL=TCP PORT=80 IP=192.168.2.3 gblip=195.102.200.253 gblport=80

REDES PRIVADAS VIRTUALES

VPN



Allied Telesyn SIMPLY CONNECTING THE WORLD

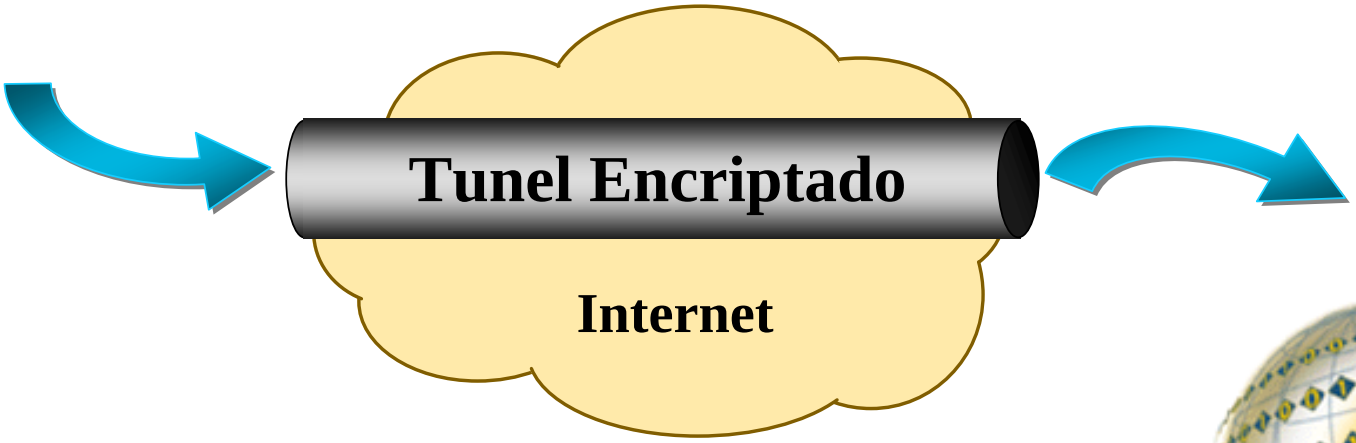
VPN

- **Una red privada creada utilizando una red pública o compartida - como internet - la cual provee seguridad, calidad de servicio, gestión y rentabilidad/escalabilidad equivalentes a la de una red privada.**

Allied Telesyn SIMPLY CONNECTING THE WORLD

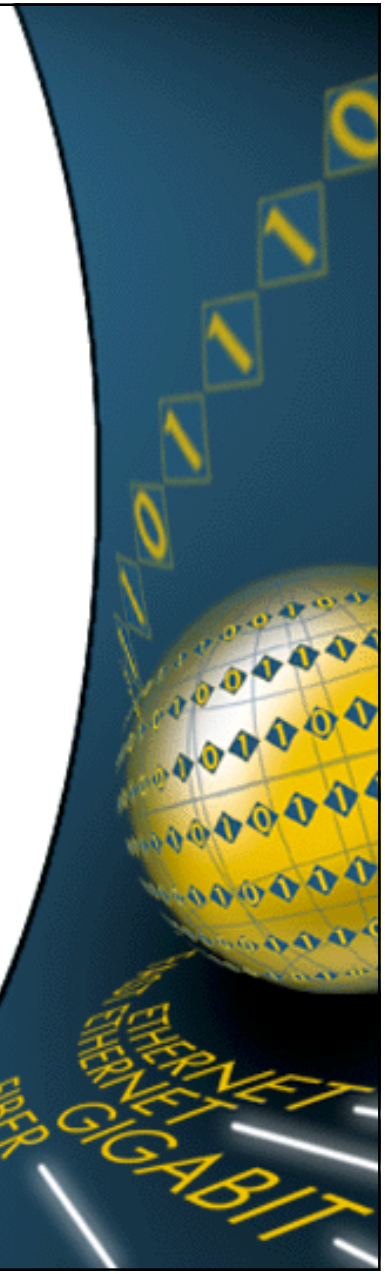
VPN - Tunneling

- Layer 3 tunnels
  - IPSec, GRE
- Layer 2 tunnels
  - L2TP



LAYER 2 TUNNELING PROTOCOL

L2TP



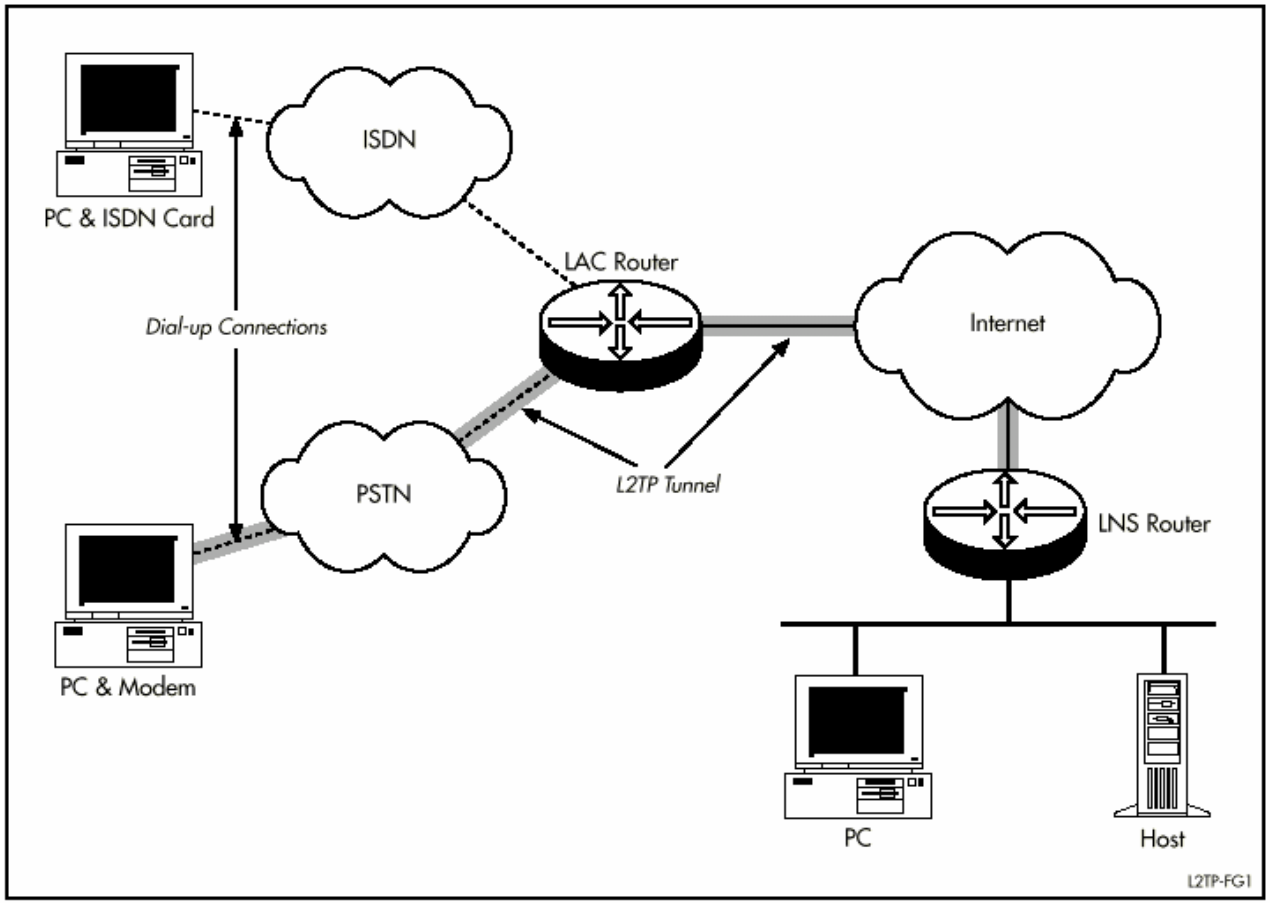
Allied Telesyn SIMPLY CONNECTING THE WORLD

Layer 2 Tunneling Protocol - L2TP

- Tunel de nivel 2
- Está definido en el RFC 2661
- Dos entidades:
  - L2TP Access Concentrator (LAC)
  - L2TP Network Server (LNS)
- Utilizado en Infovia Plus

Allied Telesyn SIMPLY CONNECTING THE WORLD

Layer 2 Tunneling Protocol - L2TP



Configuración L2TP por Internet

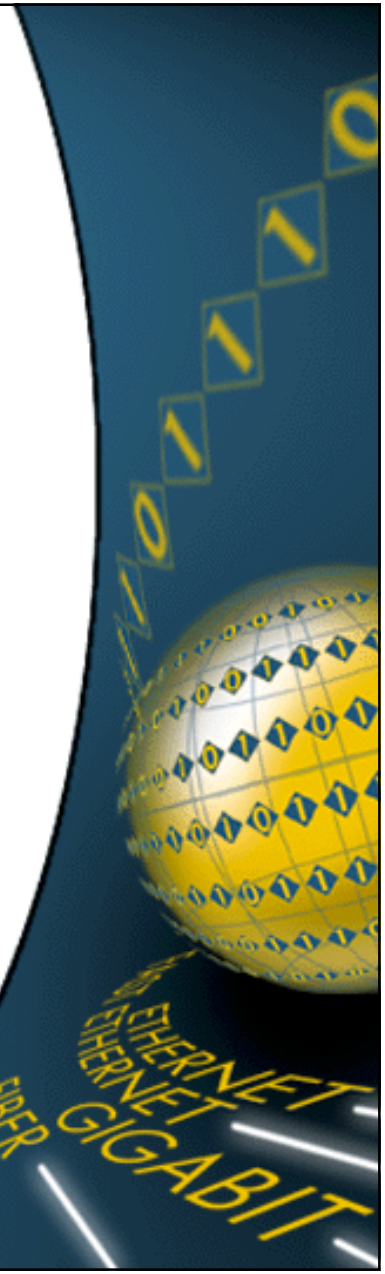
- ROUTER A:
- Set q931=0 num1=123 prof=etb
- enable ip
- add ip int=eth0 ip=10.1.1.1 mask=255.255.255.0
- add isdn call=isp numb=456 prec=out inany=on
- create ppp=0 over=isdn-isp idle=on lqr=off username=login pass=password
- add ip int=ppp0 ip=195.160.224.34
- add ip route=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
- enable l2tp
- enable l2tp server=both
- add l2tp call=test remote=test type=virtual ip=195.160.224.40 prec=out
- create ppp=1 over=tnl-test idle=180
- add ip int=ppp1 ip=0.0.0.0
- add ip route ip=10.2.2.0 mask=255.255.255.0 int=ppp1 next=0.0.0.0

Configuración L2TP por Internet

- ROUTER B:
- Set q931=0 num1=123 prof=etb
- enable ip
- add ip int=eth0 ip=10.2.2.1 mask=255.255.255.0
- add isdn call=isp numb=456 prec=in inany=on
- create ppp=0 over=isdn-isp idle=on lqr=off username=login pass=password
- add ip int=ppp0 ip=195.160.224.40
- add ip route=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
- enable l2tp
- enable l2tp server=both
- add l2tp call=test remote=test type=virtual ip=195.160.224.34 prec=out
- create ppp=1 over=tnl-test idle=180
- add ip int=ppp1 ip=0.0.0.0
- add ip route ip=10.1.1.0 mask=255.255.255.0 int=ppp1 next=0.0.0.0

GENERIC ROUTING ENCAPSULATION

GRE



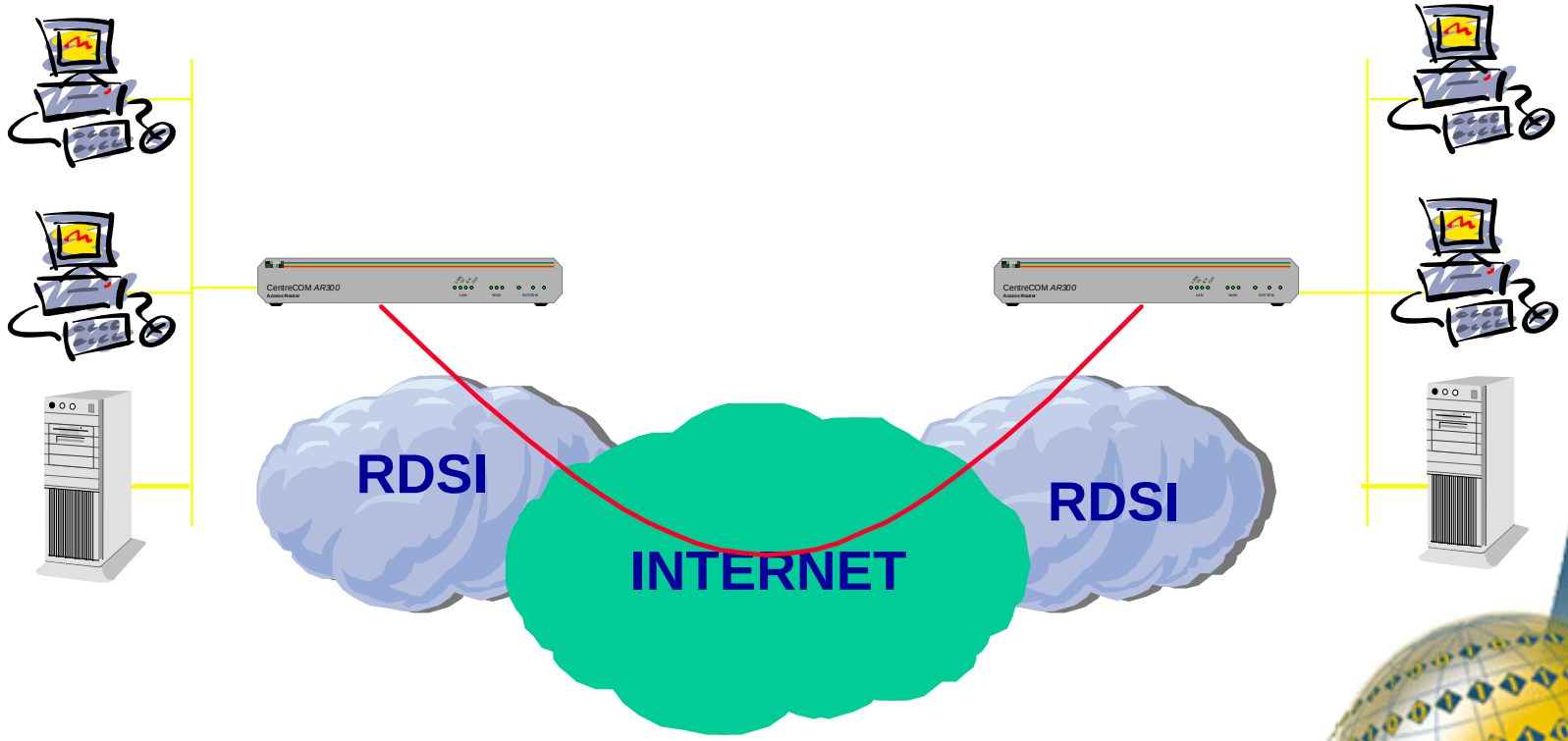
Allied Telesyn SIMPLY CONNECTING THE WORLD

GRE

- Generic Routing Encapsulation (GRE)
- Definido el genérico en RFC 1701 y la implementación sobre IP en RFC 1702
- Tunel de nivel 3
- IP encapsulado sobre IP

Allied Telesyn SIMPLY CONNECTING THE WORLD

VPN con GRE

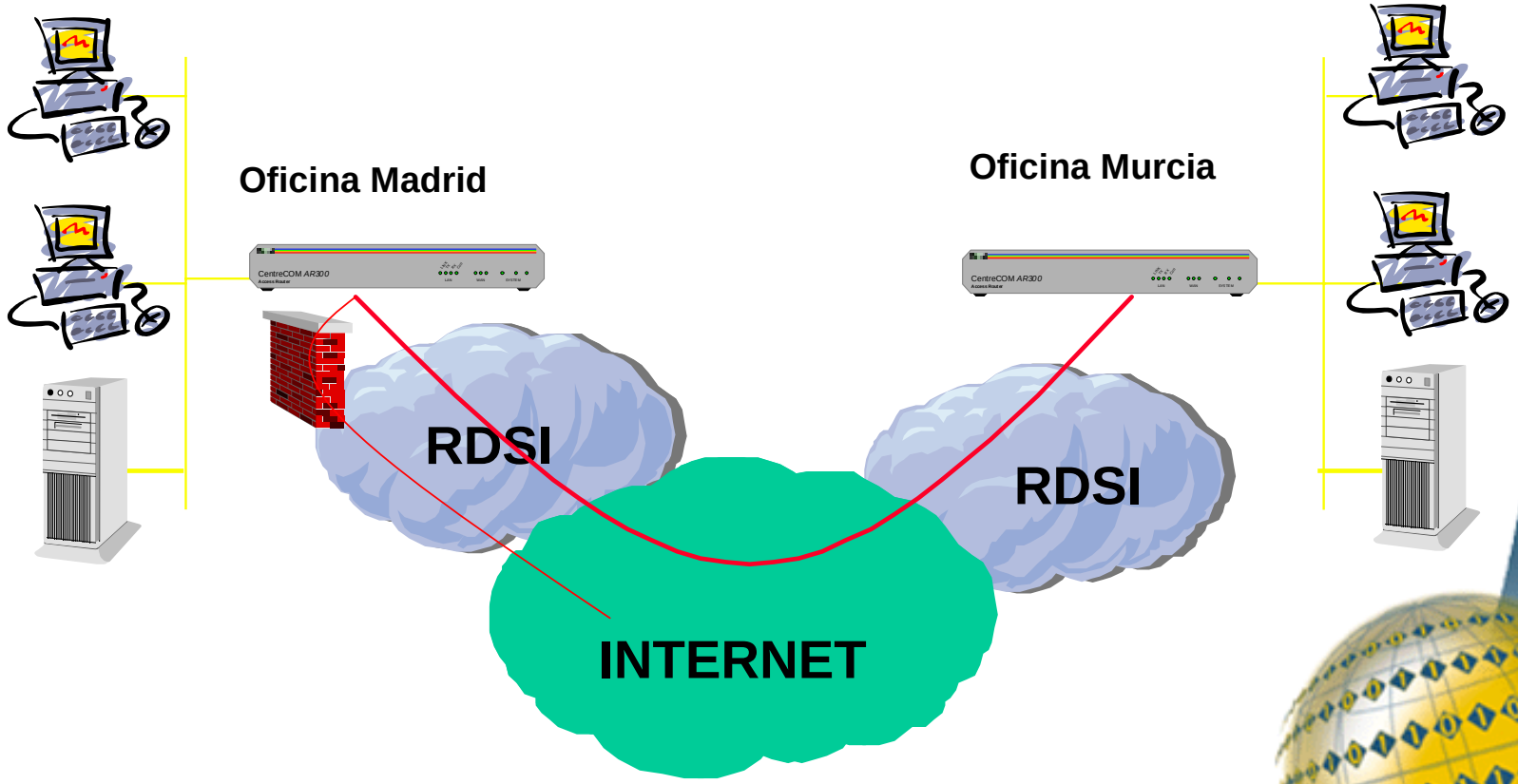


Allied Telesyn
SIMPLY CONNECTING THE WORLD

Config VPN con GRE

- Set q931=0 num1=123 prof=etb
- enable ip
- add ip int=eth0 ip=1.1.1.1 mask=255.255.255.0
- add isdn call=isp numb=456 prec=out inany=on
- create ppp=0 over=isdn-isp idle=on lqr=off username=login pass=password
- add ip int=ppp0 ip=195.160.224.34
- add ip route=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
- add gre=1 source=1.1.1.0 smask=255.255.255.0 dest=192.168.2.0 dmask=255.255.255.0 targ=195.160.224.40
- enable gre
- set ip int=eth0 gre=1
- set ip local gre=1

VPN con GRE + Internet

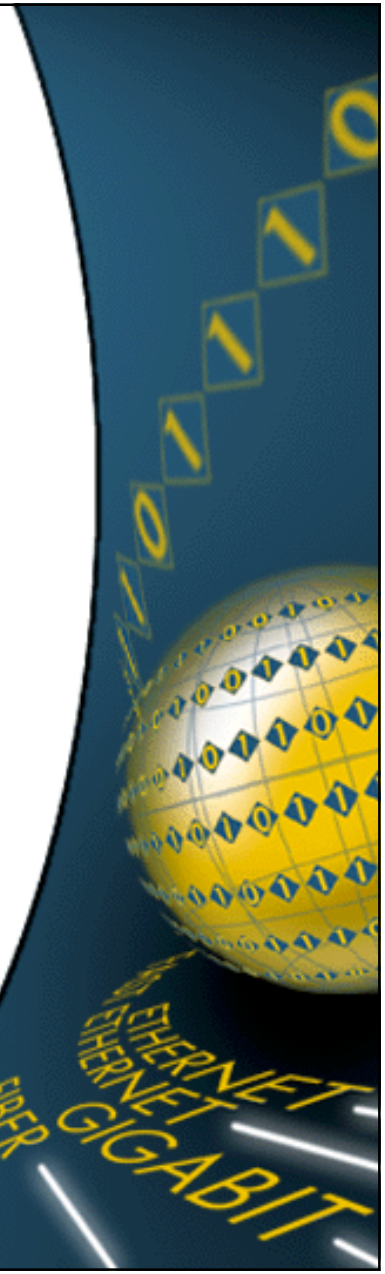


Allied Telesyn
SIMPLY CONNECTING THE WORLD

Config VPN con GRE + Internet

- Set q931=0 num1=123 prof=etb
- add isdn call=isp numb=456 prec=out inany=on
- create ppp=0 over=isdn-isp idle=on lqr=off username=login pass=password
- enable ip
- add ip int=eth0 ip=192.168.0.90
- add ip int=ppp0 ip=195.57.183.230
- add ip route=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
- enable ip nat
- add ip nat=192.168.0.0 mask=255.255.255.0 gblip=195.57.183.230
- enable gre
- add gre=1 source=192.168.0.0 mask=255.255.255.0 dest=192.168.1.0 dmask=255.255.255.0 target=195.57.183.229
- set ip int=eth0 gre=1
- set ip local gre=1

Encriptación
y
Autenficación



Allied Telesyn SIMPLY CONNECTING THE WORLD

Encriptación

- **¿Qué es encriptación?**
  - Es el proceso de convertir los datos originales (texto plano) en un formato encriptado (texto cifrado).
  - Se realiza aplicando un algoritmo de encriptación y una clave.
  - Debido a que el tipo de algoritmo utilizado es facil de descubrir, la seguridad reside en el secreto de la clave.

Tipos de Encriptación

- Encriptación Simétrica:
  - Una única clave es utilizada para encriptar y desencriptar.
  - Cualquiera que tenga acceso a la clave puede desencriptar el texto cifrado.
  - Debido a que la clave de encriptación debe guardarse en secreto, son llamados privados o de clave secreta.
  - DES, 3DES, IDEA, RC-2,4,5, Blowfish, .., son algoritmos de encriptación simétrica.

Tipos de Encriptación

- Encriptación Asimétrica:
  - Utilizan 2 claves, una para encriptar y otra para desencriptar.
  - La clave de encriptación es llamada clave pública debido a que esta clave no puede desencriptar el mensaje y por lo tanto no tiene que guardarse en secreto.
  - La clave de desencriptación o clave privada necesita guardarse en secreto.
  - Este tipo de algoritmos son conocidos también como algoritmos de clave pública de encriptación

Tipos de Encriptación

- La clave pública y privada no pueden ser aleatoriamente generadas y deben ser generadas juntas.
- RSA y Diffie Hellman son los algoritmos de encriptación asimétrica mas utilizados.
- Normalmente la estación de desencriptación genera el par de claves y distribuye la clave pública a las estaciones de encriptación, la distribución de estas claves públicas no necesitan ser guardadas en secreto, pero debe ser protegida contra la sustitución o modificación.

Tipos de Encriptación

- Requiere grandes recursos de CPU, siendo más lenta si la comparamos con los algoritmos simétricos.
- Por esta razón normalmente sólo son utilizados para pequeños bloques de datos, por ejemplo para intercambio de claves en algoritmos simétricos.
- Otro uso de este tipo de algoritmos es la firma digital.

FIRMA DIGITAL

- La estación firmante publica como clave pública y los mensajes firmados son desencriptados en el receptor con la clave privada, para verificar el origen del mensaje el receptor encripta el mensaje con la clave pública publicada y si el mensaje que resulta es válido entonces la estación firmante es autentificada como la fuente del mensaje.

Modos de Encriptación

- Link Encryption
  - Encriptación de la conexión.
  - Encripta todo el paquete incluido las cabeceras de la capa de red utilizadas para routing.
  - No transparencia y alta latencia
- Payload Encryption
  - Encriptación de la carga
  - Encripta paquetes en la capa de red sin cambiar las cabeceras.
  - Transparente para otros routers

Algoritmos de Encriptación

- Los mas utilizados son:
  - Simétricos:
    - DES
    - 3DES
  - Asimétricos:
    - RSA
    - Diffie Hellman

Allied Telesyn SIMPLY CONNECTING THE WORLD

DES

- Llamado también Lucifer, fué creado por IBM.
- Utiliza bloques de 64 bits y el tamaño de la clave es de 56 bits
- Ha resistido el test del tiempo y ha demostrado ser un algoritmo altamente seguro.
- La conformidad total con el estandar está basado en hardware, las implementaciones software son solamente compatibles y no DES compliant.
- DES ha sido optimizado para producir muy alta velocidad en las implementaciones hardware, es ideal para redes donde se necesitan altas prestaciones y baja latencia.

DES

- DES puede utilizarse en varios modos:
  - ELECTRONIC CODE BOOK (ECB), es la función fundamental DES. El texto plano es dividido en bloques de 64 bits, los cuales son encriptados con el algoritmo DES y la clave y para un determinado bloque de entrada de texto plano ECB produce el mismo bloque de texto cifrado.
  - CIPHER BLOCK CHAINING (CBC), es la forma mas popular de DES, CBC opera en bloques de 64 bits pero incluye una realimentación por la cual cadenas de bloques consecutivos de texto plano repetitivo (blancos en ASCII) no es siempre idéntico texto cifrado. CBC también introduce una dependencia entre bloques de datos la cual protege contra la inserción de datos fraudulentos y atauqes de repetición. La realimentación para el primer bloque de datos es proveida por 64 bits del vector de inicialización (IV). Este es el modo DES utilizado por los routers.

DES

- CIPHER FEEDBACK (CFB), es un método que añade una cadena de datos cifrados la cual la utiliza para generar una cadena binaria pseudo-aleatoria que combinada con el texto plano produce el texto cifrado, el texto cifrado entonces es realimentado para formar una porción del siguiente bloque DES.
- OUTPUT FEEDBACK (OFB), combina el primer vector de inicialización (IV) con el texto plano para formar el texto cifrado, el texto cifrado es utilizado como el siguiente IV.

3DES

- Es una simple variante del algoritmo DES en modo CBC.
- La función DES es reemplazada por 3 ciclos de esta misma función: encriptación seguida de desencriptación y seguida de encriptación.
- Puede ejecutarse utilizando 2 claves DES (112 bits) o 3 claves DES (168 bits).
- 2 claves: encripta con la primera, desencripta con la segunda y vuelve a encriptar con la primera.
- 3 claves: utiliza una clave para cada proceso, este está condiderado como el algoritmo más seguro debido a la longitud de su clave.

3DES

- Hay varios modos de utilización de 3DES, los dos mas comunes son:
  - INNER CBC MODE, encripta el paquete entero en CBC 3 veces y requiere 3 diferentes IV's.
  - OUTER CBC MODE, realiza una triple encriptación cada bloque de 8 bytes de un paquete en modo CBC 3 veces y requiere 1 IV.

RSA

- Utiliza operaciones matemáticas por las cuales es relativamente fácil el cálculo en un sentido pero que no tiene soluciones conocidas en el contrario.
- La clave pública utilizada es de 512 bits o superior.
- Las claves RSA pueden ser generadas por un dispositivo externo y ser importadas com un fichero de texto con extensión “.key”, la clave RSA generada en el router puede ser exportada a un fichero de texto para transferirlo a otro dispositivo.
- La generación de las claves RSA es un proceso que consume mucho tiempo y recursos del procesador.
- Se deben crear 2 números primos aleatorios muy largos y son combinados para formar la clave RSA.

RSA

- El método mas rápido para generar un número primo muy largo es generar un número aleatorio muy largo y mirar si es primo, si no lo es, se modifica se vuelve a comprobar.
- Debido a que este proceso es muy aleatorio puede tardar entre 3 segundos y 30 minutos, dependiendo de la longitud de la clave y del procesador, para asegurar el normal funcionamiento del router , la clave RSA se genera como una tarea de background.

Diffie Hellman

- Es uno de los mas utilizados en los algoritmos de intercambio de clave.
- No es un algoritmo de encriptación porque los mensajes pueden no estar encriptados.
- Provee un método para que dos partes generen la misma clave compartida con la seguridad que otra parte no puede generar el mismo valor y utiliza clave pública criptográfica.
- La dificultad se basa en resolver el “problema de logaritmo discreto” el cual puede ser comparado con la dificultad de fabricar enteros muy largos.
- DH requiere mas computación que RSA, pero no necesita del intercambio inicial de clave pública.

Diffie Hellman

- Los valores de la clave pública menores de 768 bits son considerados como inseguros.
- El intercambio DH se realiza en dos fases:
  - En la primera se genera en local un número aleatorio muy largo, es combinado con el valor de la clave pública y transmitido hacia la otra parte en el intercambio de clave.
  - En la segunda fase la clave secreta compartida es generada desde el valor intercambiado y el valor del número aleatorio local.
  - Cada fase se descompone en pequeñas piezas de procesamiento debido a la intensa carga del procesador en el cálculo de las claves públicas, como resultado el intercambio de clave es largo, pero asegura que la operativa general del router no se pare durante este proceso.

Autentificación

- Necesidad de verificar que los datos no sean alterados.
- La autentificación opera calculando un código de autentificación de mensaje (MAC - MESSAGE AUTHENTICATION CODE), referido como HASH, de los datos originales y añadido al mensaje, cuando el router remoto recibe el mensaje calcula otra MAC y la chequea con la MAC procedente del mensaje, si son idénticas el mensaje es auténtico.
- Típicamente la MAC es calculada usando A KEYED ONE WAY HASH ALGORITHM, opera con un mensaje de longitud variable y una clave y devuelve un HASH de longitud fija.

Autentificación

- Las propiedades que hacen de la función HASH un único camino son:
  - Es muy facil calcular la función HASH desde el mensaje y la clave
  - Es muy complicado computar el mensaje y la clave desde el HASH.
  - Es muy complicado encontrar otro mensaje y clave que arrojen el mismo HASH.
- Los algoritmos mas utilizados son:
  - MD-5 (Message Digest 5), devuelve un hash de 128 bits.
  - SHA-1 (Secure Hash Algorithm 1), devuelve un hash de 160 bits.
- MD-5 es mas rápido que SHA-1, pero este último es generalmente mas utilizado por ser ligeramente mas seguro.

Algoritmos de Intercambio de Clave

- Son utilizados por los routers para generar e intercambiar las claves de encriptación y autentificación con otros routers.
- Sin estos algoritmos las claves de sesión de encriptación deben cambiarse manualmente por el administrador del sistema.
- Habilita a los routers para regenerar automaticamente las claves de sesión y con una base de frecuencia.
- La propiedad mas importante de cualquier algoritmo de intercambio de clave es que sólo las partes que negocian podrán decodificar o generar la clave compartida. Debido a este requerimiento la criptografia de la clave pública juega un papel importante en estos algoritmos.
- La criptografia de la clave pública provee un método de encriptación del mensaje el cual sólo puede ser desencriptado por una parte, el router puede generar una clave de sesión , encriptar la clave , transmitir la clave por un canal inseguro y tener la certeza que la clave sólo puede ser desencriptada por el recipiente deseado.

Algoritmos de Intercambio de Clave

- Los algoritmos de clave simétrica pueden ser utilizados para el intercambio de clave, pero normalmente requiere una clave secreta inicial compartida que debe ser introducida manualmente en todos los routers de la red segura.
- Diffie Hellman es uno de los algritmos utilizados con mas frecuencia en estos algoritmos.

Creación y almacenaje de Claves

- Las claves son creadas por el módulo ENCO y almacenadas en la flash.
- Los tipos de claves son:
  - DES, utilizada para encriptación DES
  - 3DES2KEY, utilizada para 3DES con 2 claves (112 bits) en modo OUTER CBC
  - 3DESINNER, utilizada para 3DES con 3 claves (168 bits) en modo INNER CBC.
  - RSA, utilizada por RSA
  - GENERAL, utilizada para autentificación HMAC (SHA-1 y MD-5) e ISAKMP (Clave pre compartida)

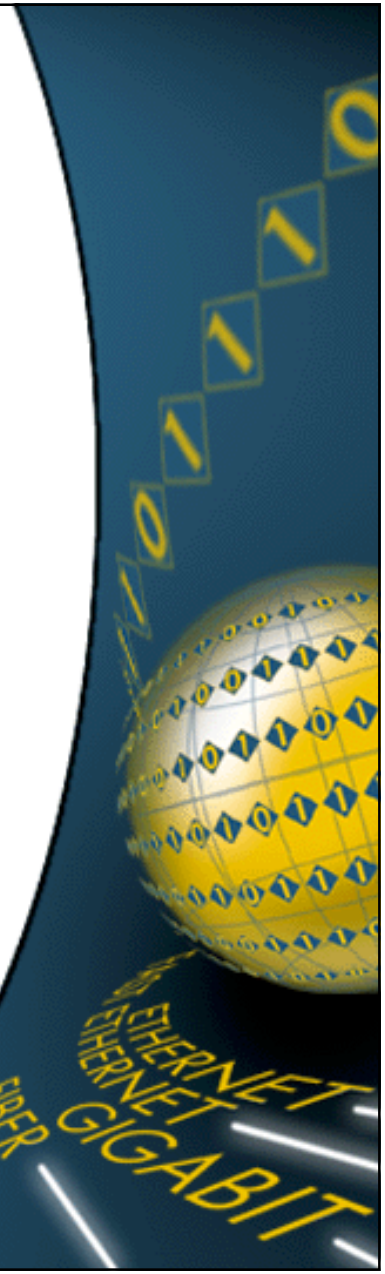
Creación y almacenaje de Claves

- Cada clave creada y almacenada en el router tiene un único número de identificación, cada clave tiene unos atributos incluyendo el módulo de usuario asociado con la clave. Por ejemplo ISAKMP y SSH utiliza la dirección IP como atributo de las claves RSA para encontrar la clave pública del extremo remoto.

Funcionamiento

- Cuando la encriptación es configurada y habilitada, el router debe ser puesto en modo de seguridad, utilizando el comando **“enable system security_mode”**
- Las claves creadas en el router si no está en mod seguridad serán destruidas cuando el router es rearrancado, hay que habilitar el modo seguridad antes de crear las claves.
- Cuando el router está en modo seguridad, sólo los usuarios con privilegios de **“security officer”** pueden ejecutar comandos que podrian impactar la seguridad del router y sus claves.
- Todas las claves pueden ser borradas deshabilitando el modo de seguridad con **“disable system security_mode”**

IPSec



Allied Telesyn SIMPLY CONNECTING THE WORLD

¿Que es IPSec?

- Autentificación y encriptación en la capa de red.
- Estandar abierto para asegurar las comunicacones privadas.
- Provee un necesario componente basado en estandars, solución flexible para desplegar una política de seguridad en una WAN.

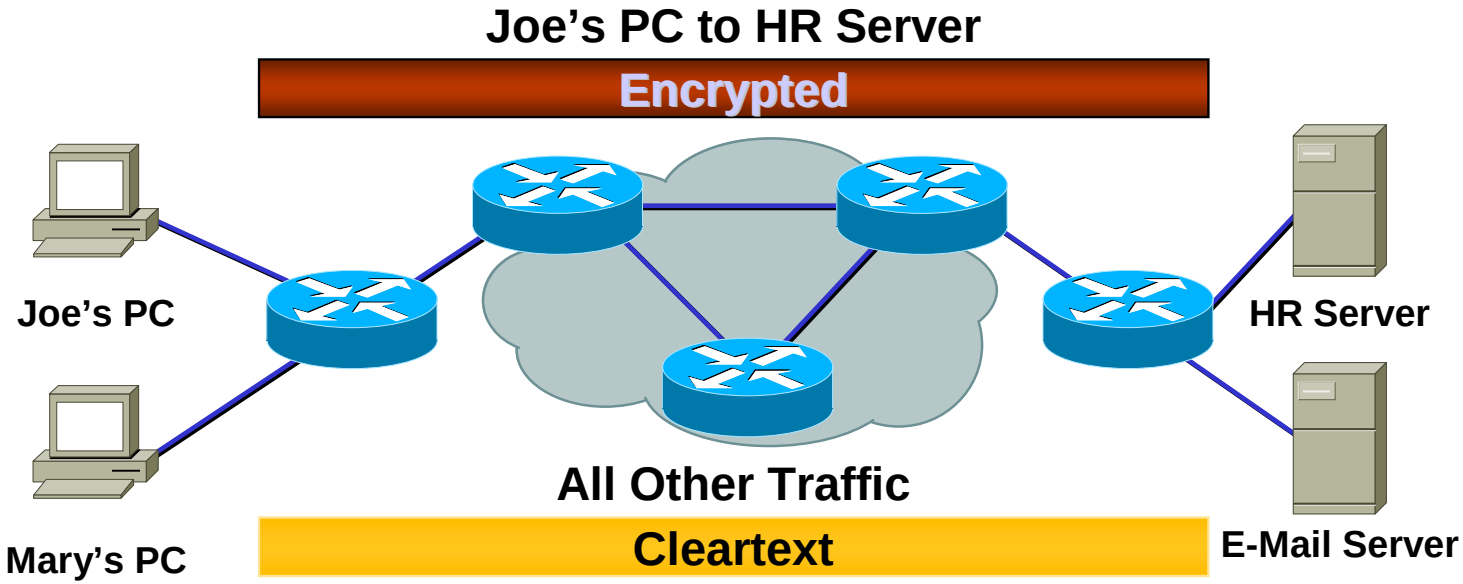
Beneficios de IPSec

- Estandar para privacidad, integridad y autenticidad para comercio en la red
- Implementado transparentemente en la infrastuctura de la red.
- Solución de seguridad end-to-end incluyendo routers, firewalls, PCs y servidores.

IPSec Servicios de Seguridad

- Integridad de conexiones, asegura que los datos no han sido cambiados en el camino.
- Autentificación de los datos, identifica quien envia los datos
- Protección anti reproducción, detecta los paquetes recibidos más de una vez para ayudar a protegerlos
- Confidencialidad (encriptación), asegura que los datos no han sido leidos en el camino

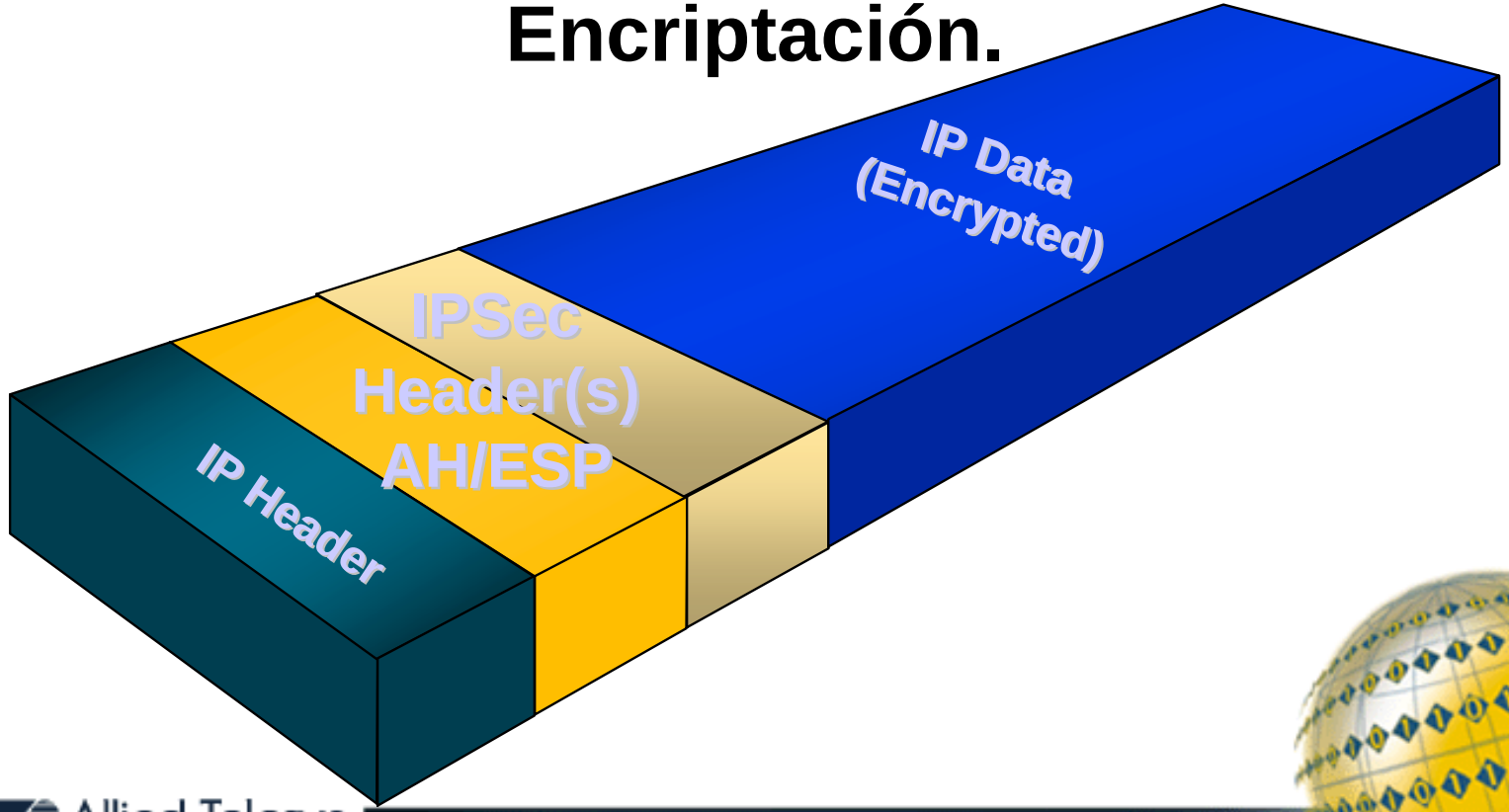
Seguridad en la Capa de Red



- Protege el tráfico flujo a flujo entre hosts específicos o subredes
- Independiente del interface y del medio
- Transparente para los dispositivos intermedios
- Independiente de la Topología

IPsec

Interoperación de Autentificación, Integridad y Encriptación.



Allied Telesyn
SIMPLY CONNECTING THE WORLD

¿Quién provee los servicios de seguridad?

- Dos protocolos se encargan de aportar estos servicios:
  - Authentication Header - AH
  - Encapsulating Security Payload - ESP

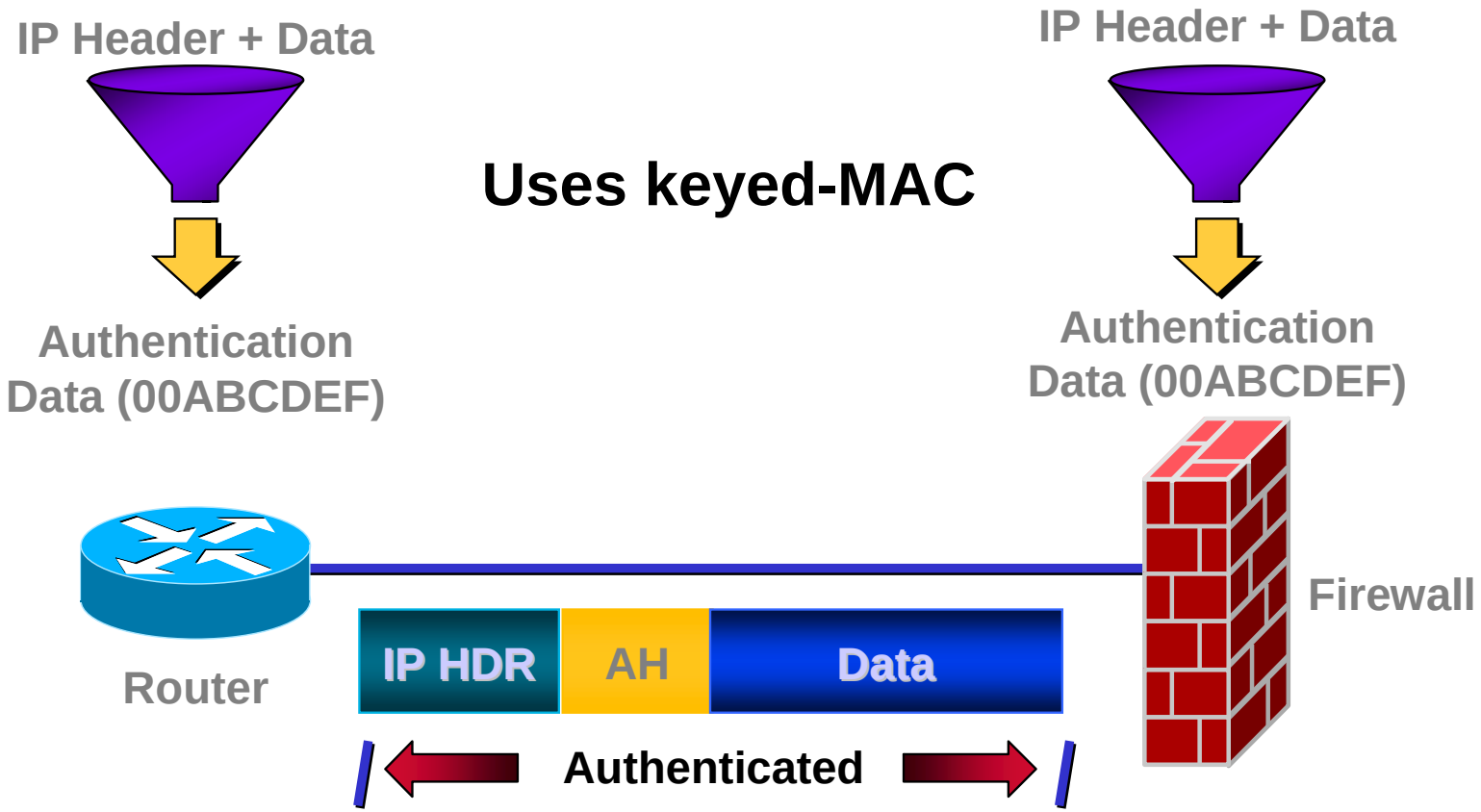
- Son independientes y se pueden utilizar uno de ellos o los dos.

Authentication Header (AH)

- Integridad de los datos
- Autentificación de los datos de origen
- Protección anti reproducción
- Protección de las cabeceras de IP
- No confidencialidad

Allied Telesyn SIMPLY CONNECTING THE WORLD

AH Provee Autentificación de Datos



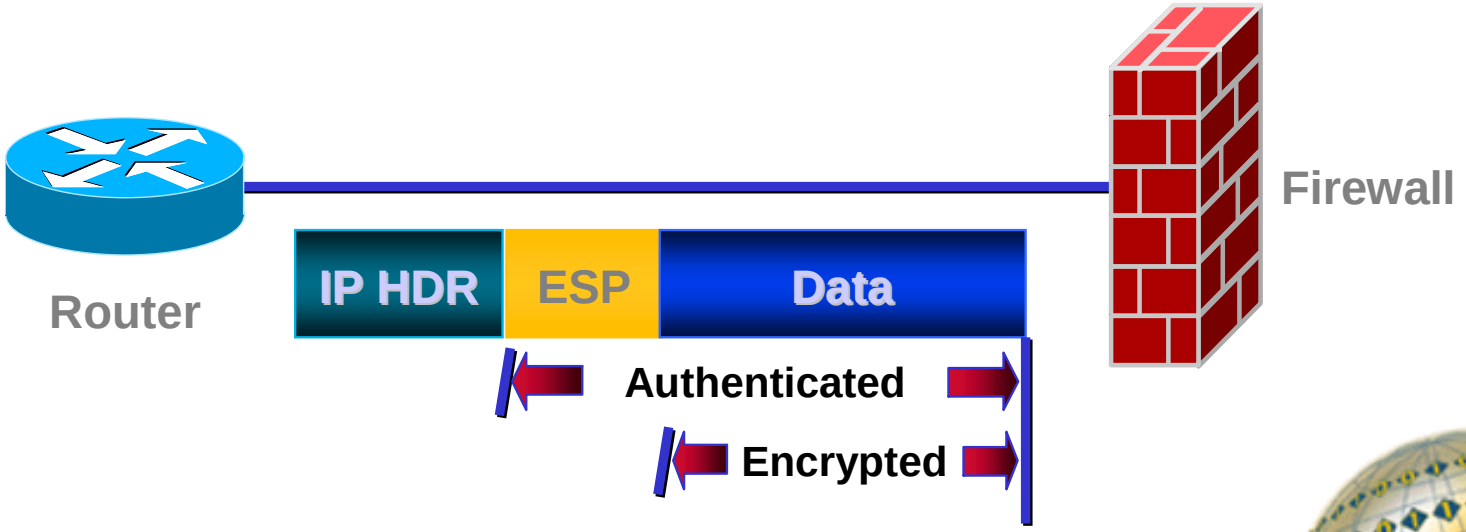
Encapsulating Security Payload (ESP)

- Confidencialidad de los datos
- Limita el flujo de tráfico confidencial
- Integridad de los datos
- Autentificación del origen de los datos
- Protección antireproducción
- No protege la cabecera IP

Allied Telesyn SIMPLY CONNECTING THE WORLD

ESP Confidencialidad e Integridad

Encryption with a Keyed-MAC



Allied Telesyn
SIMPLY CONNECTING THE WORLD

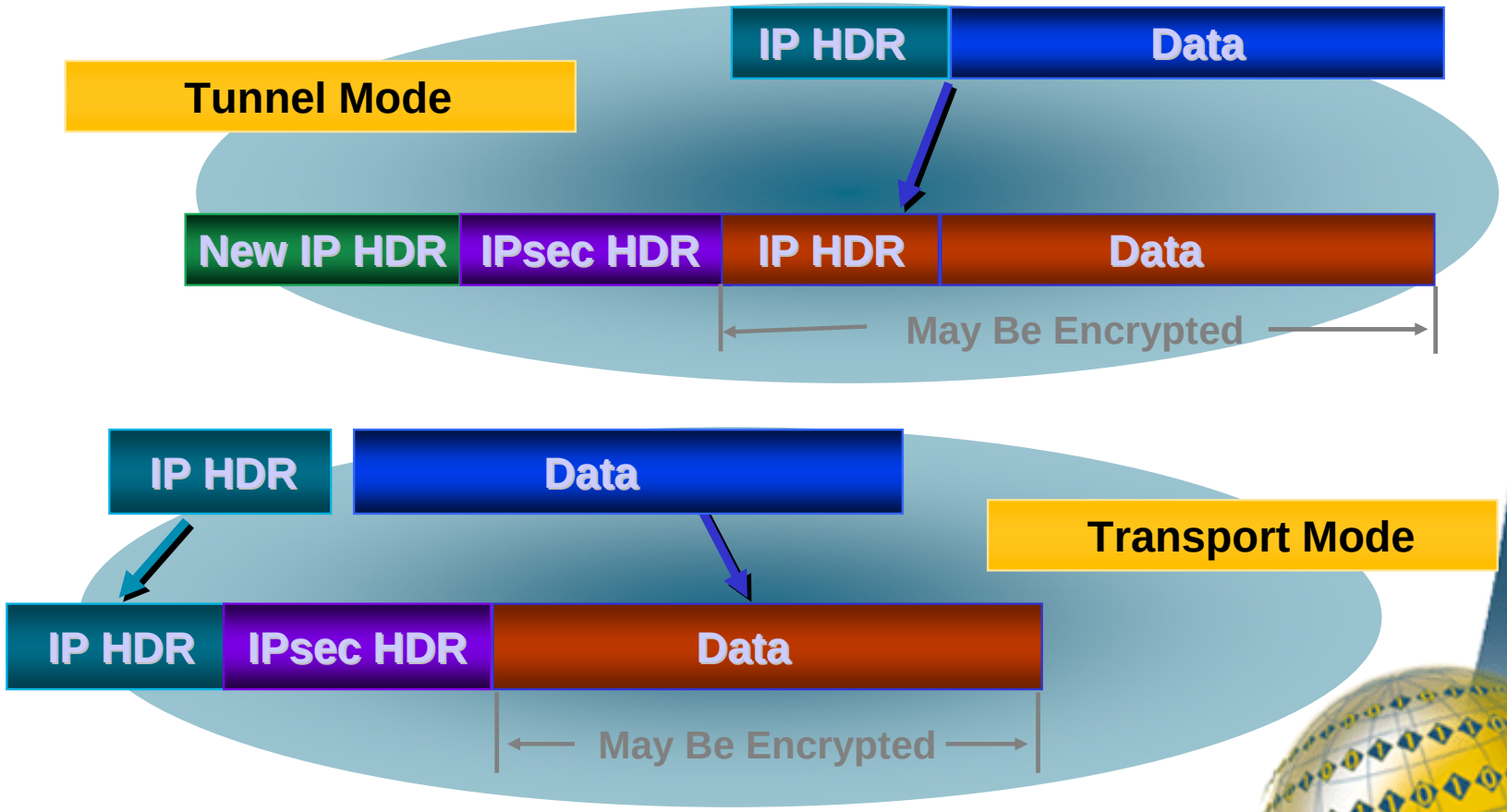
Security Association (SA)

- Contrato entre dos entidades en política de seguridad, incluye:
  - Algoritmo de Encriptación
  - Algoritmo de Autentificación
  - Distribución de claves compartidas
  - SA lifetime
- Conexión entre un par IPSec que provee servicios de seguridad.
- Unidireccional, se crean 2 SA's por conexión, una para tráfico entrante y otra para tráfico saliente.
- La seguridad la provee AH ó ESP, pero no ambos, si se utilizan ambos a la vez se crearán mas de dos SA's para cada conexión.
- Una SA está identificada por el SPI (Security Parameter Index), la dirección IP de destino y un protocolo de seguridad (AH ó ESP)

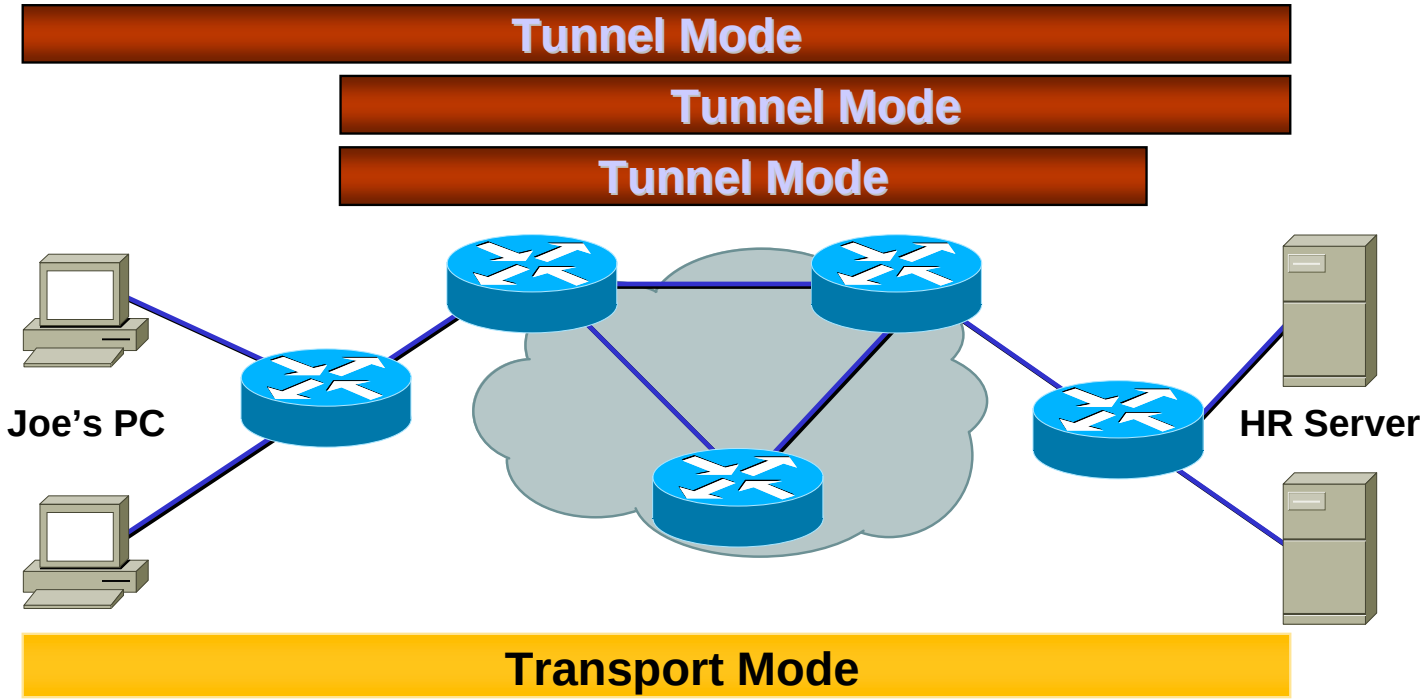
Modos de IPSec

- IPSec trabaja en dos modos, modo transporte y modo tunel:
  - Modo Transporte, se utiliza para SA entre dos hosts, AH y ESP aparecen justo detrás de la cabecera IP, ESP en modo transporte provee seguridad para los protocolos de las capas superiores y sólo encripta los datos y con AH la seguridad es ampliada a las cabeceras IP.
  - Modo Tunel, se aplica a un tunel IP cuando cualquier final de la SA es un gateway de seguridad (router, firewall, ..), esto evita las fragmentaciones reensamblajes de paquetes IPSec. Añade una cabecera IP exterior que especifica el par IPSec y una cabecera IP interior que especifica el último destino del paquete, entre ellas aparece ESP ó AH. Si se utiliza AH los paquetes tunelizados y las cabeceras son protegidas, si se utiliza ESP sólo los paquetes son protegidos.

Modos IPsec


Tunnel Mode
IP HDR
Data
New IP HDR
IPsec HDR
IP HDR
Data
May Be Encrypted
Transport Mode
IP HDR
Data
IP HDR
IPsec HDR
Data
May Be Encrypted

Modos de Tunel y Transporte



- Transport mode for end-to-end session
- Tunnel mode for everything else

Políticas IPSec

- La protección obtenida por una implementación IPSec está basada en los requerimientos definidos por las políticas de IPSec almacenadas en la SPD (Security Policy Database), establecida y mantenida por el security officer.
- IPSec selecciona un paquete IP para ser procesado en uno de los 3 modos posibles:
  - IPSec - Aplica los servisios de seguridad IPSec específicos sobre el paquete.
  - DENY - Descarta los paquetes
  - PERMIT - Permite al paquete saltar IPSec

Políticas de IPSec

- En general el modo para procesar cada paquete IP es determinar una información que concuerde desde la IP y la cabecera de la capa de transporte de un paquete IP con las políticas de IPSec en la SPD.
- Los selectores que soporta IPSec son:
  - IP origen
  - IP destino
  - Puerto origen
  - Puerto destino
  - Protocolo de la capa de transporte
  - Nombre de usuario o sistema (local ó remoto)
  - Nivel de sensibilidad de los datos
- IPSec permite granularidad para los servicios de seguridad, puede crearse una SA para todo el tráfico entre 2 pares IPSec ó crear una SA para cada conexión TCP entre los extremos.

Gestión de Claves

Allied Telesyn SIMPLY CONNECTING THE WORLD

Gestión de Claves

- Los servicios de seguridad IPSec utilizan claves criptográficas para la encriptación y la autentificación.
- IPSec utiliza un conjunto separado de mecanismos para poner estas claves en su sitio.
- IPSec requiere soporte manual y automático para la distribución de claves.
- Cuando una red una red es muy grande se hace imposible una gestión de claves manual.
- ISAKMP/IKE es el mecanismo utilizado por defecto para la gestión automática de claves.

ISAKMP

Allied Telesyn SIMPLY CONNECTING THE WORLD

ISAKMP

- Internet Security Association and Key Management Protocol (ISAKMP), Provee una estructura para negociar SA's y sus atributos, incluyendo las claves secretas.
- Está definido en el RFC 2408 y en el se prescriben los procedimientos y formatos de paquetes para establecer firmemente, negociar, modificar y borrar las SA's y sus atributos incluyendo las claves secretas.
- Provee una infraestructura para la implementación de gestión de claves y ser independiente de la generación de claves, autentificación, algoritmos de encriptación y la definición de SA's.

ISAKMP

- Un protocolo de gestión de claves basado en la infraestructura ISAKMP, debe definir su propia técnica de generación de clave, algoritmos de encriptación y tipos de autentificación.
- Diferentes definiciones de SA's son definidas en un documento separado llamado DOI (Domain of Interpretation), el DOI provee una interpretación de como está definido el protocolo e identificadores de algoritmo para un específico payload.
- ISAKMP puede implementarse sobre cualquier capa de transporte, aunque el puerto 500 de UDP es requerido para cumplir con el RFC.

ISAKMP

- ISAKMP utiliza valores aleatorios llamados cookies para separar negociaciones de identificaciones y parar los ataque de DoS.
- ISAKMP requiere que la autentificación, el intercambio de clave y la negociación de SA's sean lincadas juntas, así se evita el ataque MAN-IN-THE-MIDDLE.
- La intercepción, inserción, borrado,modificación y reproducción son protegidos por la autentificación del mensaje.
- Si cualquier cosa fuera de lo normal sucede en la negociación ISAKMP, el estado de la máquina retorna hacia su estado inactivo sin generar ninguna SA.

ISAKMP

- ISAKMP define dos fases de negociación:
  - La primera fase es el establecimiento de la SA de ISAKMP para proveer un canal seguro autentificado para el tráfico ISAKMP entre dos extremos ISAKMP. Dos dispositivos los cuales entablan la negociación ISAKMP son descritos como extremos de comienzo ISAKMP.
  - La segunda fase es la de negociación de SA's y claves en nombre de servicios como IPSec. Están definidos en un particular DOI, esto hace posible mas de una SA fase 2 sobre la misma SA ISAKMP sin tener que reestablecer la comunicación con los pares ISAKMP.

SA ISAKMP

- La SA ISAKMP es creada para proteger el tráfico ISAKMP entre 2 extremos ISAKMP, esto asegura que algunas SA's y claves negociadas para otras servicios de seguridad (por ejemplo IPSec) puedan guardarse en secreto y sean autentificadas, también provee protección de identidad para las SA's creadas. La SA ISAKMP es identificada por su cookie en la cabecera del mensaje ISAKMP y es almacenada localmente en una base de datos SA ISAKMP. Los tipos de algoritmos y el formato de SA ISAKMP son guardados en un DOI separado.

Intercambios ISAKMP

- El intercambio ISAKMP y los mensajes ISAKMP son los bloques de construcción para un protocolo de gestión de clave utilizando la infraestructura ISAKMP. Un intercambio ISAKMP consiste en un número finito de mensajes los cuales son construidos desde un definido conjunto de datos.
- ISAKMP tiene 5 tipos de intercambios:
  - Base-RFC
  - Protección de identidad
  - Autentificación
  - Agresivos
  - Informacionales
- Un protocolo de gestión de clave usando ISAKMP (ejemplo IKE), está habilitado para definir tipos adicionales de intercambios si se requieren

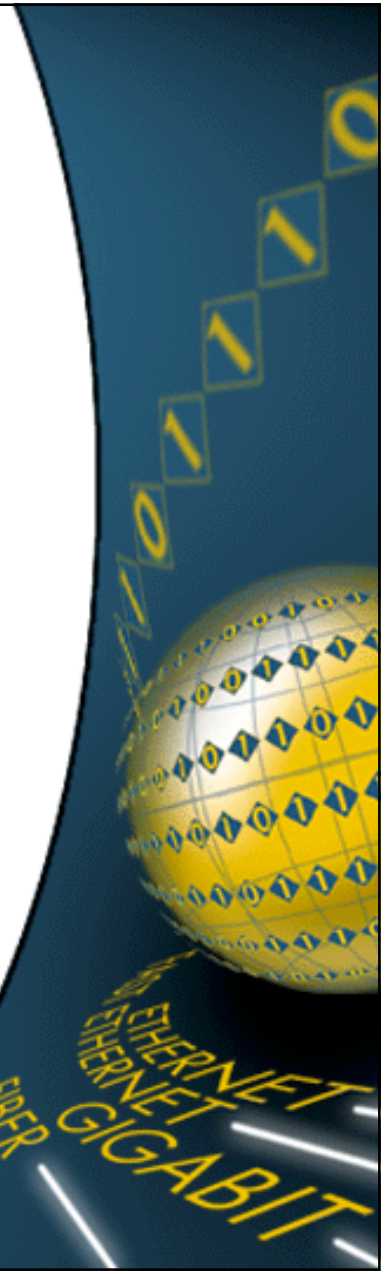
Mensajes ISAKMP

- Cada mensaje ISAKMP está construido desde una cabecera genérica ISAKMP, seguida por uno o mas payloads. El RFC ISAKMP define 13 diferentes payloads:
  - Security Association (SA) - Utilizado para negociar los atributos de seguridad e indicar el DOI y las situaciones bajo las cuales la negociación tiene lugar.
  - Proposal (P) - Parte de payload SA conteniendo protocolos de seguridad (ejemplo AH, ESP,..).
  - Transform (T) - Parte de payload P conteniendo los atributos de seguridad para el mecanismo de seguridad específico.
  - Key Exchange (KE) - Datos específicos de intercambio de clave.
  - Identification (ID) - Información de un DOI específico para identificar los pares que se están comunicando.

Mensajes ISAKMP

- Certificate (CERT) - Utilizado para el transporte de certificados
- Certificate Request (CR) - Utilizado para pedir un certificado desde el otro par.
- Hash (HASH) - Datos generados por la función hash con el propósito de verificar la integridad de los mensajes o entidades autentificadas.
- Signature (SIG) - Datos generados por la función de firma digital usado para autentificar algunas partes del mensaje.
- Nonce (NONCE) - Datos aleatorios usados para garantizar y proteger contra un ataque de reproducción.
- Notification (N) - Información de ISAKMP y DOI específicos
- Delete (D) - Notifica a otro par que una SA ha sido borrada
- Vendor ID (VID) - Utilizado para habilitar dispositivos para reconocer instancias remotas de sus implementaciones y uso de sus extensiones propietarias.

IKE



Allied Telesyn SIMPLY CONNECTING THE WORLD

IKE

- El protocolo Internet Key Exchange (IKE), está definido en el RFC 2409 y provee intercambio de clave para IPSec, combinando partes de los protocolos OAKLEY y SKEME con la estructura ISAKMP.
- El protocolo de determinación de clave OAKLEY está definido en el RFC 2412 y describe un método de intercambio de clave autentificado con PFS y protección de identidad.
- El protocolo SKEME está definido en el documento “SKEME: A Versatile Secure Key Exchange Mechanism For Internet”, también provee intercambio de clave autentificada y describe un método de autentificación de clave pública con rápida regeneración utilizando NONCES.

Intercambios IKE

- IKE define dos fases de intercambios:
  - Main Mode es una implementación de la protección de identidad del intercambio ISAKMP y debe ser implementada. Aggressive Mode es una implementación de intercambio agresivo de ISAKMP y puede ser opcionalmente implementado. Estos dos intercambios son sólo usados en la fase 1 para crear la SA ISAKMP.
  - IKE define un nuevo intercambio ISAKMP llamado Quick Mode, este intercambio sólo se puede utilizar en la fase 2 y se utiliza para negociar SA en nombre de otros servicios como es IPSec.
  - IKE también define New Group Mode, el cual debe ser usado después de la fase 1 y permite negociar nuevos valores de la clave pública DH.
  - Los intercambios informacionales ISAKMP pueden tener lugar en cualquiera de las fases y son utilizados para notificar al extremo final de los errores y SA's borradas.

Intercambios IKE

- Todos los intercambios IKE se ajustan a la sintaxis estandar de los payloads ISAKMP y atributos codificados.
- El payload SA es siempre en primer lugar en mensajes fase 1.
- El payload Hash debe ser siempre primero en mensajes fase 2.
- Otros payloads ISAKMP pueden ser recibidas en cualquier orden.

Negociación SA IKE

- El payload SA utilizado por los modos principal, agresivo y rápido siempre coge la forma de payload transform, encapsulado en payload proposal y encapsulado en un payload SA. En la fase 1 sólo puede ser un payload SA y un payload proposal.
- Las diferentes opciones para una una SA ISAKMP están descritos en un payload transform separado.
- En la fase 2 es posible negociar mas de una SA a la vez, por lo tanto puede ser mas de un payload SA, cada payload SA puede tener mas de un payload proposal (ejemplo AH y ESP). Cada payload proposal puede tener mas de un payload transform (ejemplo SHA y MD-5)

Intercambios IKE

- IKE coge el método de intercambio de clave de OAKLEY y utiliza el algoritmo de clave pública DH y puede ser completada en 3 o mas mensajes, esto provee el intercambio de clave autentificada requerido por ISAKMP y puede opcionalmente proveer PFS para la fase 2.
- El protocolo OAKLEY define un conjunto de valores de clave pública DH conocidos como grupos Oakley.
- IKE requiere que el “OAKLEY MODP GROUP1” esté soportado en una implementación conforme.

Autentificación IKE

- Deben soportar autentificación via claves pre compartidas y puede opcionalmente también soportar autentificación con encriptación de claves públicas, firmas o un método revisado de uso de encriptación de claves públicas.
- La autentificación por claves pre compartidas tiene la menor carga computacional de los diferentes métodos de autentificación, sin embargo este tipo de claves tiene que ser seguramente transportada hacia cada dispositivo antes de que cualquier negociación ISAKMP tenga lugar.
- El intercambio de clave es autentificado por añadir la clave compartida en el proceso de generación de clave

Autentificación IKE

- Cada parte provee los valores conocidos de la clave de sesión por ser capaz de encriptar y desencriptar el último mensaje de la fase 1 en el intercambio.
- La autentificación usando encriptación de la clave pública es mas lento que la clave precompartida, pero es un método fuente de autentificación. El payload nonce es encriptado usando las claves públicas de sus pares, la encriptación de clave pública también provee protección de identidad a la fase 1 por encriptar también el payload ID con la clave pública de sus pares.

Autentificación IKE

- La autentificación utilizando firmas también es mas lento que las claves pre compartidas, los hashes firmados son intercambiados en el final del intercambio y la autentificación es conseguida por la verificación de la firma con las claves públicas de sus pares, porque sólo el par propietario de la parte privada de la clave pública puede firmar el hash, mientras que el par que desencripte la firma correctamente es el verdadero propietario de la clave pública.
- La encriptación de la clave pública y la firma requiere que las claves públicas de cada parte sean intercambiadas y verificadas, en el caso simple que la clave pública pueda ser intercambiada manualmente y verificada por el administrador.

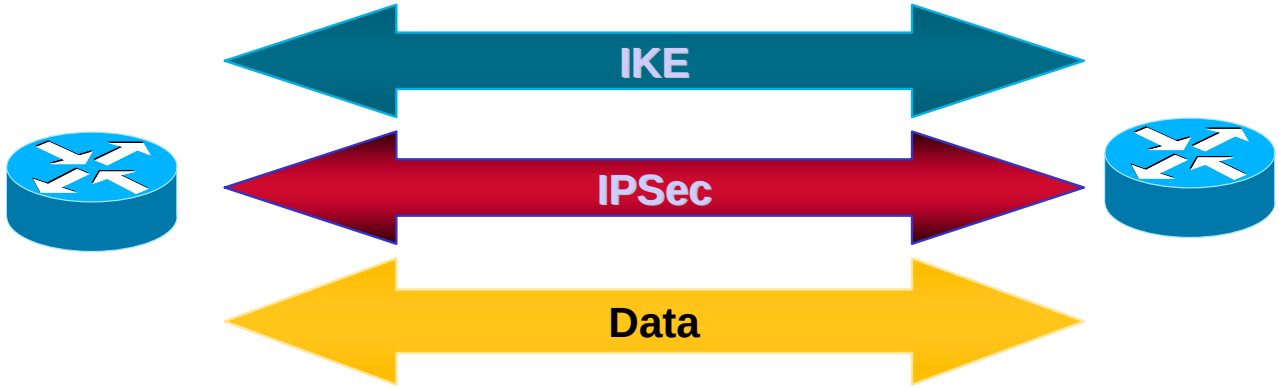
Autentificación IKE

- Alternativamente las claves públicas pueden ser extraidas desde un certificado el cual conexiona la clave hacia el par y es firmado por una tercera parte de confianza.
- IKE provee mecanismos para intercambiar certificados permitiendo a cualquier mensaje tener un opcional payload certificate o un payload certificate request, esto requiere que cada par IKE tiene un método separado para obtener certificados firmados por una autoridad certificadora (CA).

Perfect Forward Secrecy (PFS)

- Asegura que si una clave es comprometida, no será causa para que mas claves sean comprometidas
- Compromiso de que una clave simple permitirá acceder sólo a los datos protegidos para esa clave particular.
- IKE provee PFS si es requerido para usar Diffie-Hellman para cada recodificación
- Si PFS no es requerido, puede refrescar la clave sin usar Diffie Hellman

Iniciando nuevas conexiones

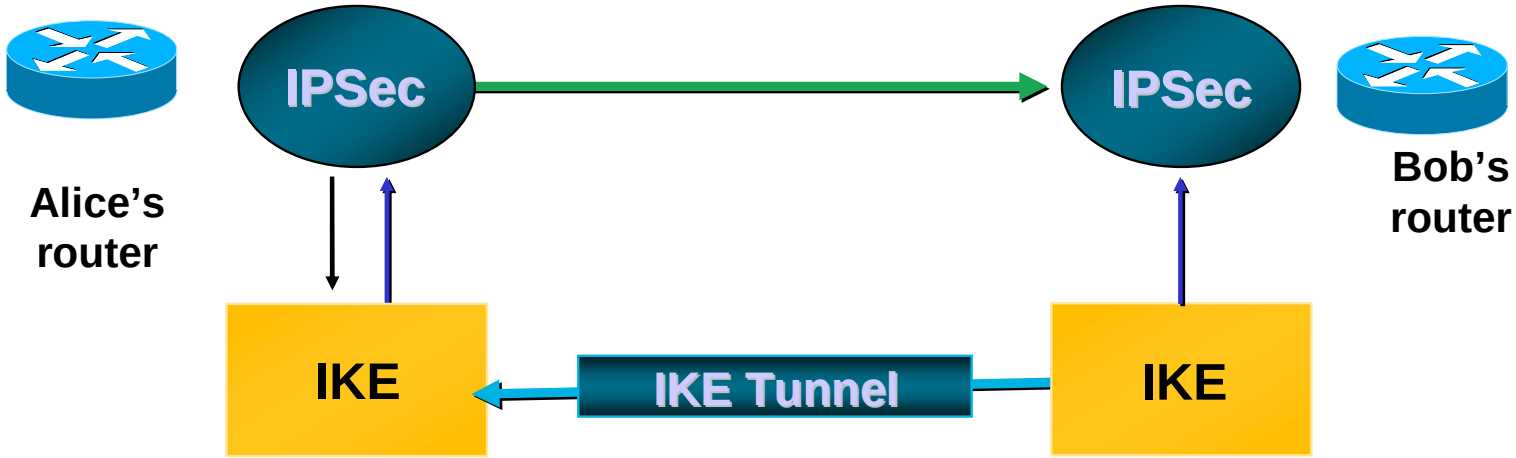


- Estableciendo IKE SA—“Main mode”
- Estableciendo IPSec SA—“Quick mode”
  - Multiple quick modes for each main mode
- Send protected data

Como IPSec usa IKE

1. Outbound packet from Alice to Bob. No IPSec SA

4. Packet is sent from Alice to Bob protected by IPSec SA

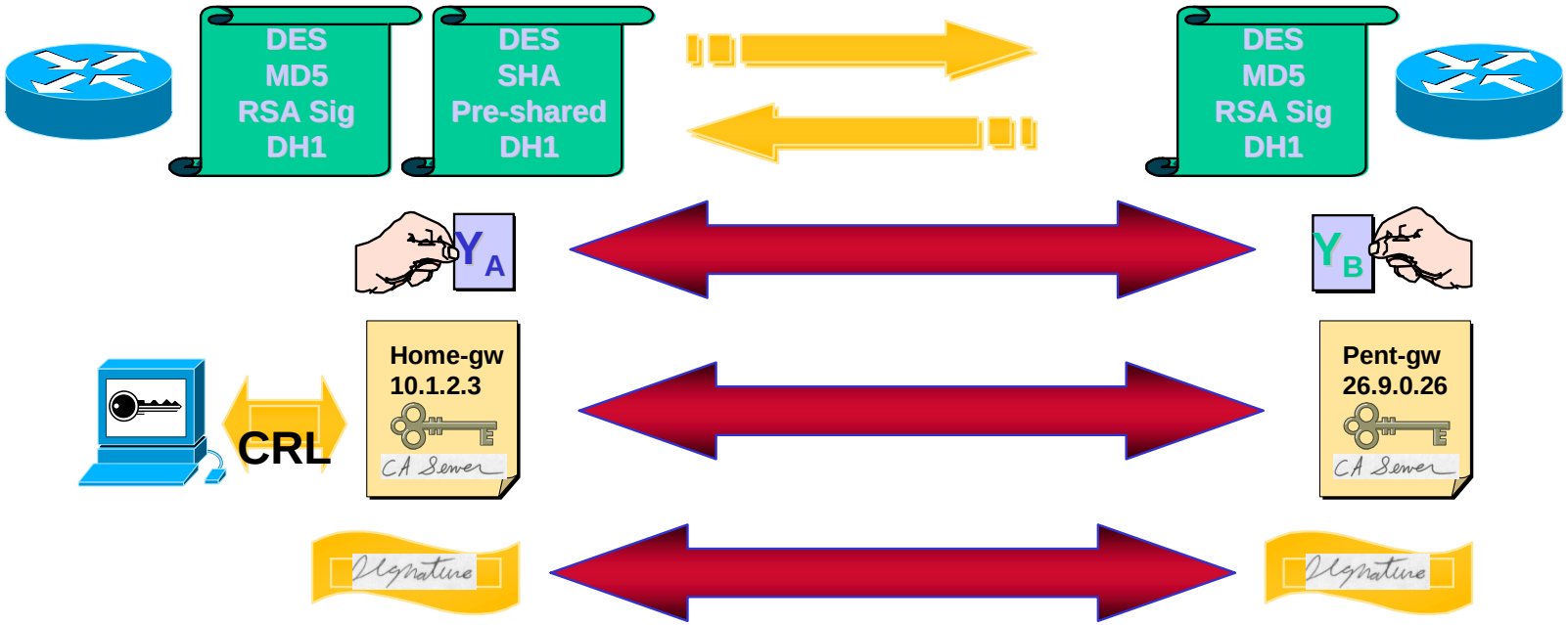


2. Alice's IKE begins negotiation with Bob's

3. Negotiation complete. Alice and Bob now have complete set of SAs in place

Allied Telesyn SIMPLY CONNECTING THE WORLD

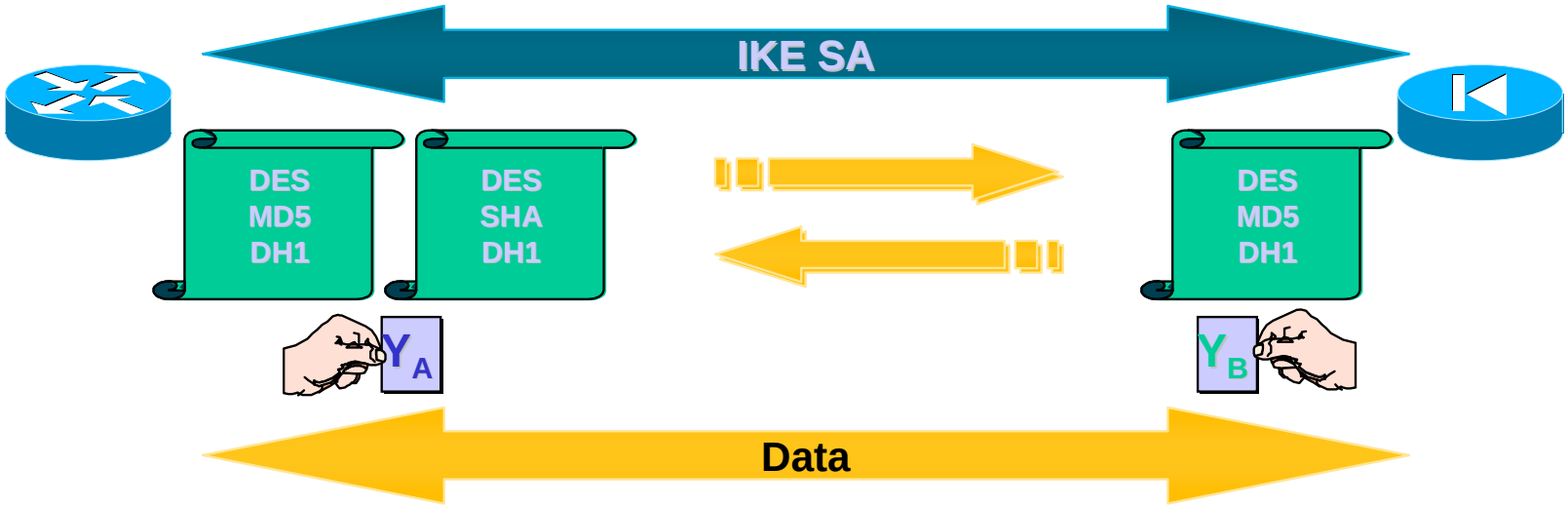
Creando una IKE SA



- Negotiate IKE parameters
- Exchange DH Numbers
- Exchange Certificates and check CRL
- Exchange signed data for authentication

Allied Telesyn SIMPLY CONNECTING THE WORLD

Creando IPSec SA— Modo Rápido



- Requires IKE SA to be in place
- Negotiate IPSec parameters
- Create shared session key

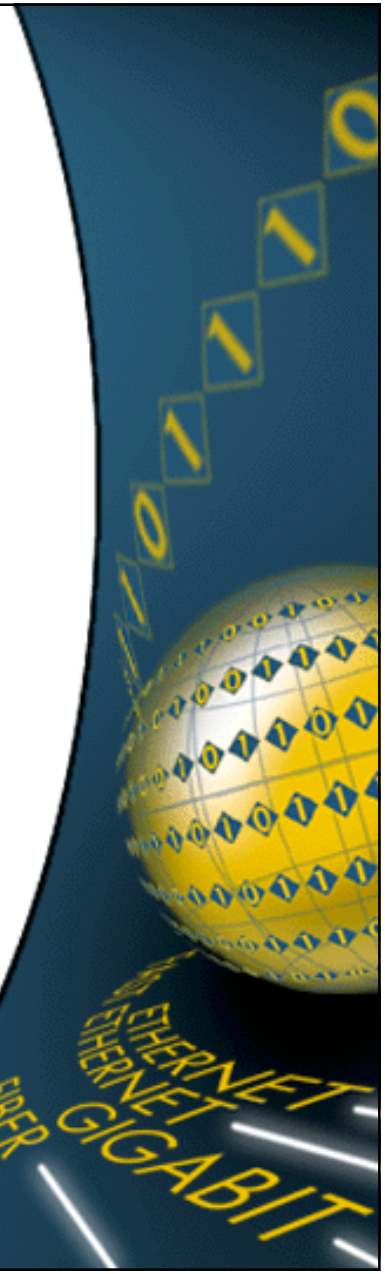
Local Policy {

Exchange DH numbers for PFS or

Exchange nonces for quick rekey

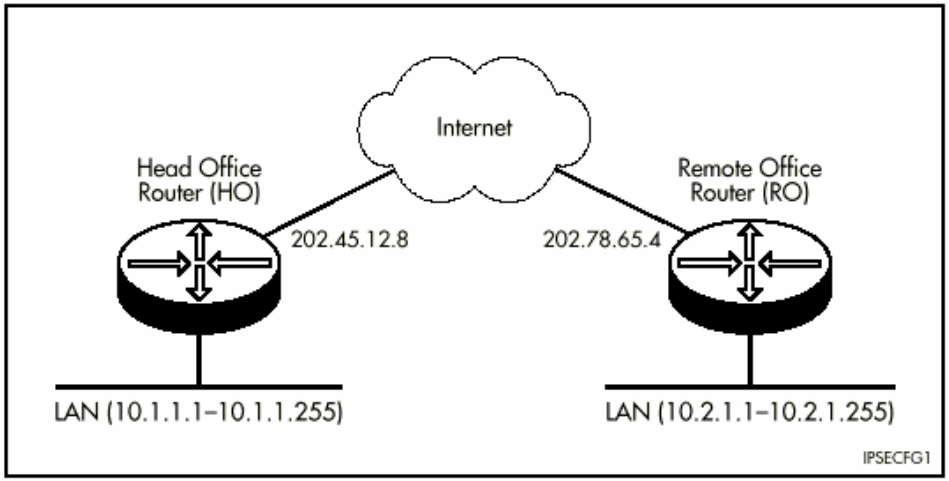
Configuraciones

IPSec



Allied Telesyn SIMPLY CONNECTING THE WORLD

Configuraciones IPSec



Allied Telesyn
SIMPLY CONNECTING THE WORLD

Configuraciones IPSec

- **Configuración de IPSec con Gestión de clave manual**

Allied Telesyn SIMPLY CONNECTING THE WORLD

Configuraciones IPSec

- **ROUTER A:**
- CREATE ENCO KEY=1 TYPE=DES VALUE=0x4385DF613B7C2C7A
- CREATE ENCO KEY=101 TYPE=GENERAL VALUE=0xFF2E6FDEBD789EE838942C558F7CEBCF
- CREATE IPSEC SASPECIFICATION=1 KEYMANAGEMENT=MANUAL PROTOCOL=ESP ENCALG=DES ENCKEY=1 HASHALG=NULL INSPI=1555 OUTSPI=1555
- CREATE IPSEC SASPECIFICATION=2 KEYMANAGEMENT=MANUAL PROTOCOL=AH HASHALG=MD5 INSPI=2666 OUTSPI=2666
- CREATE IPSEC BUNDLESPECIFICATION=1 KEYMANAGEMENT=MANUAL STRING="1 AND 2"
- CREATE IPSEC POLICY=office_vpn_ipsec INT=ppp0 ACTION=IPSEC KEYMANAGEMENT=MANUAL BUNDLESPECIFICATION=1 PEERADDRESS=202.78.65.4
- SET IPSEC POLICY=office_vpn_ipsec LADDRESS=10.1.1.1-10.1.1.50 RADDRESS=10.2.1.1-10.2.1.50
- ENABLE IPSEC

Configuraciones IPSec

- **ROUTER B:**
- CREATE ENCO KEY=4 TYPE=DES VALUE=0x4385DF613B7C2C7A
- CREATE ENCO KEY=111 TYPE=GENERAL VALUE=0xFF2E6FDEBD789EE838942C558F7CEBCF
- CREATE IPSEC SASPECIFICATION=1 KEYMANAGEMENT=MANUAL PROTOCOL=ESP ENCALG=DES ENCKEY=4 HASHALG=NULL OUTSPI=1555 INSPI=1555
- CREATE IPSEC SASPECIFICATION=2 KEYMANAGEMENT=MANUAL PROTOCOL=AH HASHALG=MD5 HASHKEY=4 OUTSPI=2666 INSPI=2666
- CREATE IPSEC BUNDLESPECIFICATION=1 KEYMANAGEMENT=MANUAL STRING="1 AND 2"
- CREATE IPSEC POLICY=office_vpn_ipsec INT=ppp0 ACTION=IPSEC KEYMANAGEMENT=MANUAL BUNDLESPECIFICATION=1 PEERADDRESS=202.45.12.8
- SET IPSEC POLICY=office_vpn_ipsec LADDRESS=10.2.1.1-10.2.1.50 RADDRESS=10.1.1.1-10.1.1.50
- ENABLE IPSEC

Configuraciones IPSec

- **Configuración de IPSec con Gestión de clave ISAKMP/IKE**

Allied Telesyn SIMPLY CONNECTING THE WORLD

Configuraciones IPSec

- **ROUTER A:**

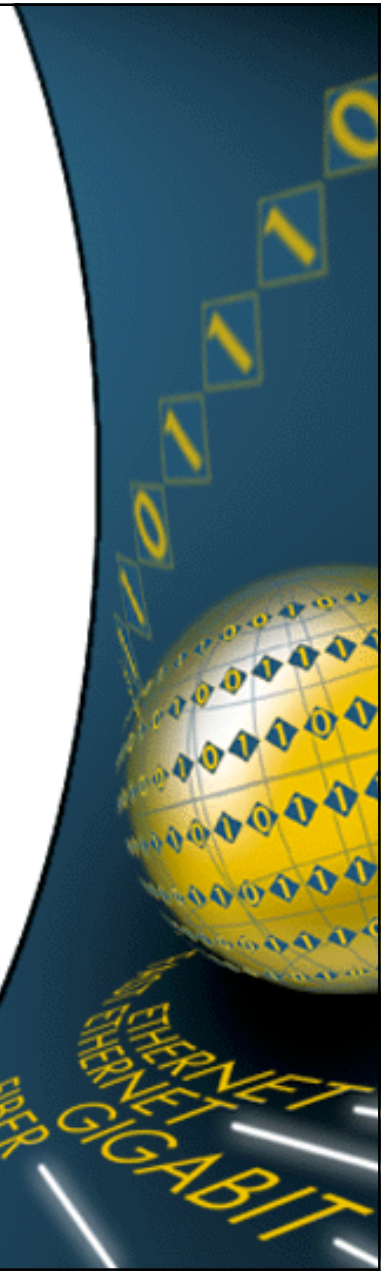
- CREATE ENCO KEY=99 TYPE=GENERAL VALUE=<SHARED_SECRET>
- CREATE ISAKMP POLICY=office_isakmp_policy PEER=202.78.65.4 AUTHTYPE=PRESHARED KEY=99 ENCALG=DES HASHALG=SHA
- CREATE IPSEC SASPECIFICATION=1 KEYMANAGEMENT=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=NULL
- CREATE IPSEC SASPECIFICATION=2 KEYMANAGEMENT=ISAKMP PROTOCOL=ESP ENCALG=3DES2KEY HASHALG=NULL
- CREATE IPSEC SASPECIFICATION=3 KEYMANAGEMENT=ISAKMP PROTOCOL=AH HASHALG=SHA
- CREATE IPSEC BUNDLESPECIFICATION=1 KEYMANAGEMENT=ISAKMP STRING="2 AND 3,1 AND 3"
- CREATE IPSEC POLICY=office_vpn_isakmp INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
- CREATE IPSEC POLICY=office_vpn_ipsec INT=ppp0 ACTION=IPSEC KEYMANAGEMENT=ISAKMP BUNDLESPECIFICATION=1 PEER=202.78.65.4
- SET IPSEC POLICY=office_vpn_ipsec LADDRESS=10.1.1.1-10.1.1.50 RADDRESS=10.2.1.1-10.2.1.50
- ENABLE IPSEC
- ENABLE ISAKMP

Configuraciones IPSec

- **ROUTER B:**

- CREATE ENCO KEY=99 TYPE=GENERAL VALUE=<SHARED_SECRET>
- CREATE ISAKMP POLICY=office_isakmp_policy PEER=202.45.12.8 AUTHTYPE=PRESHARED KEY=99 ENCALG=DES HASHALG=SHA
- CREATE IPSEC SASPECIFICATION=1 KEYMANAGEMENT=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=NULL
- CREATE IPSEC SASPECIFICATION=2 KEYMANAGEMENT=ISAKMP PROTOCOL=AH HASHALG=SHA
- CREATE IPSEC BUNDLESPECIFICATION=1 KEYMANAGEMENT=ISAKMP STRING="1 AND 2"
- CREATE IPSEC POLICY=office_vpn_isakmp INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
- CREATE IPSEC POLICY=office_vpn_ipsec INT=ppp0 ACTION=IPSEC KEYMANAGEMENT=MANUAL BUNDLESPECIFICATION=1 PEER=202.45.12.8
- SET IPSEC POLICY=office_vpn_ipsec LADDRESS=10.2.1.1-10.2.1.50 RADDRESS=10.1.1.1-10.1.1.50
- ENABLE IPSEC
- ENABLE ISAKMP

Gracias



Allied Telesyn SIMPLY CONNECTING THE WORLD