Diseño de redes VPN seguras bajo Windows server 2008

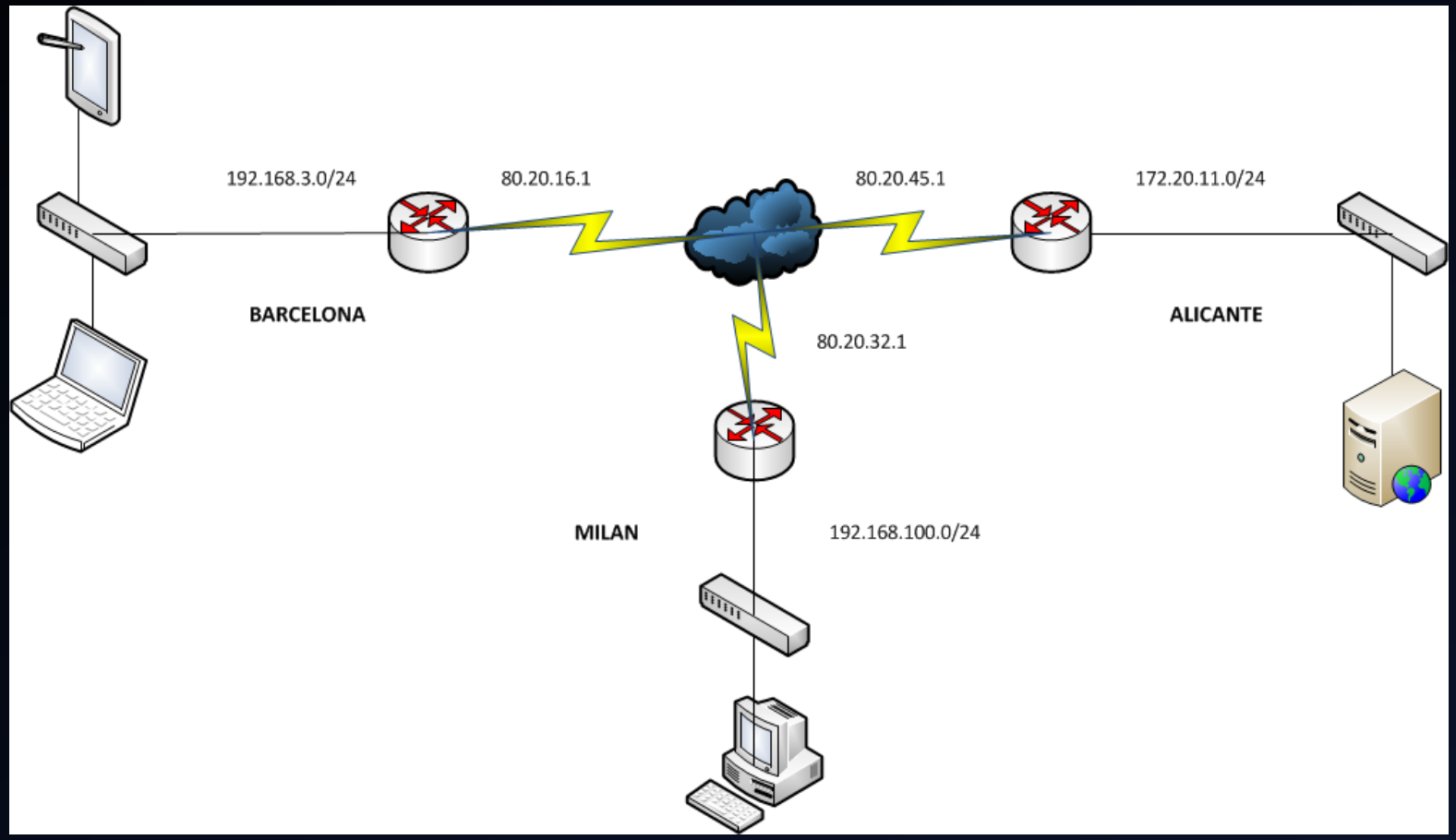
PROYECTO FINAL DE CARRERA INGENIERIA TECNICA EN TELECOMUNICACIONES ESPECIALIDAD TELEMATICA

ANTONIO TUDELA BOTELLA

ESCENARIO INICIAL

- Fusión de tres industrias del calzado completamente independientes
- Distintas sedes en Alicante, Barcelona y Milán.
- Infraestructura IT completamente segregada
- Sistemas IT obsoletos. Falta de seguridad.
- SOLUCION: VPN + FIREWALL

ESQUEMA NETWORKING INICIAL



- Tres redes LAN completamente segregadas en Alicante, Barcelona y Milán
- Los rangos privados son redes de clase C
- Cada centro con red privada LAN dispone de salida a internet mediante una IP publica estática.

BENEFICIOS VPN + FIREWALL

VIDEOCONFERENCIA

COMPARTIR INFRAESTRUCTURAS

SEGURIDAD

EN DEFINITIVA…..UNA MISMA RED

¿POR QUE WINDOWS SERVER?

SOPORTE

FACILIDAD

Microsoft TechNet

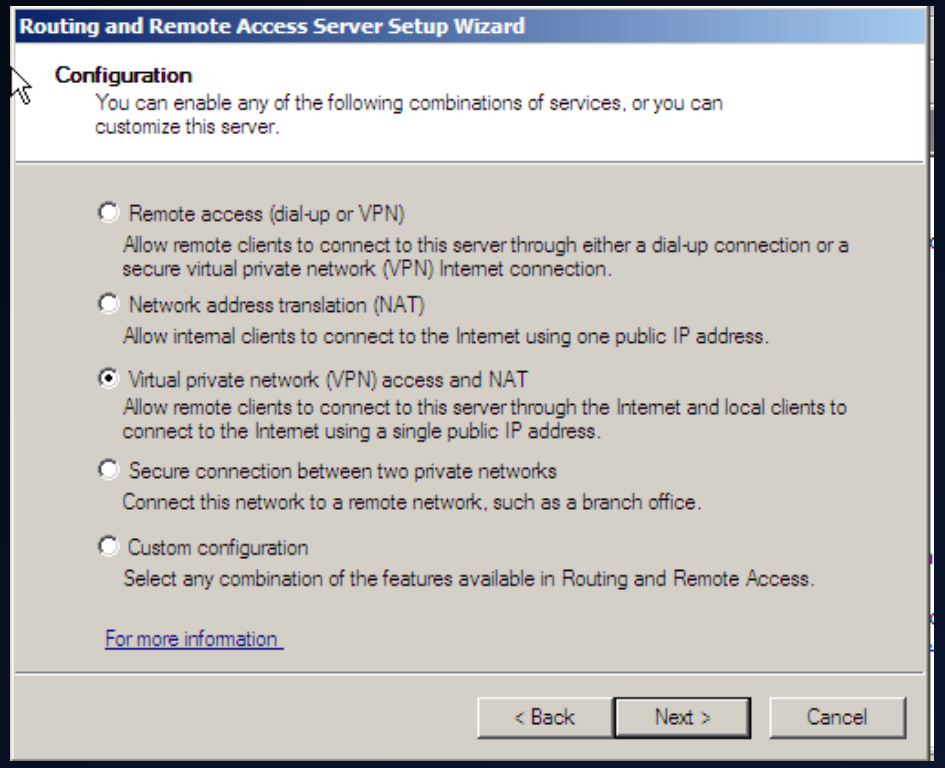
DOCUMENTACION

ARQUITECTURA VPN

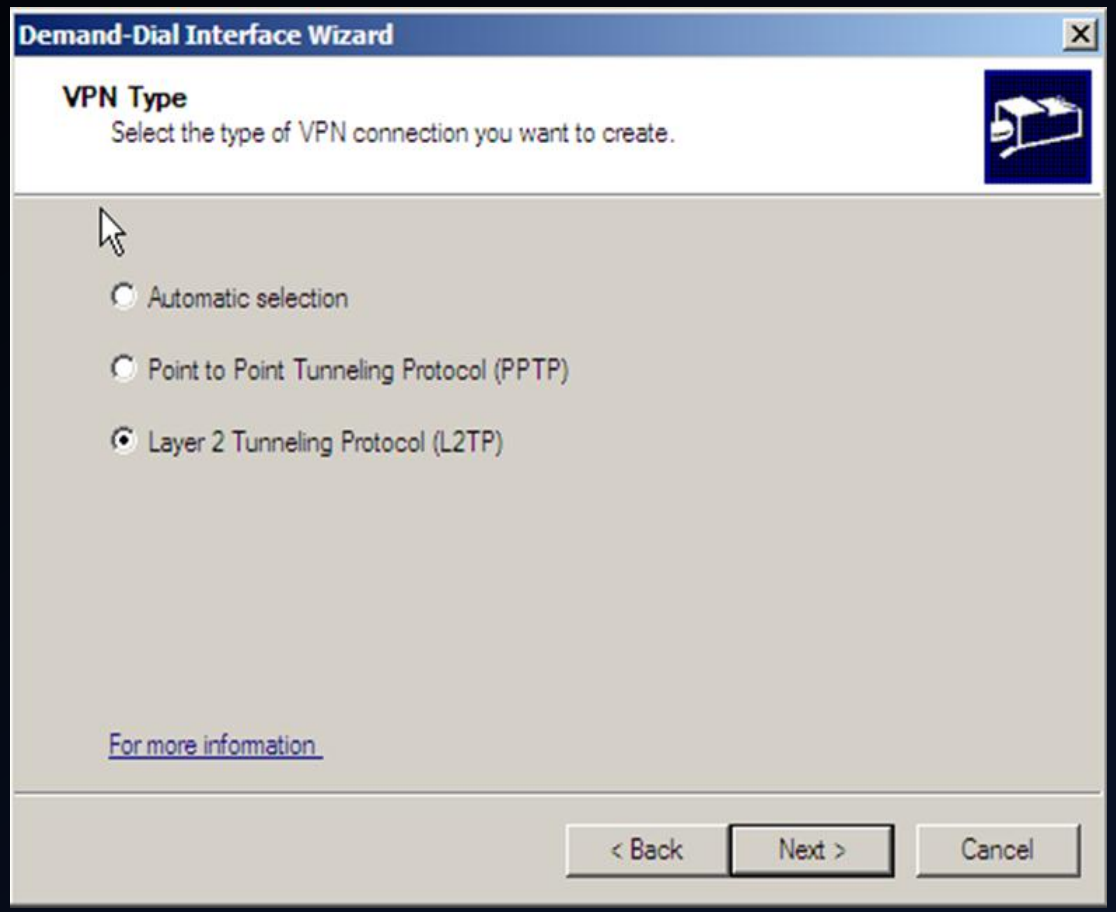
- Se basan en conexiones punto a punto sobre redes publicas
- Su misión es unir redes LAN geográficamente dispersas
- Para conseguir su finalidad utiliza el concepto de túnel
- Túnel: Encapsula paquetes dentro de otros para emular una conexión privada

VPN SITIO A SITIO

- Se debe de disponer de un servidor con Windows server 2008 en cada centro.
- Se requiere instalar el rol **Network Policy and Access Server** con funcionalidad **Routing and remote access**
- El servidor VPN permite enrutar el trafico de todos los host de una LAN local hacia otra red LAN ubicada en un lugar geográficamente separado.

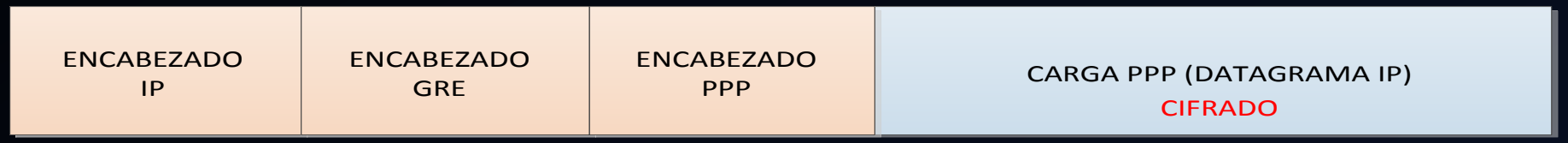


MODOS DE CONEXION VPN



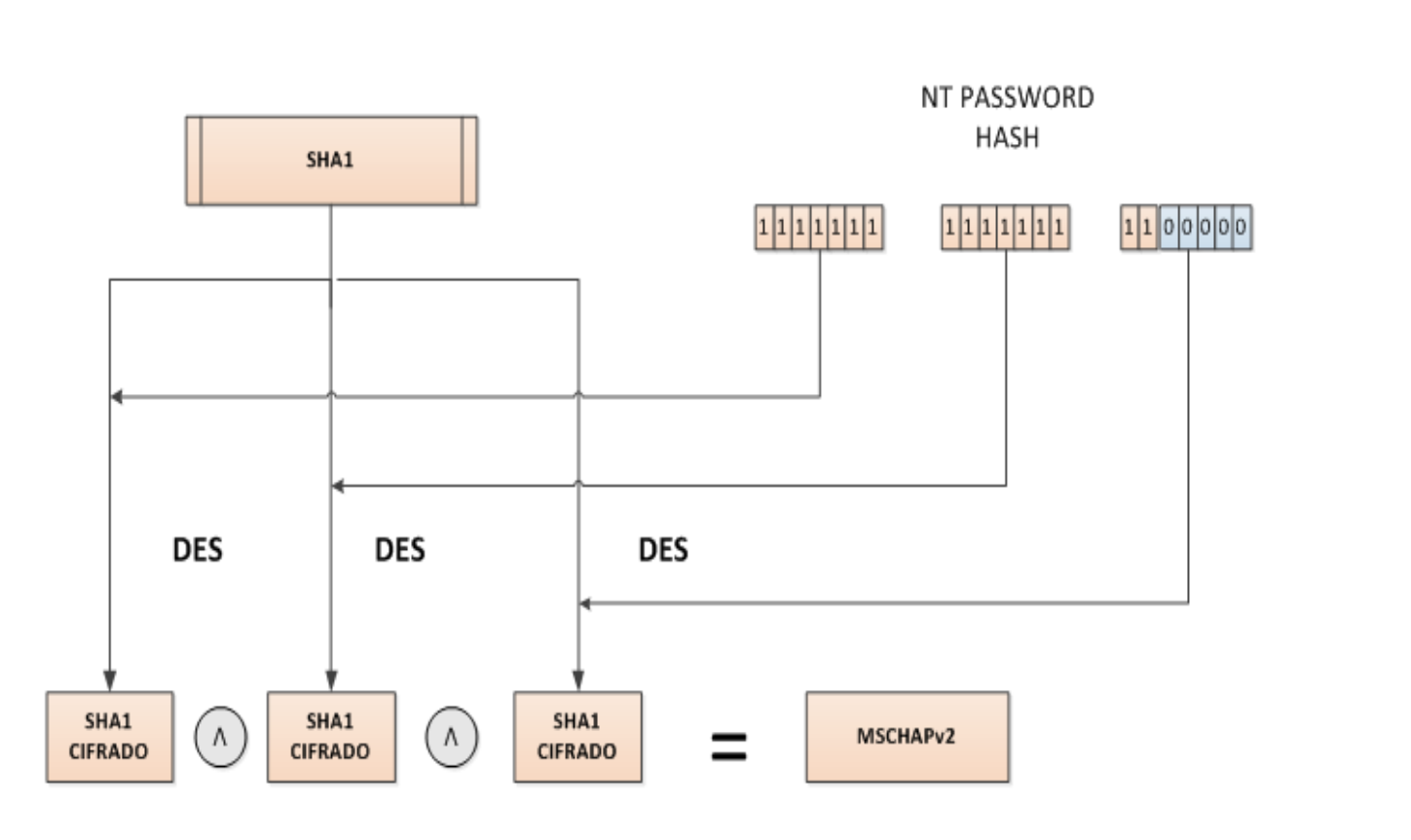
- El modo PPTP utiliza el cifrado MPPE (Microsoft point to point encription)
- El modo L2TP utiliza el cifrado estándar IPSec
- Los dos modos trabajan con PPP

MODO PPTP



- Protocolo de red creado por Microsoft
- No se encuentra contemplado por el IETF
- Utiliza una conexión TCP + un encabezado GRE para generar el Túnel
- cifra mediante un protocolo propio de Microsoft llamado MPPE.
- Las claves de cifrado son generadas mediante el proceso de autenticación MS-CHAP v2.

MS-CHAPv2



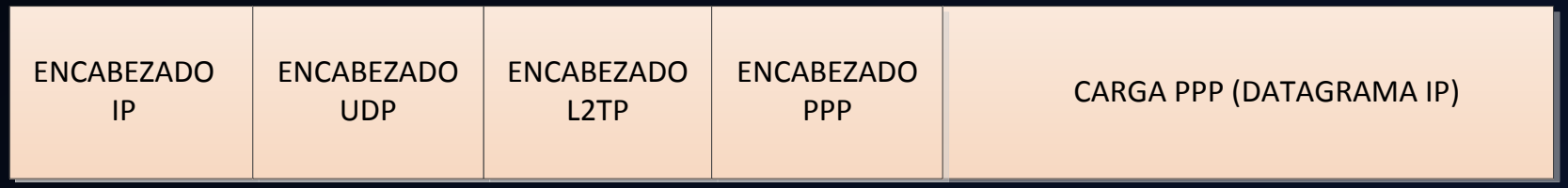
- Utiliza la unión de SHA1 y NTpassword
- Añade 5 bytes con valor 0 al NT Password
- Obtiene tres DES independientes
- Un DES solo tiene el valor 2^{16} valores
- El SHA1 es el mismo
- Concatena el resultado por lo que solo se necesita descifrar una clave de 2^{57} valores

MS-CHAPv2

¡MS-CHAPv2 ES INSEGURO!

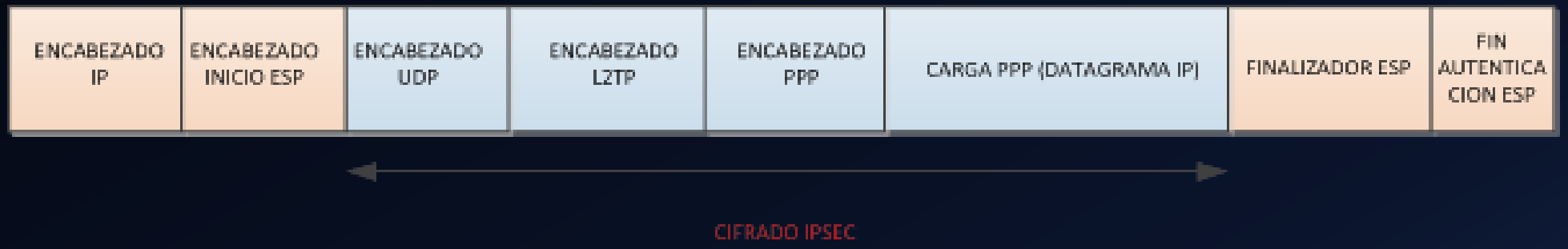
LA SOLUCION, L2TP/IPSEC

- Trabaja en la capa 2 OSI
- utiliza UDP para montar un túnel entre servidores VPN y enviar PPP encapsulado
- Contemplado por el IETF (RFC 2661)

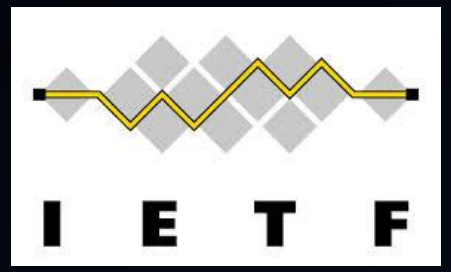


LA SOLUCION, L2TP/IPSEC

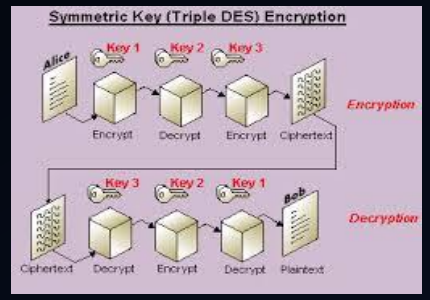
- El protocolo IKE negocia las asociaciones de seguridad
- En modo principal evita ataques «Man in the Middle»
- ESP ofrece autenticación y cifrado
- ESP utiliza 3DES con una longitud total de 168 bits o $3{,}74*10^{50}$ claves posibles



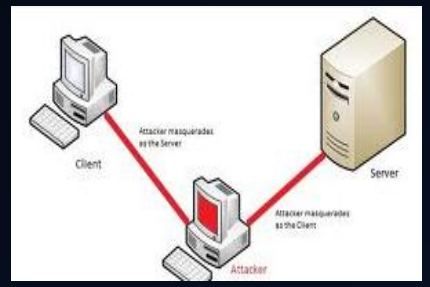
ALGUNAS VENTAJAS MICROSOFT L2TP/IPSEC



RECONOCIDO

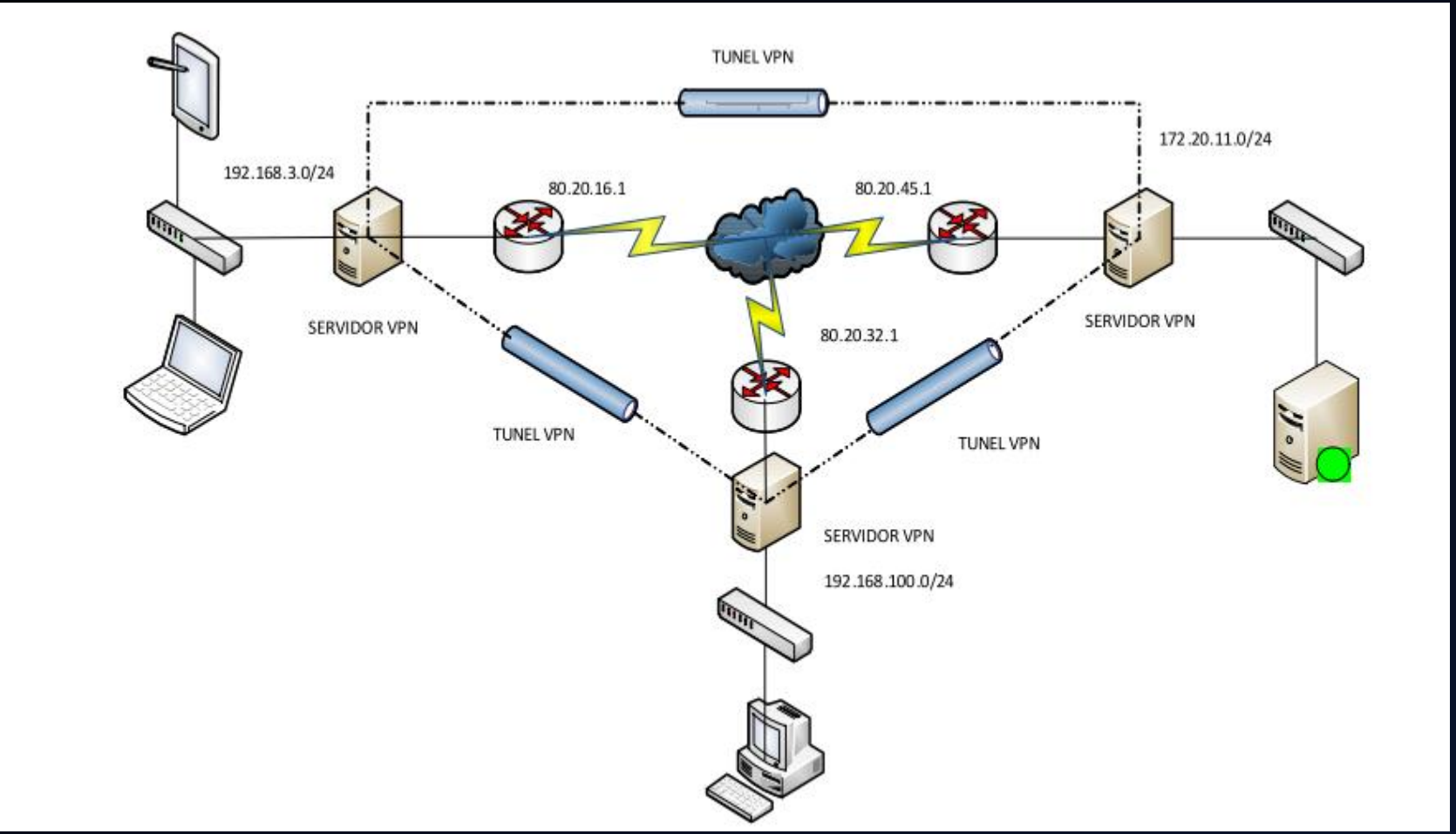


CIFRADO 3DES



EVITA ATAQUE « MAN IN THE MIDDLE»

SOLUCION VPN L2TP/IPSEC PARA EMPRESAS ZAPATERAS

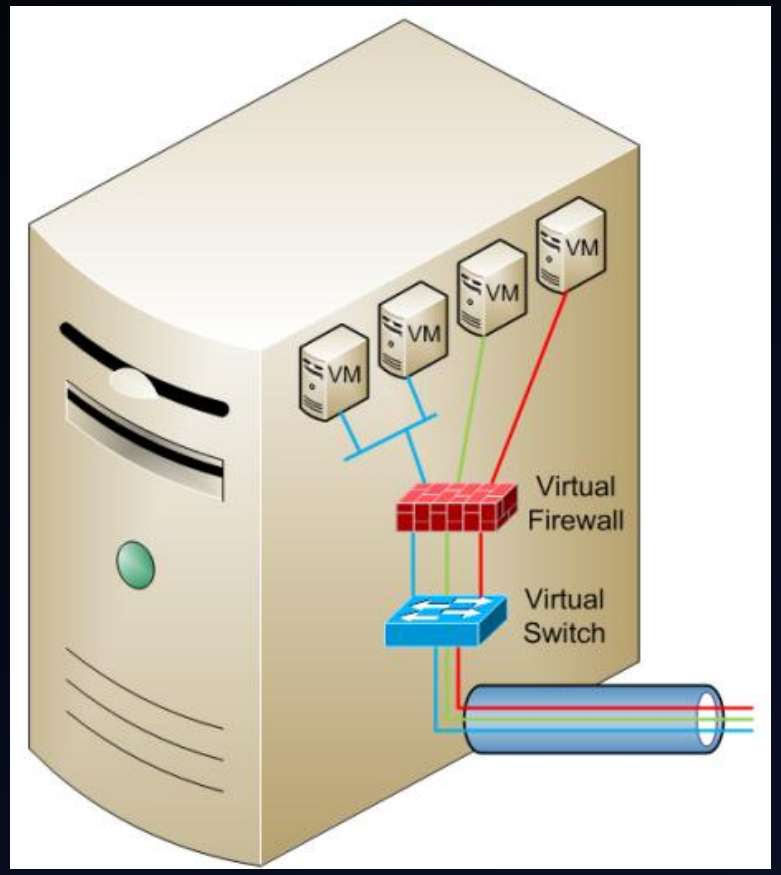


- Las tres redes LAN de las distintas oficinas son ahora visibles entre ellas mediante los túneles VPN .
- Todo el trafico que no tenga como destino una de las oficinas opera con normalidad saliendo por el Gateway hacia internet.
- La topología es en forma de malla para permitir que si uno de los servidores VPN falle no queden los demás aislados.
- Cada servidor VPN dispone de dos conexiones por marcado que generan dos PPP contra las otras sedes

¿POR QUE PROTEGER CON FIREWALL?

- Mantener al margen usuarios no autorizados
- Evita ataques BOTNET
- Evita ataques WORM
- Facilita la administración
- Evita ofrecer datos sobre la infraestructura de red

HYPER-V + LINUX IPTABLES. FIREWALL ECONOMICO

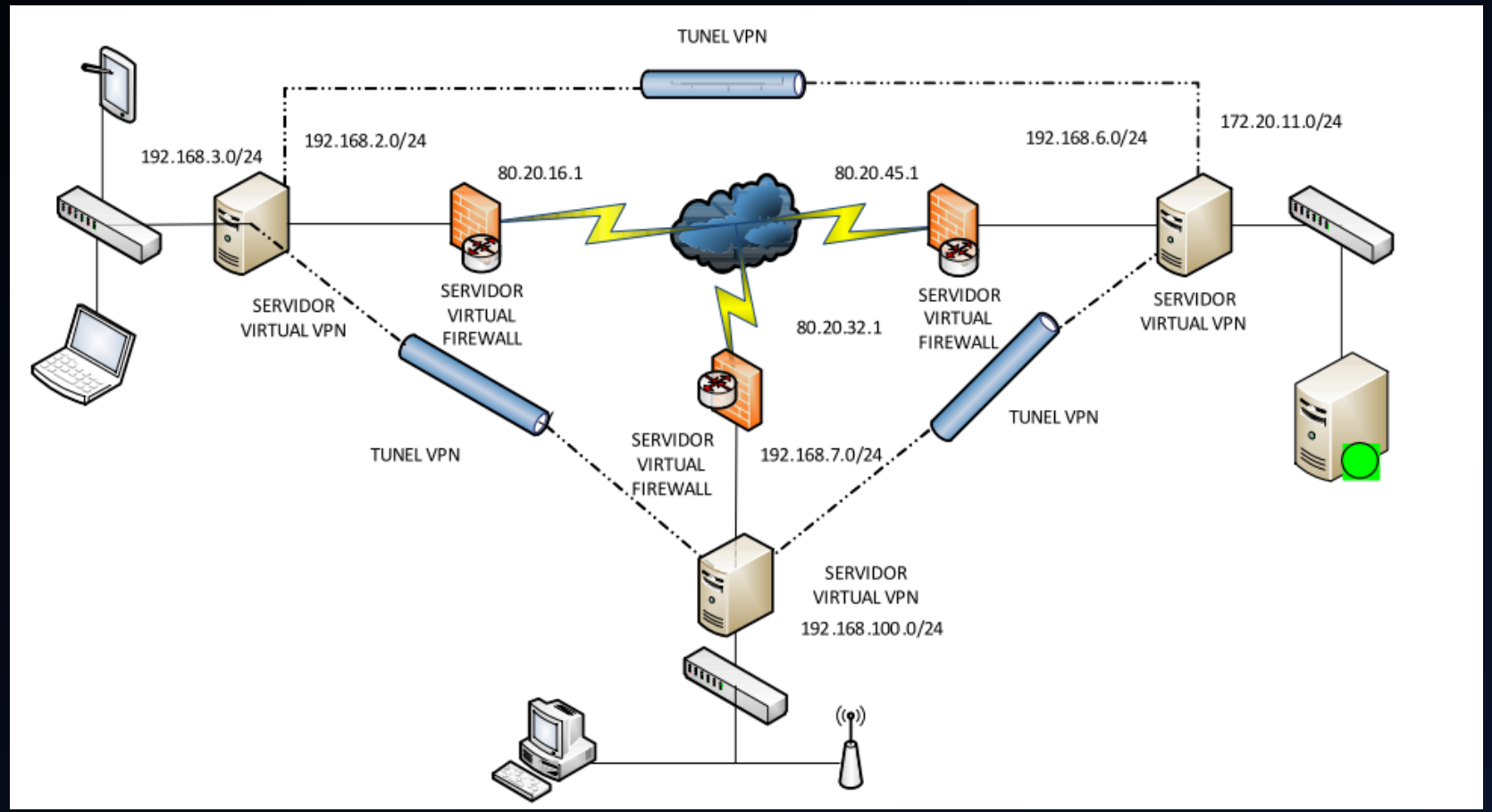


- HYPER-V es un rol hypervisor gratuito en Windows server 2008
- GNU/Linux es Software Libre.
- Se utiliza el mismo hardware . No hay gasto extra en Infraestructura
- No hay gasto de licencias extra
- Menor consumo eléctrico

CONFIGURACION VPN DETRAS DEL FIREWALL

Tipo de filtro	Puerto	Motivo
PREROUTING	UDP 500	Permite trafico IPsec IKE en la interfaz de entrada
PREROUTING	UDP 4500	Permite IPSec NAT transversal en la interfaz de entrada
PREROUTING	IP 50	Permite trafico IPSec ESP en la interfaz de entrada
POSTROUTING	UDP 500	Permite trafico IPSec IKE interfaz salida
POSTROUTING	UDP 4500	Permite IPSec NAT transversal interfaz salida
POSTROUTING	IP 50	Permite trafico IPSec ESP interfaz de salida

SOLUCION DEFINITIVA VPN L2TP/IPSEC + FIREWALL



- Las 3 redes LAN son visibles a través de los túneles VPN sin recibir restricciones de los firewall virtuales
- el tráfico que no circule por alguno de los túneles será inspeccionado por al menos un firewall y sus paquetes serán filtrados

CONCLUSIONES

- En el presente proyecto se han cumplido los objetivos propuestos desde el principio del semestre. Demostrar que se pueden unificar tres sitios geográficamente distantes mediante Windows server 2008 ofreciendo un bajo coste económico y una alta seguridad
- El proyecto puede ser implantado rápidamente en una pequeña o mediana empresa con notable éxito ya que se ha diseñado un entorno de test mediante maquinas virtuales idéntico a un entorno de producción así como una guía de configuración paso a paso incluida en la memoria.
- En el futuro, se puede implementar una variante de este proyecto para permitir que los empleados puedan trabajar desde su propia vivienda ofreciendo facilidades en la conciliación laboral-familiar y un mayor dinamismo.