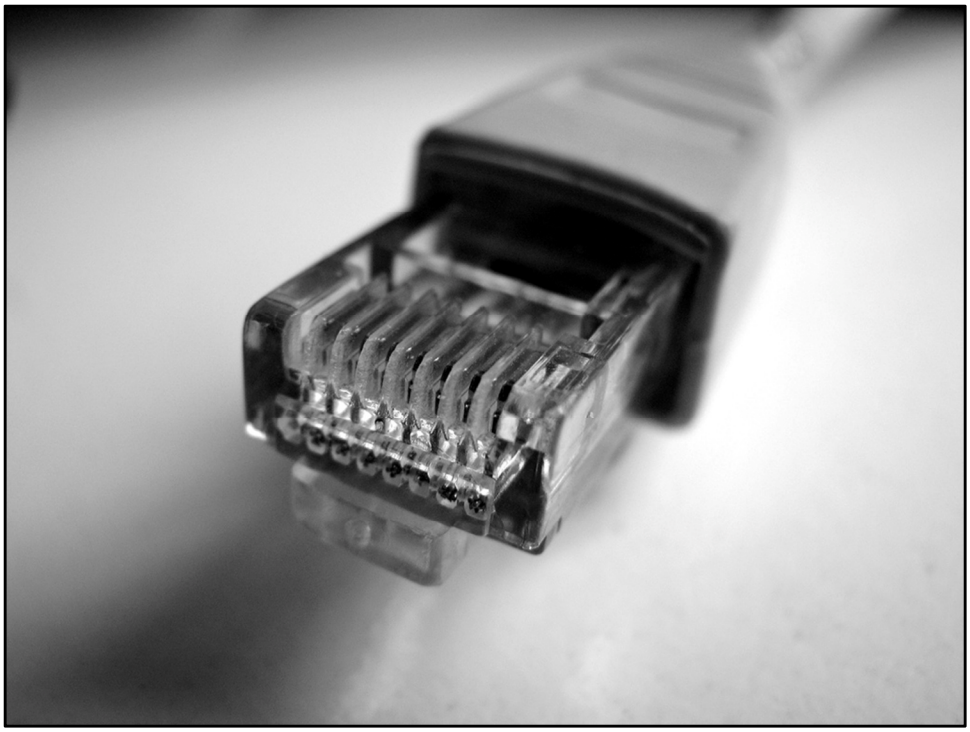

Virtual Private Networks
Cursillos e-ghost Julio 2009
Igor Ruiz Agúndez



Queremos conectar

Distintos puntos

De forma segura.
En definitiva, queremos que la conexión con nuestros servicios sea segura

Índice

¿Por qué estamos aquí?

- El curso está entre los Cursillos de Julio de el grupo de software libre de la Universidad, el eghost
- Pretende dar los primeros pasos, los suficientes para que se pueda seguir aprendiendo de autodidacta
- Los materiales se subirán a la web del eghost

Presentaciones y perfil de los asistentes

Requisitos previos

- Conocimientos básicos de GNU/Linux.
- Conocimientos básicos de redes.

Objetivos del curso

- Conocer más acerca de las VPN
- Aprender a desplegar una VPN
- Aprender a conectarse a una VPN

Temario

- Breve historia de las VPN
- Taxonomía de ataques posibles a las transmisiones de datos
- Breve introducción a la criptografía
- Introducción a OpenVPN
- Taller con OpenVPN

Estructura del curso

- Primer día (2 horas)
  - Teoría
  - Práctica
- Segundo día (2 horas)
  - Práctica

Una Virtual Private Network (VPN) es una serie de herramientas
Permiten conectar redes situadas en distintos lugares de forma segura a pesar de usar una red pública

- Enlaza una o más redes de manera privada permitiendo la comunicación como si fuera punto a punto

Utiliza cifrado para proteger las comunicaciones de ataques como eavesdropping o ataques activos
Utilizadas sobre todo para enlazar oficinas
Antes de su uso las empresas necesitaban circuitos dedicados

Características de una VPN.

Confidencialidad: la información no es interpretar por nadie más que los destinatarios de la misma.

Integridad de los datos: los datos no pueden ser modificados o eliminados durante la transmisión.

Autenticación y autorización: la emisión y recepción se realiza desde dispositivos autorizados.

Un poco de historia (I)

- IPSec fue el primer esfuerzo para desarrollar un estándar para hacer seguras las redes
- La primera versión en 1995
- Los routers no tenían capacidad para implementarlo
- Algunos componentes aún están en desarrollo
- La aparición de SSL/TLS centro los esfuerzos en el nivel de aplicación
- El desarrollo de IPSec es complejo (nivel de kernel y dependiente de la plataforma)

Un poco de historia (II)

- El lento desarrollo de IPSec derivó en otras soluciones
- SSL maduró rápido por su uso en la web
- SSL funciona a nivel de usuario, simplificando su implementación y administración
- La conocida como SSL VPN es realmente una aplicación web que trata de ofrecer VPN sin una implementación completa
- La madurez de GNU/Linux es un test bed excelente para experimentar con redes
- Surgen las interfaces de red TUN/TAP

Interfaces TUN/TAP

- TAP (as in network tap) simula un dispositivo Ethernet operando en la capa 2 con frames Ethernet
- TUN (as in network TUnel) simula un dispositivo de red a nivel de red operando en la capa 3 con paquetes IP
- TAP para crear network bridge
- TUN para routing

From TUN to VPN (I)

- Suponemos interfaz TUN en maquina A y máquina B
- Aplicación en red con dos hilos
  - Copiamos bits desde TUN y lo enviamos a un network socket
  - Copiamos bits desde un network socket a TUN
- Si ejecutamos esta aplicación en ambas máquinas tenemos una VPN muy simple

From TUN to VPN (II)

- Desde A podemos hacer ping al TUN de B, y desde B podemos hacer ping al TUN de A
- El tráfico viajará por una conexión socket encapsulada en UDP o TCP
- Está VPN no tiene seguridad alguna porque los datos viajan en texto plano
- Redirigiendo el tráfico a una herramienta como SSH construiríamos una VPN real

From TUN to VPN (III)

- Esta solución tiene pegas
  - IP es un protocolo no fiable
  - No hay tolerancia a fallos
  - IP asume que pueden perderse o corromperse paquetes. Protocolos como TCP intentan subsanar esto
- Usando SSH encapsulamos IP (que incluye TCP y UDP) en TCP
- Generamos redundancia obteniendo menos eficiencia y menos robustez
- Es mejor encapsular TCP en UDP. Responsabiliza a la aplicación de solucionar los problemas de paquetes perdidos

Encapsulación
UDP vs. TCP

- IP está diseñado para funcionar en enlaces de cable, fibra, o inalámbricos que pueden verse afectados por fallos de sistema o congestiones de tráfico
- Dado que UDP es un protocolo sin tolerancia a fallos, ofrece a IP un entorno lo más parecido a su diseño
- Encapsular IP en UDP es la solución ideal

VPN + UDP

- Actualmente las VPN son portables y fáciles de configurar
- Los paquetes IP provenientes de un interfaz TUN/TAP son cifrados y encapsulados en una conexión UDP y enviados al host remoto
- El host remoto descifra, autentifica y desencapsula los paquetes IP redirigiendo lo a la interfaz TUN/TAP de destino

Transparencia

- El nivel de aplicación VPN enlaza un dispositivo TUN/TAP u otro dispositivo TUN/TAP remoto
- Pueden introducirse reglas de routers y firewalls a TUN/TAP
- Las aplicaciones de usuario no distinguen las interfaces de red de las de las VPN

User-space TUN/TAP vs. IPSec

- User-space es más portable y sencillo de configurar
- IPSec es más complejo, necesita soporte entre soluciones de distintos vendedores
- IPSec es una compleja modificación de la pila IP
- IPSec tiene problemas con NAT
- Idílicamente IPSec simplemente funciona (cifrado oportunista)

The "Two Minds" of IPSec -- N. Ferguson and B. Schneier

- We are of two minds about IPsec. On the one hand, IPsec is far better than any IP security protocol that has come before: Microsoft PPTP, L2TP, etc. On the other hand, we do not believe that it will ever result in a secure operational system. It is far too complex, and the complexity has lead to a large number of ambiguities, contradictions, inefficiencies, and weaknesses. [...] We strongly discourage the use of IPsec in its current form for protection of any kind of valuable information, and hope that future iterations of the design will be improved. However, we even more strongly discourage any current alternatives, and recommend IPsec when the alternative is an insecure network. Such are the realities of the world.

Soluciones VPN

- Protocolos
  - El protocolo estándar de hecho es el IPSEC,
  - También tenemos PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.
- Hardware
  - Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software.
  - SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen, Symantec, Nokia, U.S. Robotics, D-link, etc.
- Software
  - Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general.
  - OpenVPN, Vtun, Tinc, Cipe, OpenSSH, FreeS/Wa

Ataques pasivos y activos

- VPN debe proteger contra ataques pasivos y activos
  - Un atacante pasivo es un oyente furtivo que no puede interrumpir ni modificar el tráfico entre dos puntos
  - Un atacante activo pude interrumpir o modificar o borrar datos del tráfico entre dos puntos
    - a.k.a Man-in-the-middle
- El cifrado es efectivo para detener ataques pasivos
- La autentificación es efectiva para detener ataques activos (i.e. con HMAC)

Replay Attacks

- Suponemos que un atacante se conecta al TUN/TAP de su banco a las 03:00, cuando hay poco tráfico
- Observa el tráfico cifrado cuando se conecta y realiza pequeñas transferencias bancarias
- Realizando análisis de tiempo es capaz de obtener los paquetes cifrados correspondientes a las transferencias
- ¿Qué ocurre si bombardea el banco con muchos de esos paquetes?
- No necesita conocer el algoritmo de cifrado para reproducir paquetes
- El banco necesita protección contra replay attacks
- La inclusión de un timestamp a cada paquete antes de su firma es efectiva para detener ataques de replay

Known plaintext attacks

- Supongamos que un atacante realiza 5 transferencias bancarias de distintas cantidades
- Analizando el texto cifrado podemos discernir que parte del mensaje representa el importe transferido aún cuando los importes en si están cifrados
- El atacante podría insertar valores aleatorios en la parte correspondiente al importe
- El uso de un Initialization Vector (IV) aleatorio es efectivo para detener los known plaintext attacks

Requisitos de seguridad

- El cifrado no es suficiente para protegerse de ataques activos
- Debe combinarse con
  - Autenticación (HMAC)
  - IV aleatorios
  - Timestamp


Rousseau
2007 © John H. Postik

OpenVPN y criptografía

- La criptografía es una ciencia avanzada y especializada
- OpenVPN usa un paradigma modular
- La mayoría de las funciones son de la librería open OpenSSL
- Tiene protección contra ataques pasivos y ataques activos conocidos

Keying

- Soporta cifrado de clave privada y de clave pública
- Provee de claves estáticas y pre-shared para una configuración rápida
- Provee de una infraestructura de clave pública (PKI) completa
- Provee de SSL/TLS para la autentificación inicial y para el intercambio de claves simétricas
- La autentificación lleva a un problema de gestión de claves
  - HMAC necesita de un secreto compartido

Public key cryptography (I)

- In the September, 1977 issue of The Scientific American, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman introduced to the world their RSA cipher, applicable to public key cryptography and digital signatures. The authors offered to send their full report to anyone who sent them self-addressed stamped envelopes, and the ensuing international response was so overwhelming the NSA balked at the idea of such widespread distribution of cryptography source code. When no response was made by the NSA as to the "legal basis of their request", distribution recommenced, and the algorithm was published in The Communications of the ACM the following year.

Public key cryptography (II)

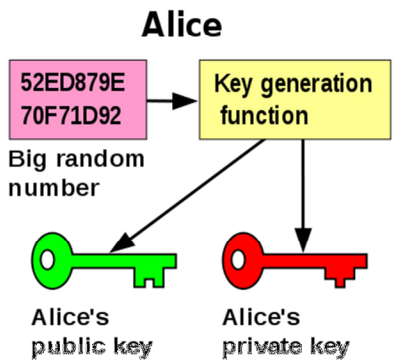
- La criptografía de clave pública es una solución al problema de autentificación
- Antes de la aparición de los ordenadores la criptografía se practicaba entre individuos que conocían una clave compartida
- La criptografía de clave pública permite que individuos se comuniquen de forma segura sin necesidad de un canal seguro previo para el envío de las claves
- Permite crear un canal seguro sobre el que enviar una clave compartida con la que por motivos de eficiencia se realizará el cifrado

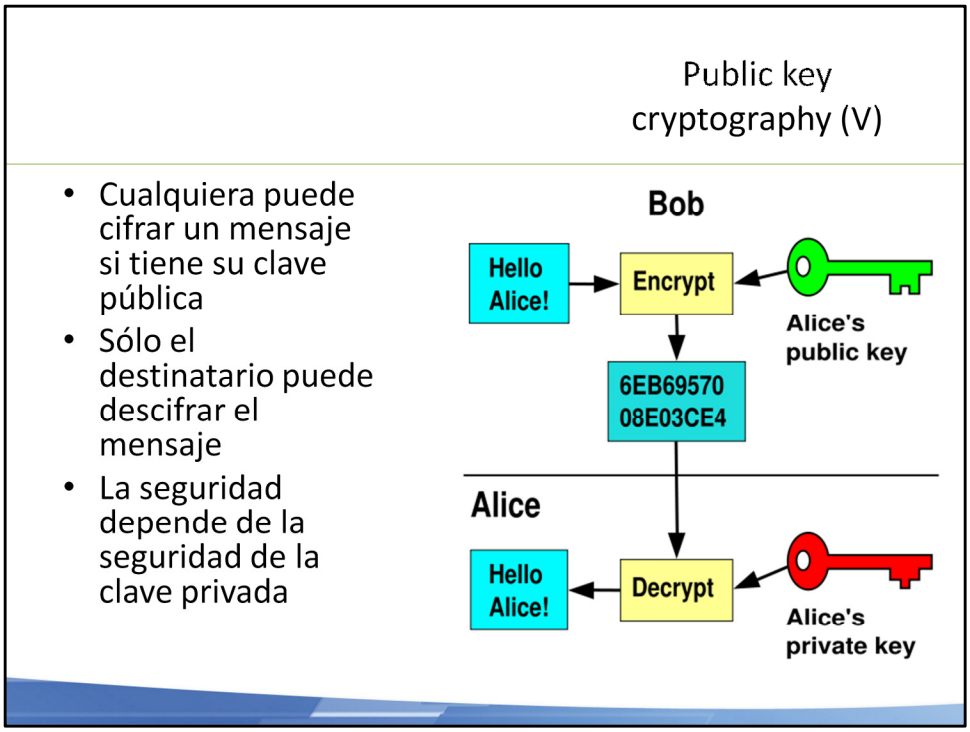
Public key cryptography (III)

- La criptografía de clave pública permite generar un par de claves pública y privada
- La clave privada es secreta
- La clave pública es compartida
- Para cifrar se utiliza la clave pública
- Para descifrar se utiliza la clave privada
- También es utilizada para autentificar el origen mediante certificados

Public key cryptography (IV)

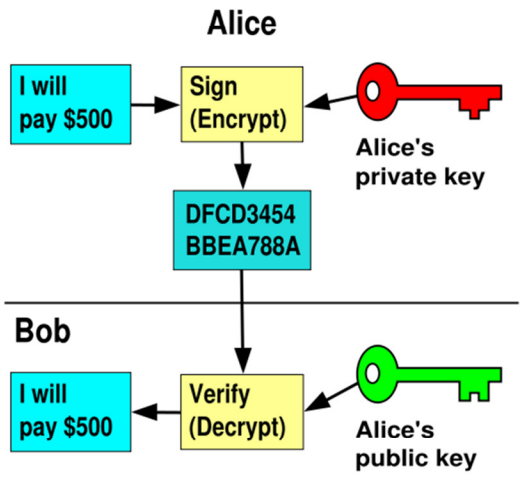
- Se genera un número aleatorio muy grande
- Usado para la generación de un par de claves aceptable para su uso por el algoritmo asimétrico




Public key cryptography (V)
Cualquiera puede cifrar un mensaje si tiene su clave pública
Sólo el destinatario puede descifrar el mensaje
La seguridad depende de la seguridad de la clave privada
Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Public key cryptography (VI)

- La clave privada se utiliza para firmar
- Cualquiera puede validar la firma con la clave pública



Certificados

- La criptografía de clave pública fue la pionera en el concepto de firmas seguras
- La certificate authority (CA) resuelve el problema de la autenticación
- La CA tiene una clave maestra
- Esta clave firma las claves de los clientes
- Resuelve el problema de la autentificación gracias a un punto central de confianza

Resumen

- OpenVPN protege contra ataques activos, pasivos, replay, Known plaintext entre otros
- No protege contra ataques como el análisis de tráfico
  - Solución: generar tráfico aleatorio de forma que el flow de la comunicación sea constante
- No protege contra ataques desconocidos
- Es una buena solución para las necesidades de la mayoría de los usuarios que necesitan una VPN

Conclusiones

- Las VPN une conceptos relativos a la criptografía, las redes y los firewalls
- Es modulable y escalable. Desde una solución de comunicación sencilla a una WAN segura
- Tienen mucho por recorrer hasta que sean automáticamente configurables dinámicamente y en cualquier lugar


OPENVPN™
TECHNOLOGIES

Características de OpenVPN

- OpenVPN persigue ofrecer todas las posibilidades que dan las VPN
- Portabilidad
- Desplegable como un servicio/daemon
- No requiere modificaciones de kernel
- Actualizado al usar la librería OpenSSL
- Soporta direcciones dinámicas y NAT
- Disponible en “todos” los sistemas operativos

Seguridad en 3 niveles (I)

- La complejidad es el mayor enemigo de la seguridad
- Una sencilla forma de hacer más seguro el software es hacer pasar el tráfico entrante por un firewall en lugar de filtrar paquetes en el nivel de aplicación

Seguridad en 3 niveles (II)

- Nivel 1: Previene a un atacante de inyectar paquetes en el subsistema SSL/TLS. Comprueba la firma de los paquetes antes de aceptarlos
- Nivel 2: Utiliza SSL/TLS para autentificación bidireccional (tanto cliente como servidor)
- Nivel 3: Puede ejecutarse con un bajo nivel de privilegios para evitar inyecciones de código

Routing vs. Bridging (I)

- Existen dos técnicas para construir una VPN
  - Bridging: permite crear una red LAN virtual que funcione en una única subred (único dominio de broadcast)
    - Permite funcionar a programas que necesiten broadcast
    - No hay que configurar rutas
    - Funciona con cualquier protocolo ethernet
    - Sencillo para soluciones road warriors
    - Menos eficiente que routing, no escala bien

Routing vs. Bridging (II)

- Existen dos técnicas para construir una VPN
  - Routing: permite crear una red LAN virtual con varias subredes y con rutas entre ellas (varios dominios de broadcast)
    - Eficiente y escalable
    - Permite ajustar mejor el Maximum Transmission Unit(MTU)
    - En Windows, los clientes requieren un servidor WINS para descubrimiento
    - Deben definirse reglas para cada subnet
    - Software que utilice broadcast no funcionará con las máquinas tras la VPN

VPN + Firewall

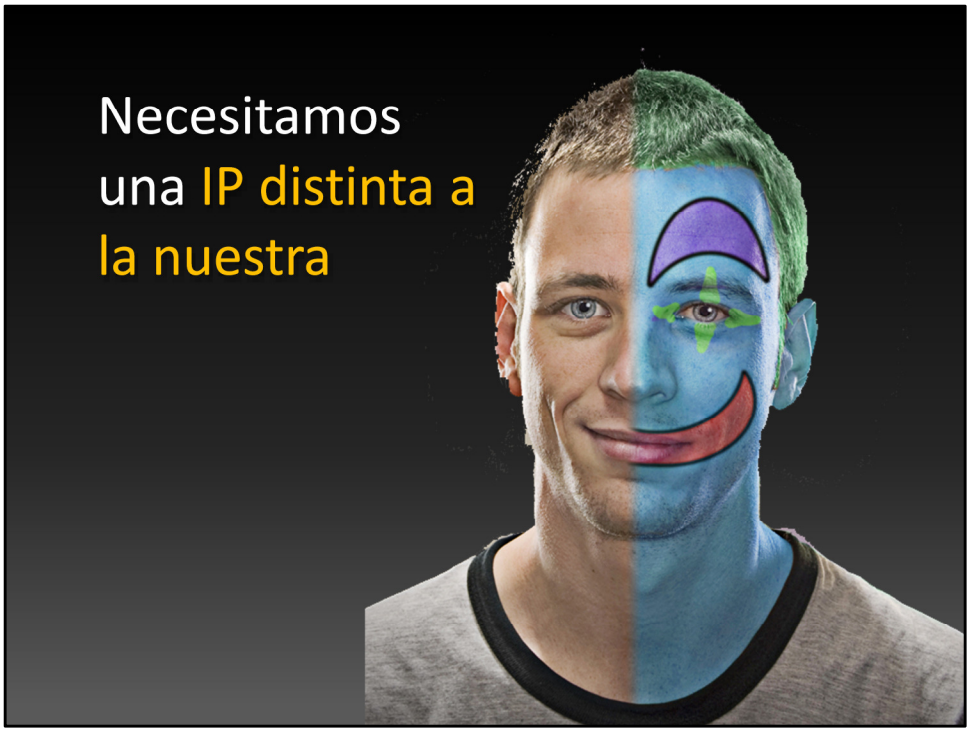
- Las VPN actuales usan interfaces TUN/TAP como endpoints
- Pueden aplicarse políticas de firewall sobre estas interfaces
- Las reglas de firewall sobre una VPN pueden crear una relación de confianza entre dos redes


Casos de uso
Nuts II © 2009 Mark Tomlinson

Imaginad que estamos en nuestra oficina de Miami Beach y queremos conectarnos a los recursos de nuestra oficina central. También podríamos querer conectarnos al equipamiento de una fábrica remota o incluso a nuestra propia casa.

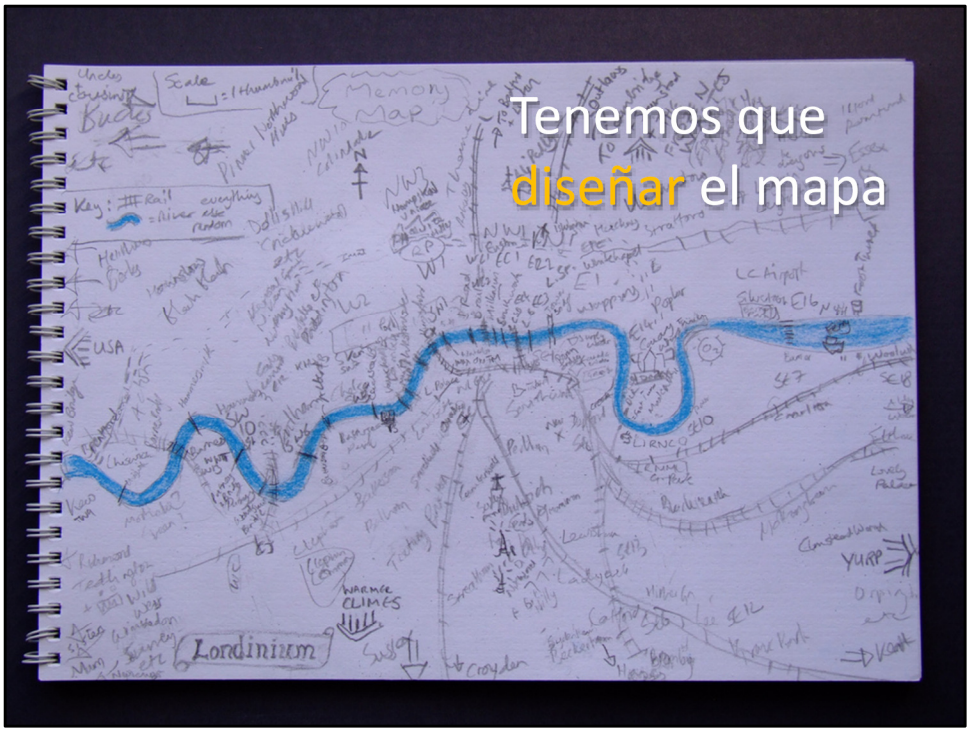
Queremos que la conexión con estos servicios sea segura

Estamos en una red que no permite conectividad a ciertos servicios.
Filtrado de puertos
Intrusion Detection Systems (IDS)
Intrusion Prevention Systems (IPS)



Necesitamos una IP distinta de la que nos ofrece la red en la que estamos
Internet TV, servicios basados en IP de origen…


Pasos a realizar



Design

- Equipos finales
- Equipos de respaldo (servidores)
- Redes y subredes
- Bridge vs. Routing
- Mapa de red

Build
- Servicio de OpenVPN
- Infraestructura de claves
- Generación de claves
- Configuración

Run
- Pruebas y documentación
- Explotación

Manage
- Control

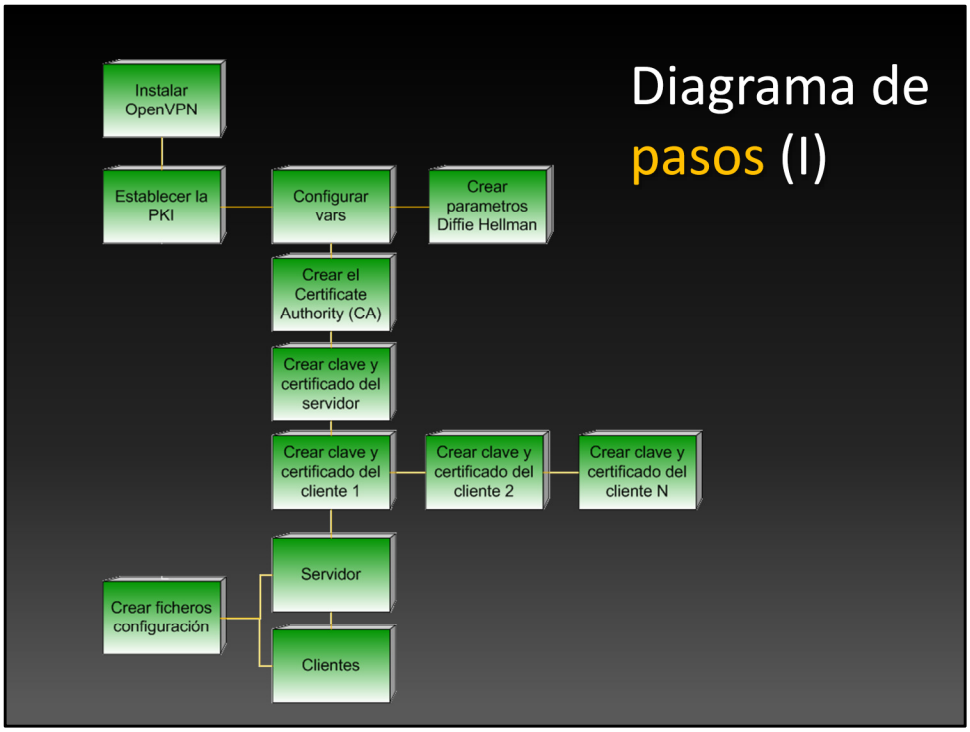


Diagrama de pasos (I)
Instalar OpenVPN
Establecer la PKI
Configurar vars
Crear parametros Diffie Hellman
Crear el Certificate Authority (CA)
Crear clave y certificado del servidor
Crear clave y certificado del cliente 1
Crear clave y certificado del cliente 2
Crear clave y certificado del cliente N
Crear ficheros configuración
Servidor
Clientes

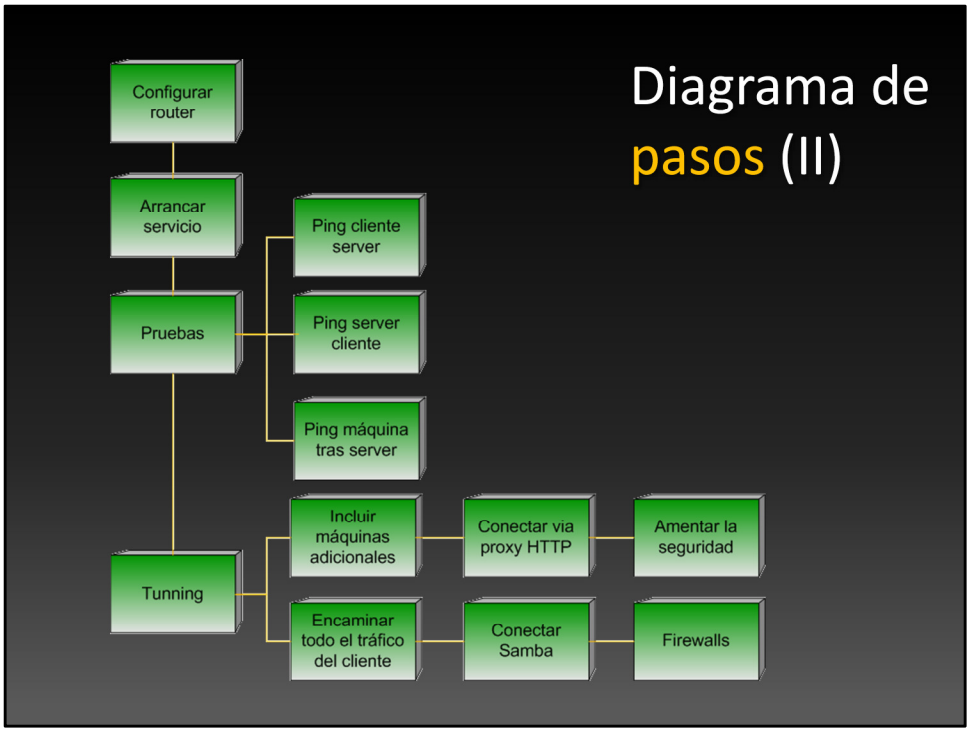


Diagrama de pasos (II)
Configurar router
Arrancar servicio
Pruebas
Ping cliente server
Ping server cliente
Ping máquina tras server
Tunning
Incluir máquinas adicionales
Conectar via proxy HTTP
Amentar la seguridad
Encaminar todo el tráfico del cliente
Conectar Samba
Firewalls

Encuestas de satisfacción

http://www.e-ghost.deusto.es/cursillosjulio/encuestas/

Hay 2 encuestas:
1) Para cada cursillo (vía PHP sólo se deja rellenar encuestas de cursillos el mismo día que acaban dichos cursillos).

2) La encuesta general (a rellenar el ultimo dia del ultimo cursillo al que se asista, para dar una visión en conjunto)


Virtual Private Networks
www.bideidea.com
igor [AT] bideidea [DOT] com

Bibliografía

- OpenVPN [Link]
- The User-Space VPN and OpenVPN [Link]
- Implementación de una red VPN con la aplicación OpenVPN en un servidor [Link]
- Public-key cryptography [Link]
- Red privada virtual [Link]

Intelectual Property Rights

Intelectual Property Rights

All images are property of their respective owners

Todas las imágenes son propiedad de sus respectivos dueños