



**UNIVERSIDAD CENTRAL DE VENEZUELA
COMISIÓN DE ESTUDIOS DE POSTGRADO
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA**

**Diseño e Implantación de una WAN Segura para el
Transporte y Procesamiento de Datos Estadísticos del
Instituto Nacional de Estadística (INE)**

Por:

Ing. Nando Alessio Vitti Vitti

Tutor Académico:

Prof. Vincenzo Mendillo

Trabajo de Grado presentado ante la ilustre
Universidad Central de Venezuela
para optar al Título de
Especialista en Comunicaciones y Redes de Comunicación de Datos

Caracas, 20 de Noviembre del 2003

Dedicatoria

A la memoria de mi ejemplar padre Onorio Vitti

A mi madre Maria Vitti

A mi hermano Aurelio Vitti

A mis hijas Minervita y Michelle

Título del trabajo: Diseño e Implantación de una WAN Segura para el Transporte y Procesamiento de Datos Estadísticos del Instituto Nacional de Estadística (INE)

Resumen

El presente trabajo trata sobre el diseño e implantación de la WAN Segura del Instituto Nacional de Estadísticas (INE) para el transporte de datos estadísticos a nivel nacional desde el interior del país y Caracas hasta la sede principal del INE. La red abarcará el desarrollo de tres (3) nodos regionales ubicados en Maracay, Valencia y Maracaibo, para ampliarse posteriormente al resto de las capitales de estado. La Red Platino, actualmente en servicio, se utilizará como puente entre los nodos regionales y la sede principal del INE, por lo que el proyecto incluye las adecuaciones necesarias en ambas redes para proveer las características de seguridad requeridas: confidencialidad, integridad, autenticación y disponibilidad. El diseño se fundamenta en el uso del equipo Equipo Firebox, de la empresa WatchGuard, como elemento de seguridad para proporcionar los servicios de Firewall/Proxy, túneles VPN, NAT, entre otros. También se utilizan servicios como SQUID e IPTABLES, soportados en LINUX para tareas específicas. Finalmente se provee un sistema de contingencia para casos de fallas en la red principal.

La red fue instalada y probada en los aspectos de tráfico y seguridad, sin embargo, por motivos económicos, debió suspenderse el uso del servicio Frame Relay por parte de CANTV. Esta situación prevalecerá hasta que se resulta el problema de la nueva adscripción de Red Platino.

En el Capítulo I se expone la teoría básica de los servicios tratados en el proyecto. En el Capítulo II se tratan la situación actual de la red Platino-INE y la solución propuesta mediante el uso de las redes seguras. Finalmente, en el Capítulo III se explica la ingeniería de detalle aplicada para la distribución física de las redes y la configuración de equipos.

Caracas, Noviembre 2003

Índice de contenido

| Contenido | Página |
|--|------------|
| Capítulo 1 : Marco Teórico..... | 1 |
| 1.1 Servicio DHCP..... | 1 |
| 1.2 Servicio NAT..... | 3 |
| 1.3 Servicio Firewall/Proxy..... | 8 |
| 1.4 Ataques Comunes..... | 22 |
| 1.5 Criptografía..... | 29 |
| 1.6 Redes Virtuales Privadas (VPN)..... | 35 |
| Capítulo 2: Solución planteada para la WAN Segura..... | 49 |
| 2.1 Situación Actual de la Plataforma INE-Red Platino..... | 49 |
| 2.2 Desarrollo de la Solución para la WAN de INE..... | 50 |
| 2.3 Fase I Estudio de Flujo de Datos..... | 51 |
| 2.4 Fase II Topología, Arquitectura y Planes de Enrutamiento/Direccionamiento..... | 54 |
| 2.5 Fase III Diseño de las Políticas y Mecanismos de Seguridad..... | 59 |
| 2.6 Fase IV Diseño y Desarrollo de los Nodos Regionales..... | 61 |
| 2.7 Fase V Adecuación de la Red Platino..... | 70 |
| 2.8 Fase VI Adecuación de la Red INE..... | 78 |
| 2.9 Fase VII Sistema de Contingencia..... | 82 |
| 2.10 Fase VIII Supervisión y Monitoreo de la WAN..... | 83 |
| Capítulo 3: Ingeniería Básica de Detalle..... | 86 |
| 3.1 Configuración del Equipo Firebox..... | 87 |
| 3.2 Servicios IPTABLES y SQUID sobre Sistema Operativo Linux..... | 140 |
| 3.3 Configuración de los Conmutadores..... | 150 |
| 3.4 Configuración de los Enrutadores..... | 152 |
| 3.5 Configuración de los Servidores..... | 154 |
| 3.6 Estructura Física de la Red..... | 156 |
| Conclusiones | 164 |
| Recomendaciones..... | 165 |
| Referencias..... | 166 |
| Bibliografía..... | 166 |

Indice de Figuras

| Figura | Página |
|---|--------|
| Figura N° 1 Uso del NAT..... | 6 |
| Figura N° 2 Distribución más simple de un host de bastión | 10 |
| Figura N° 3 Un host de bastión con una sola interfaz..... | 11 |
| Figura N° 4 El filtro de paquetes | 12 |
| Figura N° 5 La configuración de la tabla de enrutamiento..... | 12 |
| Figura N° 6. Los servidores proxy | 15 |
| Figura N° 7 Un cortafuegos/servidor proxy..... | 17 |
| Figura N° 8 Acceso al Web desde adentro..... | 20 |
| Figura N° 9 La arquitectura Proxy Server..... | 21 |
| Figura N° 10 Cumplimiento de peticiones proxy..... | 21 |
| Figura N° 11 IP Spoofing | 24 |
| Figura N° 12 Uso de los flags..... | 26 |
| Figura N° 13 Ataque TCP SYN..... | 26 |
| Figura N° 14 Ataque SMURF | 28 |
| Figura N° 15 Proceso de Cifrado..... | 29 |
| Figura N° 16 Algoritmos y transmisión de claves..... | 30 |
| Figura N° 17 Criptografía simétrica y asimétrica..... | 31 |
| Figura N° 18 Sistema DES..... | 32 |
| Figura N° 19 Firma Digital..... | 34 |
| Figura N° 20 Prueba de la autenticidad de un mensaje..... | 34 |
| Figura N° 21 Comparación entre línea dedicada y VPN..... | 36 |
| Figura N° 22 Una conexión RAS convencional..... | 36 |
| Figura N° 23 Una conexión por Internet..... | 37 |
| Figura N° 24 Un datagrama IPSec y el header AH..... | 41 |
| Figura N° 25 Detalles del header AH..... | 42 |
| Figura N° 26 Estructura de los datagramas..... | 43 |
| Figura N° 27 Detalles del header ESP..... | 43 |
| Figura N° 28 Firewall y VPN..... | 48 |
| Figura N° 29 VPN + firewall..... | 48 |
| Figura N° 30 Diagrama General de la WAN..... | 53 |
| Figura N° 31 Túneles VPN en la WAN de INE..... | 61 |
| Figura N° 32 Nodo Regional..... | 62 |
| Figura N° 33 Red Platino..... | 71 |
| Figura N° 34 Control de Tráfico..... | 76 |

| | | |
|--------------|--|-----|
| Figura N° 35 | Sitio www.sistine.gov.ve | 79 |
| Figura N° 36 | Red INE..... | 80 |
| Figura N° 37 | Conexión de Usuarios Remotos..... | 83 |
| Figura N° 38 | Supervisión de la WAN..... | 85 |
| Figura N° 39 | Equipo de Seguridad "Equipo Firebox" | 87 |
| Figura N° 40 | El Equipo Firebox y su entorno..... | 88 |
| Figura N° 41 | Modos de Operación del Equipo Firebox..... | 91 |
| Figura N° 42 | Modo Enmascarado ("drop-in")..... | 94 |
| Figura N° 43 | Configuración de Interfaces | 95 |
| Figura N° 44 | Modo "Drop-In"..... | 96 |
| Figura N° 45 | Servicio DHCP..... | 98 |
| Figura N° 46 | Tipos de NAT en el Equipo Firebox..... | 100 |
| Figura N° 47 | Servicio NAT | 101 |
| Figura N° 48 | Asignación de dirección al servicio..... | 104 |
| Figura N° 49 | Ejemplos de NAT's estáticos..... | 105 |
| Figura N° 50 | Control de tráfico Web: applets y similares..... | 108 |
| Figura N° 51 | Control de tráfico Web..... | 109 |
| Figura N° 52 | "Arena" de servicio..... | 110 |
| Figura N° 53 | Políticas de uso del HTTP..... | 111 |
| Figura N° 54 | Bloqueo de HTTP saliente..... | 112 |
| Figura N° 55 | SMTP Proxy: Controlando el contenido del correo..... | 113 |
| Figura N° 56 | SMTP Proxy: Evitando el "Open Relay"..... | 115 |
| Figura N° 57 | Creación de un Alias..... | 118 |
| Figura N° 58 | Proceso de Autenticación..... | 119 |
| Figura N° 59 | Tipo de Autenticación..... | 120 |
| Figura N° 60 | Autenticación para usuario remoto..... | 121 |
| Figura N° 61 | Pantalla inicial para la autenticación..... | 122 |
| Figura N° 62 | Red VPN entre sucursales..... | 123 |
| Figura N° 63 | Configuración del gateway IPsec (manual)..... | 125 |
| Figura N° 64 | Configuración del gateway IPsec (dinámica)..... | 125 |
| Figura N° 65 | Configuración de Túneles (manual)..... | 126 |
| Figura N° 66 | Configuración de Túneles (automática)..... | 127 |
| Figura N° 67 | Túneles para usuarios remotos y móviles..... | 130 |
| Figura N° 68 | Usuarios en los grupos ipsec_users y pptp_users..... | 132 |
| Figura N° 70 | Túneles VPN configurados..... | 135 |
| Figura N° 71 | Status Report | 137 |
| Figura N° 72 | Conexiones por Tipo de Servicio..... | 138 |
| Figura N° 73 | Visualización de los logs..... | 140 |

| | |
|--|-----|
| Figura N° 74 SQUID e IPTABLES..... | 142 |
| Figura N° 75 Diagrama de Planta Nodo Regional Maracay..... | 157 |
| Figura N° 76 Diagrama de Planta Nodo Regional Valencia..... | 159 |
| Figura N° 77 Diagrama de Planta Nodo Regional Maracaibo..... | 161 |

Indice de Tablas

| Tabla | Página |
|---|--------|
| Tabla n°1 Formato del mensaje DHCP..... | 3 |
| Tabla n° 2 Traducciones dinámicas..... | 7 |
| Tabla n° 3 Traducciones Estáticas..... | 8 |
| Tabla n° 4 Direcciones IP Red Platino..... | 57 |
| Tabla n° 5 Incoming requests by method..... | 77 |
| Tabla n° 6 Requested extensions..... | 78 |
| Tabla n° 7 Conmutador Nodo INE..... | 161 |
| Tabla n° 8 Conmutador Nodo Regional..... | 162 |
| Tabla n° 9 Conmutador Nodo Platino..... | 163 |

Introducción

El presente trabajo trata sobre el estudio, diseño y desarrollo de la WAN Segura del INE (Instituto Nacional de Estadísticas) para la recolección y el transporte de datos a nivel nacional. El proyecto contempla, inicialmente, la creación de tres nodos piloto regionales ubicados en Maracay, Valencia y Maracaibo, donde operan actualmente las coordinaciones regionales de INE. También considera la adecuación y reorganización de las LAN's existentes en los nodos Platino (Plataforma Nacional de Información) e INE, las cuales deberán integrarse a los nodos regionales.

El objetivo primordial es la recolección de datos en los puntos donde se produzca el evento estadístico (encuestas de censo, encuestas a la industria, etc.) y su inmediata transmisión a los servidores ubicados en la sede principal de INE, donde serán analizados y procesados, para posteriormente publicarlos en forma electrónica o impresa.

A nivel tecnológico, el proyecto se fundamenta en la red pública transporte Frame Relay y en la versatilidad del equipo de seguridad Equipo Firebox de la empresa WatchGuard. Sin embargo, también se incorporan otros elementos, como las herramientas SQUID e IPTABLES para el control de tráfico, enrutadores, conmutadores, etc.

Los siguientes capítulos cubren estos contenidos:

Capítulo 1: Aspectos teóricos de la seguridad, tipos de ataques y técnicas de defensa.

Capítulo 2: Situación actual de la red INE.

Capítulo 3: Solución planteada. Incluye planes de enrutamiento, direccionamiento IP y técnicas aplicadas de seguridad, entre otros.

Capítulo 4: Ingeniería de detalle para la solución planteada. Se describen, en detalle, las configuraciones de equipos, diagramas de piso y cableado.

Finalmente se presentan las conclusiones y recomendaciones.