

Proyecto de fin de carrera:

Monitorización remota en redes de área local

Autor: Rafael Micó Miranda

Tutor: D. Antonio J. Estepa Alonso

Ingeniería de Telecomunicación

Departamento de Ingeniería de Sistemas y Automática

Área de Ingeniería Telemática



Escuela Superior de Ingenieros



Universidad de Sevilla

Índice general

1. Introducción y objetivos	11
2. Análisis de requisitos y descripción funcional del sistema	15
2.1. Introducción	15
2.2. Catálogo de requisitos	15
2.3. Funcionalidades de la solución planteada	17
2.3.1. Justificación	20
3. Planificación y costes	25
3.1. Planificación del Proyecto	25
3.2. Estimación de costes	25
4. Monitorización estadística de tráfico	29
4.1. Introducción a <i>NetFlow</i>	29
4.2. Sonda de <i>NetFlow</i> : <i>fprobe-ng</i>	30
4.2.1. Sondas de <i>NetFlow</i>	30
4.2.2. Introducción al paquete <i>fprobe-ng</i>	31
4.2.3. La sonda y el protocolo <i>NetFlow</i>	32
4.3. Recolector de <i>NetFlow</i> : <i>flow-tools</i>	33
4.3.1. Recolectores de <i>NetFlow</i>	33
4.3.2. Introducción al paquete <i>flow-tools</i>	33
4.3.3. El recolector y el protocolo <i>NetFlow</i>	34
4.4. Consideraciones de seguridad para <i>NetFlow</i>	34
5. Monitorización de tráfico	37
5.1. La retransmisión del tráfico	37
5.2. Retransmisión del tráfico: <i>iptables</i>	39
5.2.1. Introducción a <i>iptables</i>	39
5.2.2. <i>iptables</i> y el módulo <i>ROUTE</i>	39
5.3. Ejecución remota de operaciones	41
6. Recogida de registros	43
6.1. Introducción a los registros del sistema	43
6.2. Estado del arte	44
6.3. Recogida de registros: <i>syslog-ng</i>	45
6.3.1. Introducción al paquete <i>syslog-ng</i>	45
6.4. Consideraciones de seguridad: <i>stunnel</i> y <i>openssl</i>	45

7. Tratamiento de la información	49
7.1. Tratamiento de la información de <i>NetFlow</i>	49
7.1.1. Presentación mediante consola	50
7.1.2. Exportando a <i>ntop</i>	50
7.1.3. Exportando a una base de datos	51
7.2. Tratamiento de la información de los registros	53
7.2.1. Visualización en consola	53
7.2.2. Visualización mediante página <i>Web</i>	54
8. Interfaz de configuración	57
8.1. Introducción	57
8.2. Estudio de viabilidad	58
8.3. Análisis	60
8.3.1. Catálogo de requisitos de la interfaz	60
8.3.2. Modelo del sistema	61
8.4. Diseño	65
8.4.1. Consideraciones sobre la arquitectura del sistema	65
9. Conclusiones y líneas de avance	67
9.1. Conclusiones	67
9.2. Futuras líneas de avance	68
A. Monitorización estadística de tráfico	71
A.1. <i>NetFlow</i> versión 7	71
A.2. Instalación y configuración de la sonda	74
A.2.1. Instalación de <i>fprobe-ng</i>	74
A.2.2. Configuración de <i>fprobe-ng</i>	74
A.3. Instalación y configuración del recolector	76
A.3.1. Instalación de <i>flow-tools</i>	76
A.3.2. Configuración de <i>flow-capture</i>	76
B. Monitorización de tráfico	79
B.1. Instalación del módulo <i>ROUTE</i>	79
B.1.1. Obtención de los paquetes	79
B.1.2. Aplicando <i>patch-o-matic-ng</i> para compatibilizar con el módulo <i>ROUTE</i>	82
B.1.3. Compilación e instalación del <i>kernel</i>	83
B.1.4. Compilación en instalación de <i>iptables</i>	87
B.1.5. Activación del módulo <i>ROUTE</i>	92
B.2. Instalación y configuración del paquete <i>ssh</i>	93
B.2.1. Instalación de <i>ssh</i>	93
B.2.2. Configuración de <i>ssh</i>	94
C. Recogida de registros	97
C.1. Instalación y configuración de <i>syslog-ng</i>	97
C.1.1. Instalación de <i>syslog-ng</i>	97
C.1.2. Configuración de <i>syslog-ng</i>	97
C.2. Consideraciones de seguridad: transporte mediante <i>stunnel</i>	105
C.2.1. Instalación de <i>stunnel</i>	105
C.2.2. Configuración de <i>stunnel</i>	106

C.2.3.	Autenticación mediante <i>stunnel</i> : el paquete <i>openssl</i>	108
D.	Tratamiento de la información	113
D.1.	Tratamiento de la información de <i>NetFlow</i>	113
D.1.1.	Presentación mediante consola	113
D.1.2.	Exportando a <i>ntop</i>	118
D.1.3.	Exportando a una base de datos <i>MySQL</i>	123
D.1.4.	Exportando a bases de datos <i>Round Robin</i>	126
D.2.	Tratamiento de la información de los registros	139
D.2.1.	Visualización en consola y página <i>Web</i> : <i>ccze</i>	139
E.	Interfaz de configuración	143
E.1.	Requisitos previos para la interfaz	143
E.1.1.	Servidor <i>Web</i> : <i>lighttpd</i>	143
E.1.2.	Soporte PHP: <i>PEAR</i>	145
E.1.3.	Ejecución de instrucciones con privilegios: <i>sudo</i>	146
E.1.4.	Acceso a ficheros con privilegios restringidos	147
E.1.5.	Ejecutando <i>lighttpd</i> como superusuario	148
E.2.	Construcción de la interfaz	149
E.2.1.	Estructura de los ficheros fuente	149
E.2.2.	Notas sobre la implementación	150
E.3.	Instalación de la interfaz	160
E.4.	Interfaz para <i>flow-capture</i>	161
E.4.1.	Formulario de configuración	161
E.4.2.	Importación y exportación de parámetros desde otros módulos	163
E.5.	Interfaz para <i>FlowScan</i>	163
E.5.1.	Formulario de configuración	163
E.5.2.	Importación y exportación de parámetros desde otros módulos	165
F.	Validación y pruebas realizadas	167
F.1.	Escenario de pruebas	167
F.2.	Pruebas de depuración realizadas sobre la interfaz	169
F.2.1.	Depuración de la interfaz para <i>flow-capture</i>	169
F.2.2.	Depuración de la interfaz para <i>FlowScan</i>	170
Bibliografía		171

Índice de cuadros

3.1. Planificación temporal del Proyecto	26
3.2. Coeficientes del modelo	26
4.1. Ficha de <i>fprobe-ng</i>	32
4.2. Ficha de <i>flow-tools</i>	34
5.1. Ficha de <i>Linux Kernel</i>	40
5.2. Ficha de <i>iptables</i>	40
5.3. Ficha de <i>patch-o-matic-ng</i>	40
5.4. Ficha de <i>ssh</i>	42
6.1. Ficha de <i>syslog-ng</i>	46
6.2. Ficha de <i>stunnel</i>	47
6.3. Ficha de <i>openssl</i>	48
7.1. Ficha de <i>flowscan</i>	52
7.2. Ficha de <i>flowscan-cuflow</i> y <i>flowscan-cugrapher</i>	53
7.3. Ficha de <i>flowscan-flowmonitor</i>	53
7.4. Ficha de <i>ccze</i>	55
A.1. Campos de la cabecera de <i>NetFlow V7</i>	72
A.2. Campos del registro de <i>NetFlow V7</i>	73
A.3. Parámetros de <i>fprobe-ng</i>	75
A.4. Parámetros de <i>flow-capture</i>	77
C.1. Parámetros de <i>stunnel</i>	106
D.1. Parámetros de <i>flow-cat</i>	114
D.2. Parámetros de <i>flow-print</i>	114
D.3. Parámetros de <i>flow-nfilter</i>	116
D.4. Parámetros de <i>flow-stat</i>	117
D.5. Parámetros de <i>flow-send</i>	119
D.6. Parámetros de <i>flow-fanout</i>	122
D.7. Parámetros de <i>flow-export</i>	123
D.8. Relación de la exportación de <i>flow-export</i> con los campos de <i>NetFlow V7</i>	124
D.9. Parámetros de <i>ccze</i>	139
E.1. Objeto Config para <i>flow-capture.conf</i>	156

ÍNDICE DE CUADROS

E.2. Objeto Config para <code>flowsan.cf</code>	157
E.3. Objeto Config para <code>CUFLOW.cf</code>	159

Índice de figuras

2.1. Ejemplo de red con <i>DMZ</i> intermedia	16
2.2. <i>DMZ</i> intermedia con sistema de monitorización	18
2.3. Funcionalidades y su identificación con la red de ejemplo	19
4.1. Ubicación de las sondas y el recolector	30
4.2. Separación de la red de datos de la red de datos de gestión	35
5.1. Tráfico retransmitido capturado con <i>ethereal</i>	38
5.2. Esquema de funcionamiento de la retransmisión de tráfico	41
6.1. Ubicación de <i>syslog-ng</i>	46
6.2. Uso de <i>stunnel</i>	47
7.1. Plugin de <i>ntop</i> para activar el soporte de <i>NetFlow</i>	51
8.1. Diagrama de clases de la interfaz	62
A.1. Esquema de funcionamiento de la sonda y el recolector	78
B.1. Menú de configuración del <i>kernel</i> en modo consola	84
B.2. Ubicación del módulo <i>ROUTE</i>	93
B.3. Uso de <i>ssh</i> y sus llaves para la ejecución de comandos	95
C.1. Esquema de funcionamiento de <i>syslog-ng</i>	105
C.2. Esquema de funcionamiento de <i>syslog-ng</i> con <i>stunnel</i>	108
C.3. Esquema de funcionamiento de <i>syslog-ng</i> con <i>stunnel</i> y certificados de <i>openssl</i>	112
D.1. Esquema de funcionamiento de <i>flow-send</i> para la exportación a <i>ntop</i>	119
D.2. Esquema de funcionamiento de <i>flow-fanout</i> para la exportación a <i>ntop</i>	121
D.3. <i>ntop</i> con la información ya exportada	122
D.4. Scoreboard de <i>CUFlow</i>	132
D.5. Presentación de <i>CUGrapher</i>	134
D.6. Uso de <i>ccze</i> mediante consola	140
D.7. Uso de <i>ccze</i> mediante página <i>Web</i>	141
E.1. Pantalla principal de la interfaz de configuración.	160

ÍNDICE DE FIGURAS

E.2. Interfaz de configuración de <i>flow-capture</i>	161
E.3. Interfaz de configuración de <i>FlowScan</i>	163