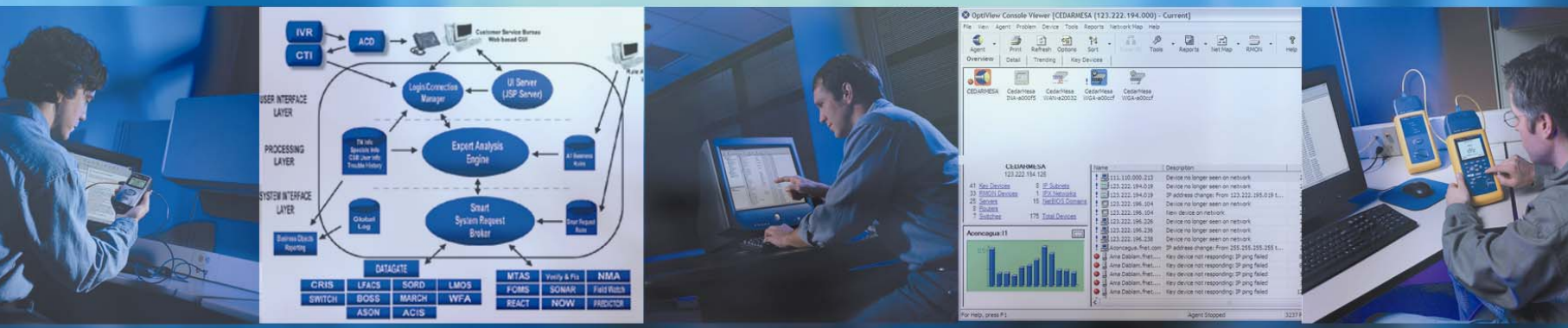
Cisco IOS NetFlow:
El sistema más completo y eficiente de controlar el tráfico de Aplicaciones



NETWORKSUPERVISION

Web: www.flukenetworks.com/es

Agenda: 28 de Febrero	
8.30 – 9.00	Registro
9.00 – 11.00	La calidad de servicio al usuario: Lo único importante
11.00 – 11.30	Pausa Café
11.30 – 13.30	Cisco IOS NetFlow: El sistema más completo y eficiente de controlar el tráfico de Aplicaciones
15.00 – 15.30	Registro
15.30 – 17.00	Monitorización y Análisis de Redes VoIP
17.00 – 17.30	Pausa Café
17.30 – 19.00	Monitorización y Análisis de Redes Inalámbricas

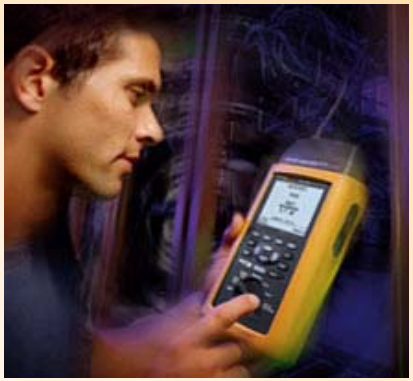
Gamas de productos

Enterprise SuperVision (ESV)

Sistemas distribuidos y analizadores portátiles

Infrastructure SuperVision (ISV)

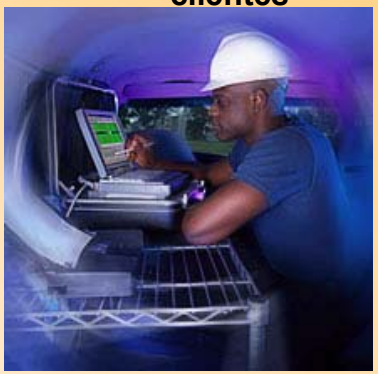
Certificación de la infraestructura de cobre y fibra



Outside Plant SuperVision (OSV)

Soluciones Telecomunicaciones.

Medición de enlaces de clientes



Enterprise SuperVision

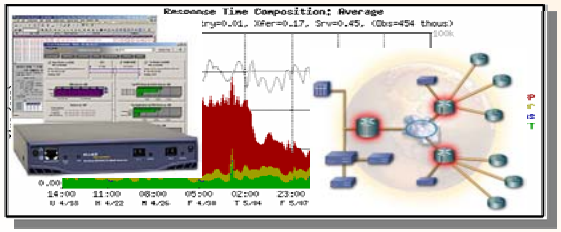
Sistemas Distribuidos

Sondas LAN y WAN

Análisis VoIP

Análisis Rendimiento de Aplicaciones

Gestión de tráfico con NetFlow



Analizadores Portátiles

Analizadores LAN y WiFi

Asistentes de Red

Sofware de análisis y documentación

Comprobadores de Conectividad

¿Cómo obtener la información del tráfico de red… sondas o Netflow?

1. Sondas de Análisis (RMON2, analizadores protocolos)

+ Posibilidad de analizar tiempos de respuesta de aplicaciones
+ Captura y decodificación de tramas
- Necesario desplegar sondas en la red
- Acceso a la red mediante taps o réplica de puerto
- Escalabilidad limitada: dependiente del tipo de interfaz
- Escalablidad limitada: necesario despliegue físico

2. Tecnología NetFlow

+ El propio router o switch informa del tráfico
+ Escalable: independiente del tipo de interfaces
+ Escalable: fácil de añadir más interfaces
- Análisis menos detallados
- Dependiente si la electrónica de red soporta NetFlow

Origen de la tecnología NetFlow

- **Desarrollado por Darren Kerr y Barry Bruins de Cisco Systems en 1996**

- **NetFlow es ahora la tecnología principal de la industria para contabilizar el tráfico de red**

- **NetFlow versión 9 es ahora un estándar de la IETF**

  El grupo de trabajo dentro de la IETF es el IPFIX (Internet Protocol Flow Information eXport)

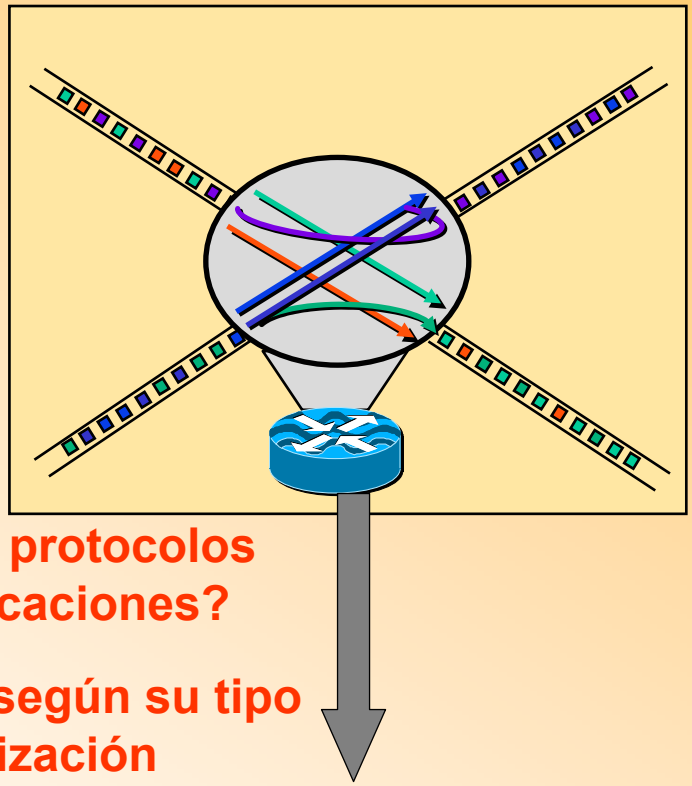
  http:// ipfix.doit.wisc.edu

Versiones NetFlow

NetFlow Version	Comments
1	Original
5	Estándar y el más utilizado
7	Específico de los conmutadores Cisco Catalyst 6500 y 7600 Similar a versión 5 pero no incluye información AS, interfaz, TCP Flag & TOS
8	Hasta 11 esquemas de agregación Reduce los recursos requeridos al sistema
9	Formato de trama flexible y extensible que facilita el soporte de campos de información adcionales (por ejemplo BGP next Hop y MPLS “aware”)

¿Qué datos ofrece NetFlow? (Versión 5)

Ofrece los siguiente campos de información de los flujos de tráfico en la red:



Dirección IP origen
Dirección IP destino
¿Quién habla con quién?

Puerto UDP/TCP origen
Puerto UDP/TCP destino
Tipo de protocolo de nivel 3
¿Qué protocolos y aplicaciones?

TOS byte (Type of Service)
Tráfico según su tipo de priorización

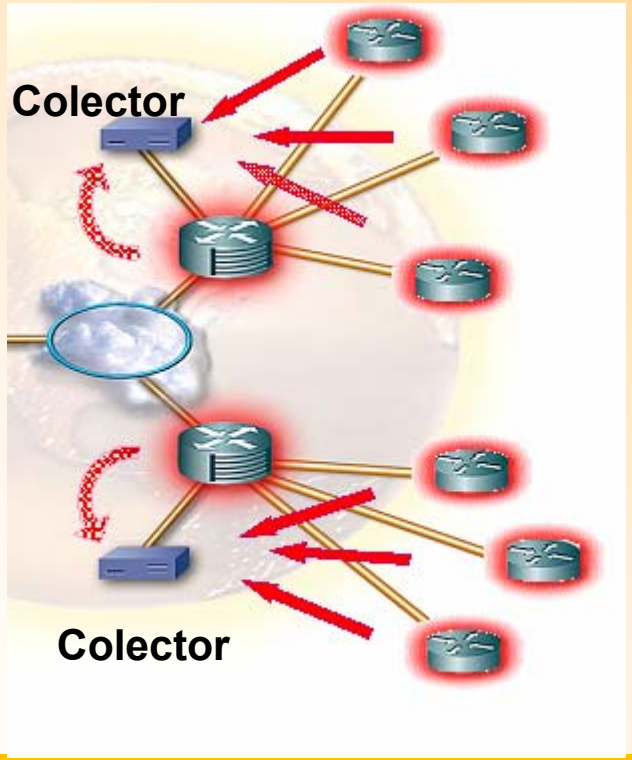
Interfaces lógicos de entrada y de salida (ifIndex)
¿Dónde?

Datos exportados vía paquetes UDP

Flags TCP
¿Ataques DoS?

¿Cómo funciona?

- **Los routers exportan la información de los flujos mediante Netflow a un sistema de colectores.**
- **Las tramas se exportan vía UDP. Las tramas son típicamente de 1500 bytes y cada una contiene información de entre 20 y 50 flujos**

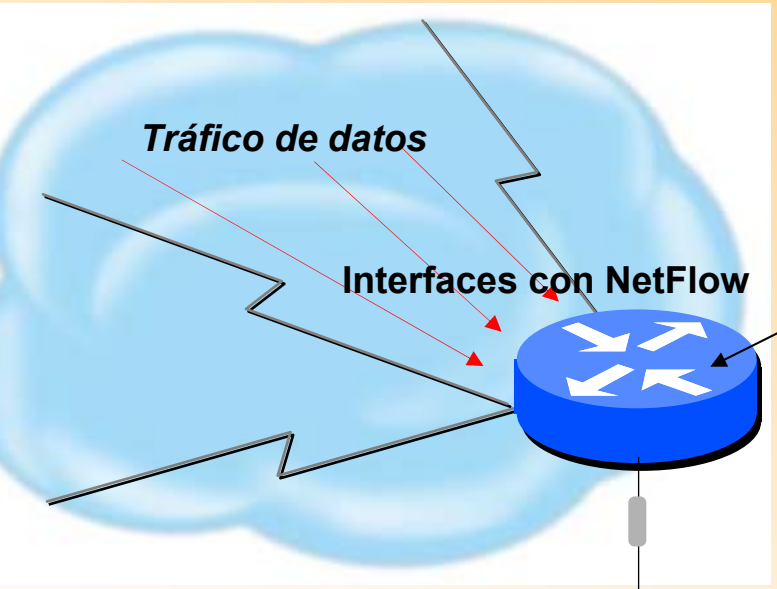


¿Cómo funciona?

Configurar NetFlow en router Cisco:

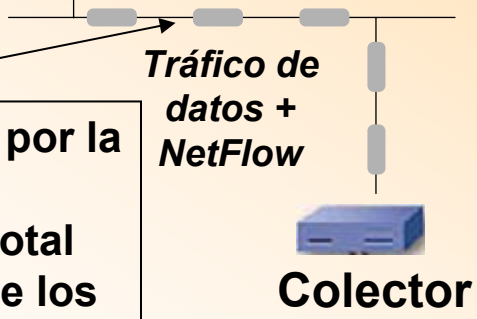
- En la configuración global
  - ip flow-export source loopback
  - ip flow-export version 5
  - ip flow-cache timeout active 1
  - ip flow-export destination [*harvesterIP*] 9995
- Para cada interfaz a monitorizar
  - ip route-cache flow

Impacto de habilitar NetFlow



Número de flujos activos	Utilización adicional de CPU
10,000	<4%
45,000	<12%

Algunos switches disponen de ASICs dedicados a NetFlow por lo que no habría incremento de consumo de CPU



Colector

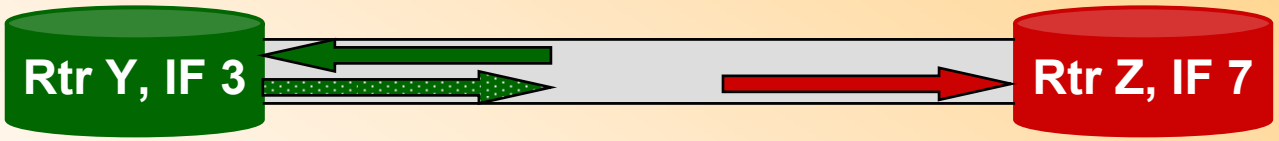
Tráfico adicional generado por la Exportación NetFlow:

- **Aprox. 1,5% del tráfico total real en cada momento de los interfaces monitorizados**

Optimización de recursos

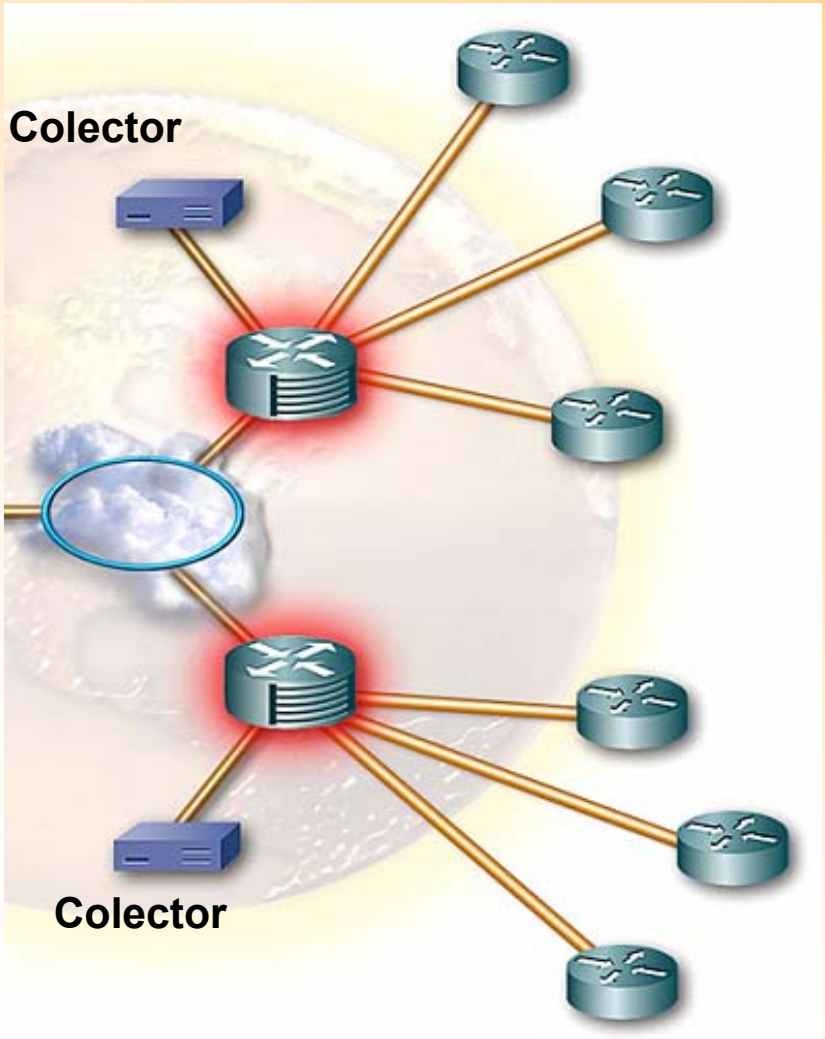
- Sin embargo conocemos el interfaz origen y destino.
- Podemos por lo tanto calcular el tráfico que sale basándonos en una simple regla:

"Todo lo que entre tiene que salir".

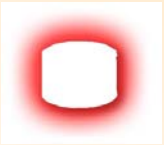


- NetFlow es una tecnología de "ingreso"
- Solamente contabiliza el tráfico que entra en un interfaz
- Para conocer el tráfico total en un enlace por lo tanto tendríamos que habilitar NetFlow en los routers de ambos extremos.

Optimización de recursos: solución ReporterAnalyzer



- Con ReporterAnalyzer de Fluke Networks, NetFlow solamente necesita ser habilitado en los routers centrales
- Debido a ello se elimina tráfico NetFlow innecesario y se simplifica la gestión de los routers



= Router con NetFlow habilitado

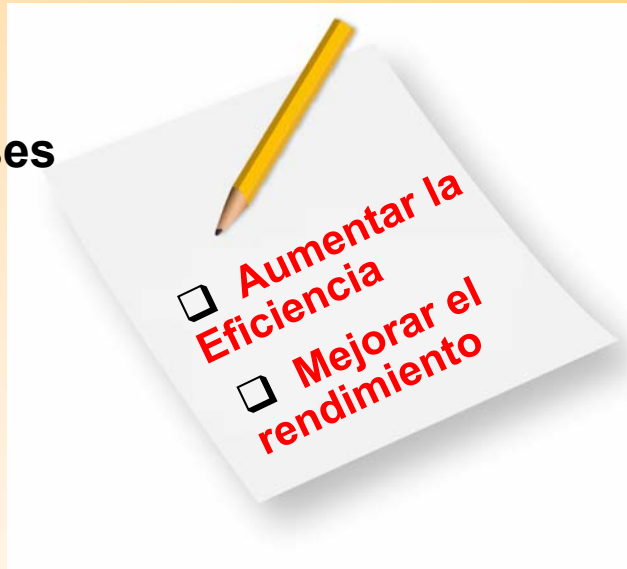
¿Alguna vez…

… le han encargado reducir los costes WAN pero no disponía de la visibilidad global para conseguir el objetivo?

… le han exigido resolver problemas de red en el momento que ocurren?

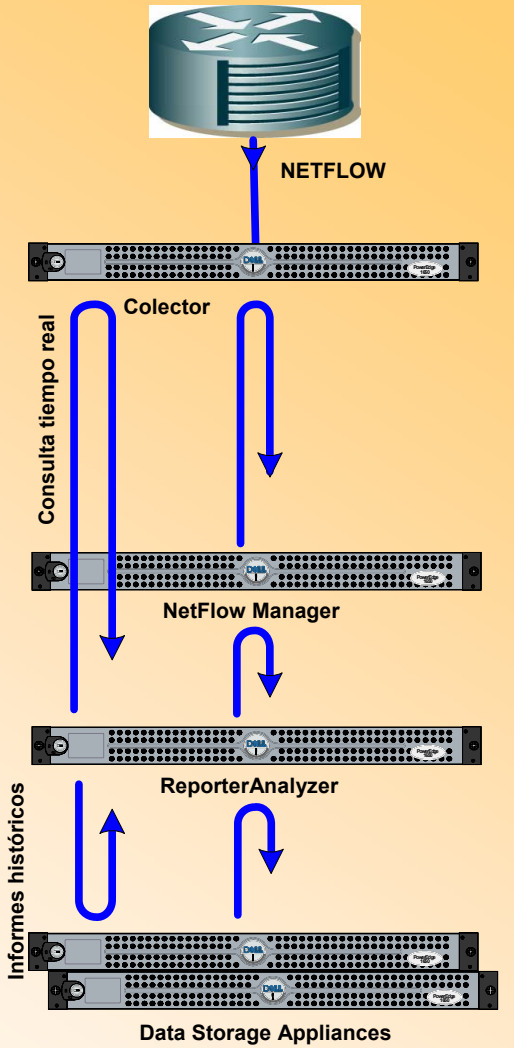
… le han presionado para ampliar el ancho de banda de los enlaces sin saber si esto resolvería el problema?

… ha tenido que identificar rápidamente los viruses y usuarios infectados?



Solución: ReporterAnalyzer

- **Sistema escalable de uno o varios appliances – depende del número de interfaces a monitorizar**
- **Informes en tiempo real e históricos altamante customizables**
- **Alertas SNMP e email**
- **Funcionalidades de análisis forénsico para completar un sistema de seguridad**
- **Instalación en menos de 2 h.**



Solución: ReporterAnalyzer

- **Guarda una extensa cantidad de información – necesario para poder realizar una planificación adecuada basándose en datos históricos.**

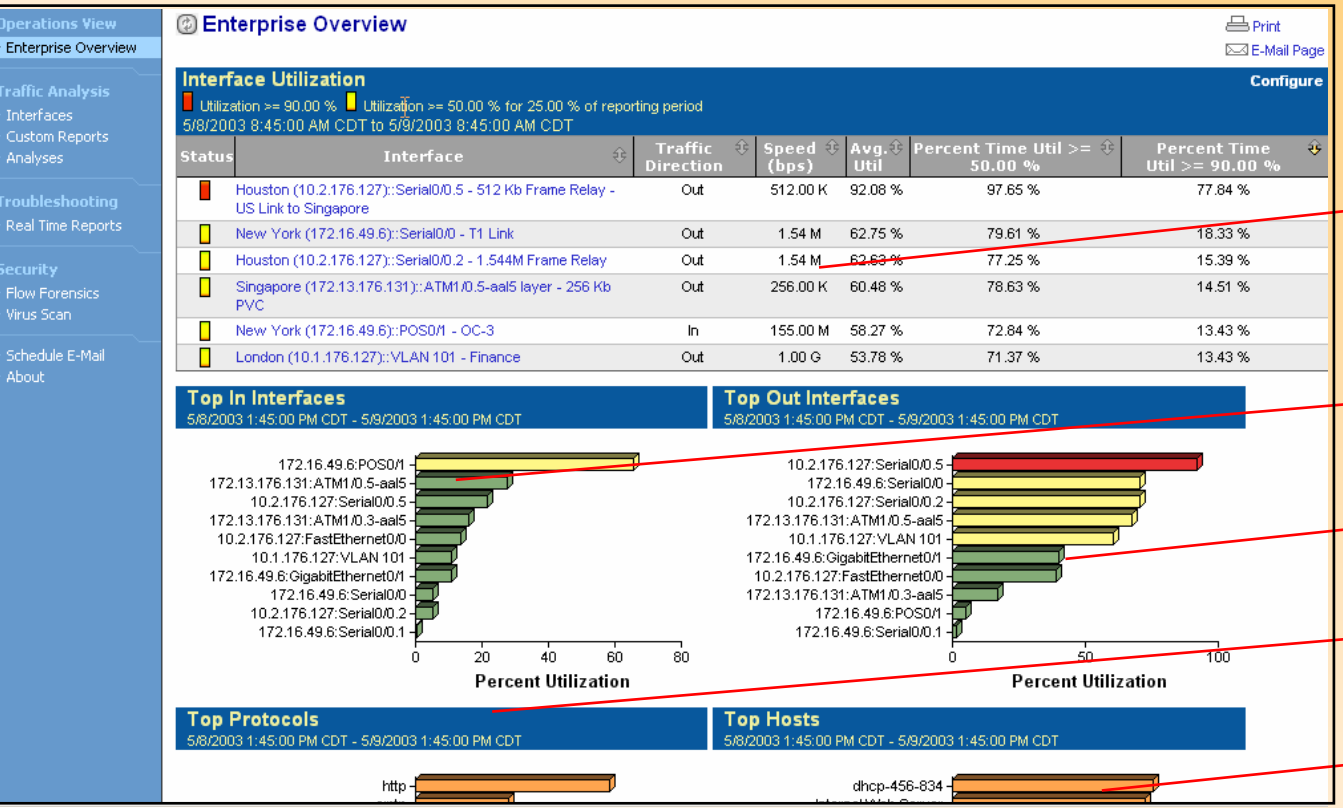
- **“Tiempo real”: En la última hora se dispone de una granularidad de 1 minuto en los datos**

- **Análisis Forénsico: 100% de los protocolos y 100% de los usuarios/conversaciones en las últimas 4 h.**

- **Histórico: información de protocolos hasta 13 meses con 15 min. de resolución.**
  (top 200 protocolos de cada 15 minutos)
  información de conversaciones hasta 2 meses con 15 min. de resolución.
  (top 15 conversaciones para cada uno de los 15 top protocolos + los top 50 conversaciones globales = 275)

- **Cada colector soporta entre 20 y 200 routers (un total de 1 millón de flujos por minuto)**

Interfaz de usuario: Pantalla inicial



Top interfaces por tráfico total

Top interfaces tráfico de entrada

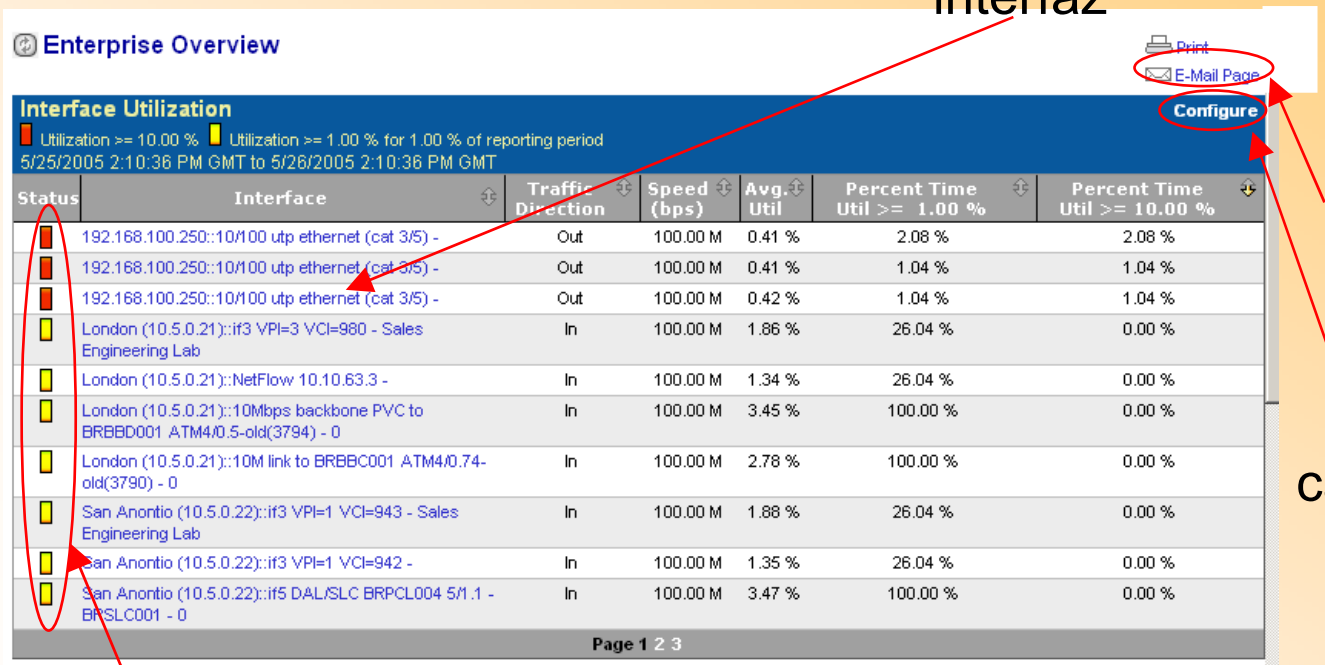
Top interfaces tráfico de salida

Top Protocols

Top usuarios

Interfaz de usuario: Pantalla inicial

clic para información detallada de éste interfaz

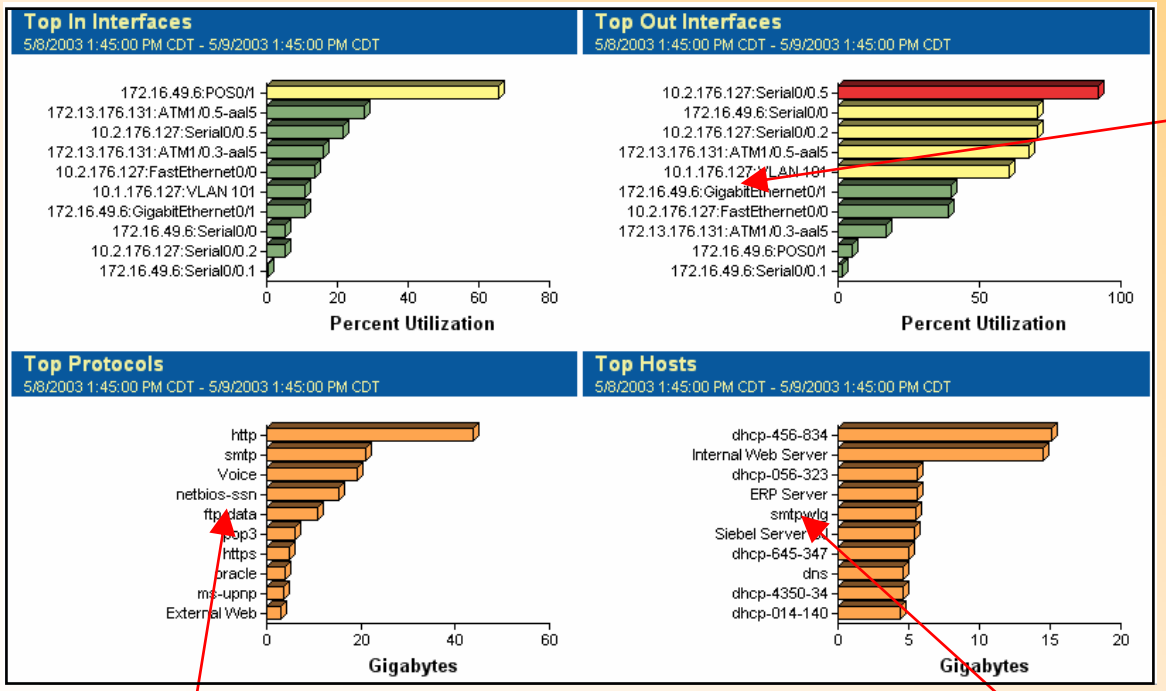


enviar el informe por email

cambiar los umbrales de los indicadores

indicadores de la cantidad de tráfico

Interfaz de usuario: Pantalla inicial



Clic para información detallada de éste interfaz

clic para top interfaces y top usuarios de éste protocolo

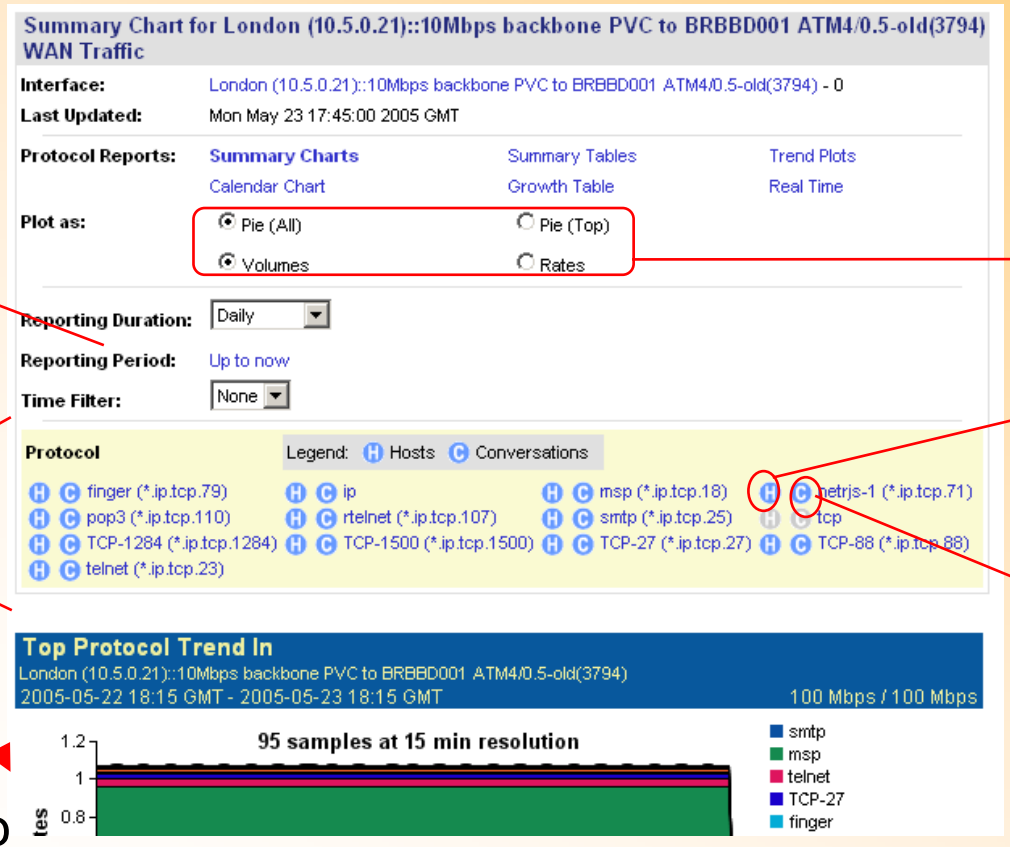
clic para ver los top interfaces y top protocolos para éste usuario

Interfaz de usuario: Información detallada de un interfaz

periodos y filtros de tiempo

Protocolos en éste interfaz

históricos de tráfico por protocolo



Tipo de gráfico

clic para ver hosts o conversaciones

Informes avanzados: Tabla comparativa

¿Por qué éste interfaz muestra menos consumo de ancho de banda?

Growth Table csv /

Protocol	April 17, 2005	April 24, 2005	May 1, 2005	May 8, 2005	May 15, 2005	May 22, 2005	Growth
all	0.00 bps	7.48 Mbps	7.61 Mbps	7.59 Mbps	7.51 Mbps	6.28 Mbps	-3.34%
ip	0.00 bps	7.48 Mbps	7.61 Mbps	7.59 Mbps	7.51 Mbps	6.28 Mbps	-3.34%
tcp (*.ip.6)	0.00 bps	7.42 Mbps	7.54 Mbps	7.56 Mbps	7.51 Mbps	6.28 Mbps	-3.10%
smtp (*.ip.tcp.25)	0.00 bps	3.87 Mbps	3.94 Mbps	3.94 Mbps	3.93 Mbps	3.42 Mbps	-2.32%
msp (*.ip.tcp.18)	0.00 bps	2.89 Mbps	2.02 Mbps	2.15 Mbps	2.87 Mbps	2.27 Mbps	-1.32%
telnet (*.ip.tcp.23)	0.00 bps	172.33 Kbps	175.72 Kbps	175.79 Kbps	175.05 Kbps	155.46 Kbps	-2.00%
TCP-27 (*.ip.tcp.27)	0.00 bps	170.57 Kbps	119.13 Kbps	128.31 Kbps	173.27 Kbps	154.06 Kbps	1.24%
finger (*.ip.tcp.79)	0.00 bps	87.47 Kbps	89.19 Kbps	89.23 Kbps	88.85 Kbps	87.70 Kbps	0.01%
netrjs-1 (*.ip.tcp.71)	0.00 bps	84.86 Kbps	59.27 Kbps	63.84 Kbps	86.20 Kbps	67.52 Kbps	-0.91%
TCP-88 (*.ip.tcp.88)	0.00 bps	82.96 Kbps	83.88 Kbps	85.56 Kbps	85.95 Kbps	66.23 Kbps	-3.78%
pop3 (*.ip.tcp.110)	0.00 bps	51.42 Kbps	35.30 Kbps	74.48 Kbps	92.20 Kbps	46.21 Kbps	9.04%
rtelnet (*.ip.tcp.107)	0.00 bps	8.67 Kbps	6.05 Kbps	6.52 Kbps	8.81 Kbps	7.66 Kbps	0.84%
udp (*.ip.17)	0.00 bps	0.00 bps	0.00 bps	0.00 bps	0.00 bps	0.00 bps	0.00%
rdp (*.ip.27)	0.00 bps	65.89 Kbps	66.40 Kbps	35.37 Kbps	0.00 bps	0.00 bps	-23.16%
UDP-25 (*.ip.udp.25)	0.00 bps	0.00 bps	0.00 bps	0.00 bps	0.00 bps	0.00 bps	0.00%
TCP-4000 (*.ip.tcp.4000)	0.00 bps	0.00 bps	1.01 Mbps	844.43 Kbps	0.00 bps	0.00 bps	-16.63%

Comparación de los últimos 6 meses o 6 semanas

Flow Forensics: Informes de seguridad

ecurity Reports

Application Clients - Which clients are connecting to the specified ports?

Example: Show me any infected hosts using UDP-1434 (port used by SQL Slammer V client-application port with a flow rate above the specified threshold.

Application Servers - Which servers are hosting the specified ports?

Example: Show me any infected hosts using UDP-1434 (port used by SQL Slammer V server-application port with a flow rate above the specified threshold.

Unauthorized Servers - Which unauthorized servers are hosting a specified port?

Example: Specify authorized FTP servers and then look for any unauthorized servers FTP servers.

Peer Count - Who communicates with many other hosts?

Example: Show me any potential worm attacks by identifying hosts attempting to communicate with a large number of other hosts.

Port Count - What hosts are using many ports?

Example: Show me any hosts that may be port scanning.

TCP Resets - What hosts are experiencing a high number of TCP resets?

Example: Show me any hosts that may be under a DoS attack as indicated by a large number of TCP resets.

Conversation Report - What hosts are communicating with other hosts?

Example: Show me any conversation pairs using the specified port(s) above a specified threshold.

Traffic Analysis Reports

- **Server Protocols** - What protocols are active on the specified host(s)?

  Example: Show me all protocols in use on an SMTP server.
- **Network Protocols** - Which protocols are active on the network?

  Example: Show me the traffic volume for all of my enterprise network applications.
- **Host Access** - Who is accessing the specified host?

  Example: Show me any hosts that are communicating with my proxy servers.
- **Server Volume** - What is the total volume of traffic to/from a specified host?

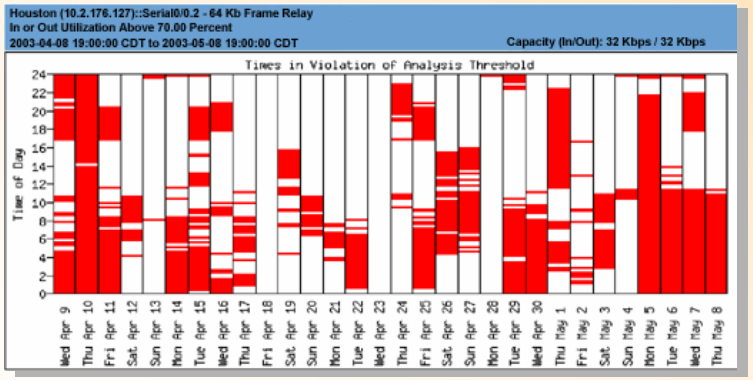
  Example: Show me the traffic volume for each of my DNS servers

Ejemplos de análisis

¿Qué interfaces han soportado un tráfico NetBIOS de más de un 70% en el último mes en horario laboral?

Interface Name	Time over Threshold	Total Time	Percent Time over Threshold	Average Rate In (bps)	Average Rate Out (bps)	Maximum Rate In* (bps)	Maximum Rate Out* (bps)	Longest Violation
Houston (10.2.176.127)::Serial0/0.2	10.72 days	30.00 days	36%	6.86 K	18.26 K	60.37 K	128.75 K	22.00 hrs
London (10.1.176.127)::Serial0/0.4	1.55 days	30.00 days	5%	10.48 K	7.18 K	120.33 K	118.08 K	3.25 hrs
Singapore (172.13.176.131)::ATM1/0.3-aal5 layer	8.50 hrs	30.00 days	1%	1.05 K	4.25 K	40.66 K	65.74 K	1.50 hrs
New York (172.16.49.6)::Serial0/0.1	7.50 hrs	30.00 days	1%	122.34	1.83 K	12.80 K	291.19 K	1.50 hrs
Houston (10.2.176.127)::Serial0/0.4	6.25 hrs	30.00 days	1%	6.34 K	7.63 K	159.01 K	107.69 K	2.50 hrs
London (10.1.176.127)::Serial0/0.3	2.50 hrs	30.00 days	0%	1.48 K	3.27 K	40.48 K	59.56 K	30.00 mins
Houston (10.2.176.127)::Serial0/0.1	2.00 hrs	30.00 days	0%	223.13	199.30	14.77 K	5.48 K	1.00 hrs
Houston (10.2.176.127)::Serial0/0.3	1.00 hrs	30.00 days	0%	2.26 K	3.74 K	47.28 K	61.33 K	30.00 mins

¿Cuándo ha ocurrido y cuánto ha durado?



Algunos clientes referencia

Caso práctico: Planificación de ancho de banda

Caso real ocurrido en un cliente:

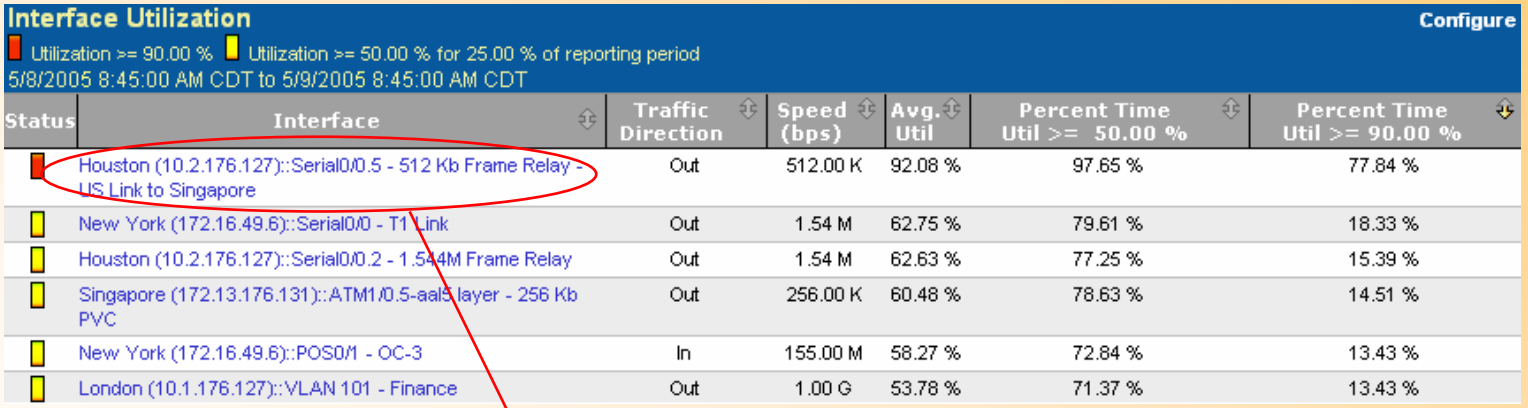
Las aplicaciones a través de un enlace transoceánico experimentan una rendimiento muy bajo.

Las estadísticas SNMP del router muestran un tráfico muy elevado

Se propone un incremento de ancho de banda con un coste adicional de €120.000 al año

Caso práctico: Planificación de ancho de banda

Desde la pantalla inicial confirmamos que el enlace en cuestión (Houston a Singapore) presenta un 90% de consumo de ancho de banda.



Interface Utilization — Configure

Utilization >= 90.00 % | Utilization >= 50.00 % for 25.00 % of reporting period

5/8/2005 8:45:00 AM CDT to 5/9/2005 8:45:00 AM CDT

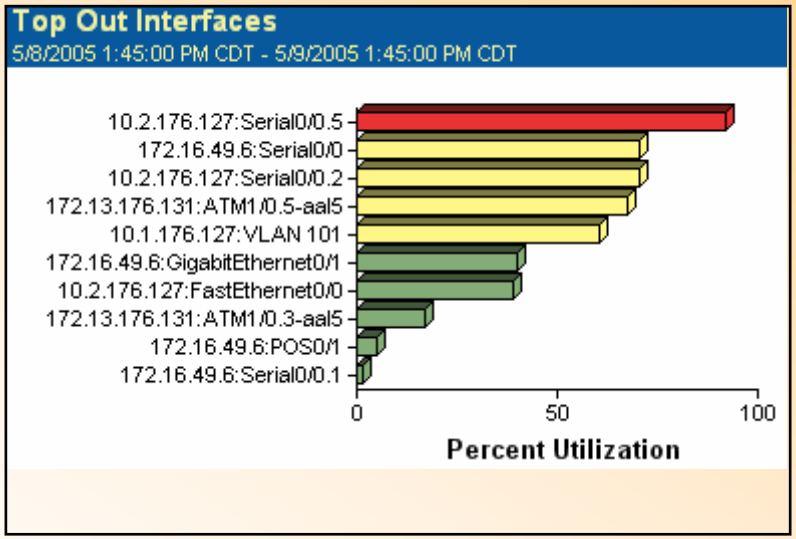
Status	Interface	Traffic Direction	Speed (bps)	Avg. Util	Percent Time Util >= 50.00 %	Percent Time Util >= 90.00 %
	Houston (10.2.176.127)::Serial0/0.5 - 512 Kb Frame Relay - US Link to Singapore	Out	512.00 K	92.08 %	97.65 %	77.84 %
	New York (172.16.49.6)::Serial0/0 - T1 Link	Out	1.54 M	62.75 %	79.61 %	18.33 %
	Houston (10.2.176.127)::Serial0/0.2 - 1.544M Frame Relay	Out	1.54 M	62.63 %	77.25 %	15.39 %
	Singapore (172.13.176.131)::ATM1/0.5-aal5 layer - 256 Kb PVC	Out	256.00 K	60.48 %	78.63 %	14.51 %
	New York (172.16.49.6)::POS0/1 - OC-3	In	155.00 M	58.27 %	72.84 %	13.43 %
	London (10.1.176.127)::VLAN 101 - Finance	Out	1.00 G	53.78 %	71.37 %	13.43 %

clic para ver detalles del interfaz

Caso práctico: Planificación de ancho de banda

Éste enlace está en la lista de los top interfaces con más tráfico.

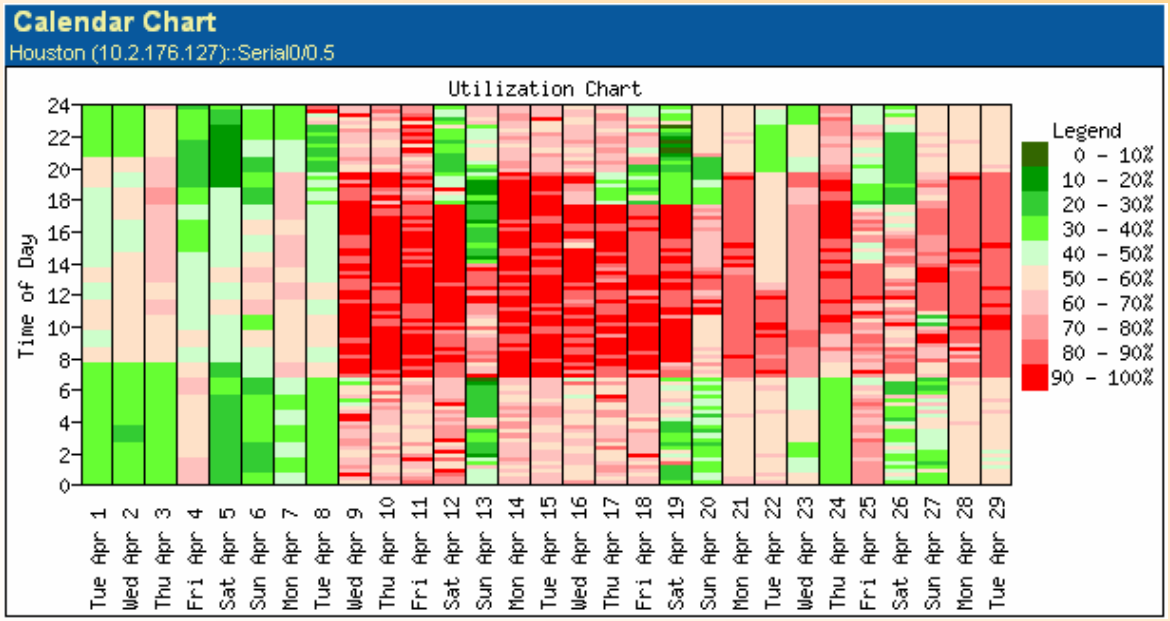
Clic para ver un gráfico de calendario con los consumos de ancho de banda.



Caso práctico: Planificación de ancho de banda

El gráfico calendario muestra que el excesivo consumo de ancho de banda comenzó el 8 de Abril y ha continuado así desde entonces.

Clic para más detalles.

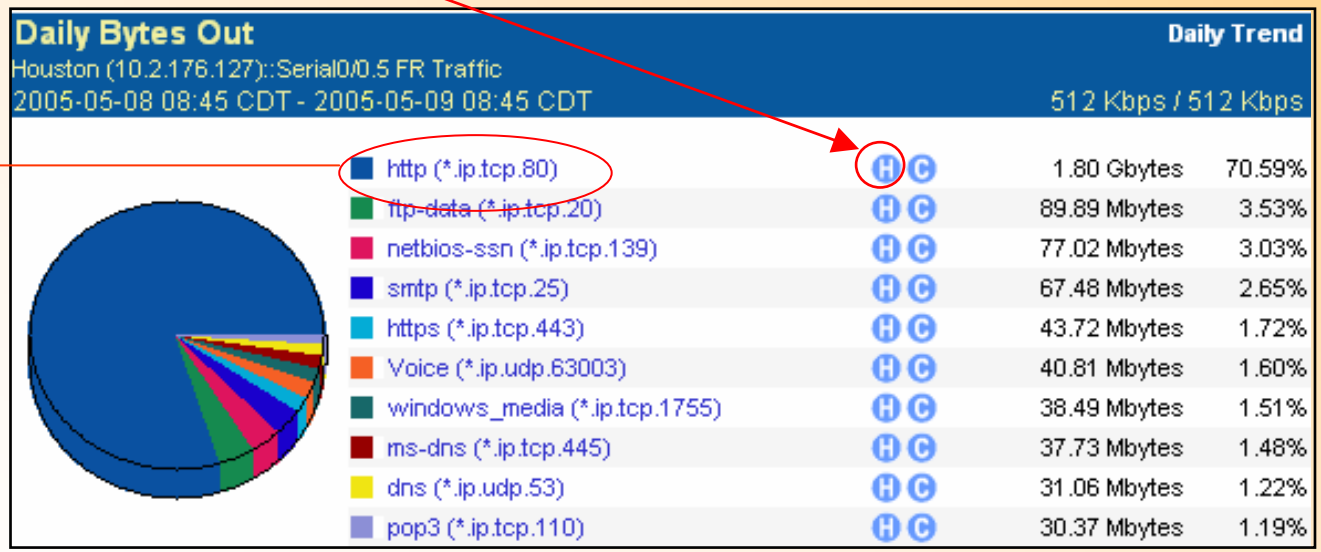


Caso práctico: Planificación de ancho de banda

La distribución de protocolos muestra que el 70% del tráfico es HTTP.

Clic en H para ver los usuarios de éste protocolo.

osibilidad e mejora

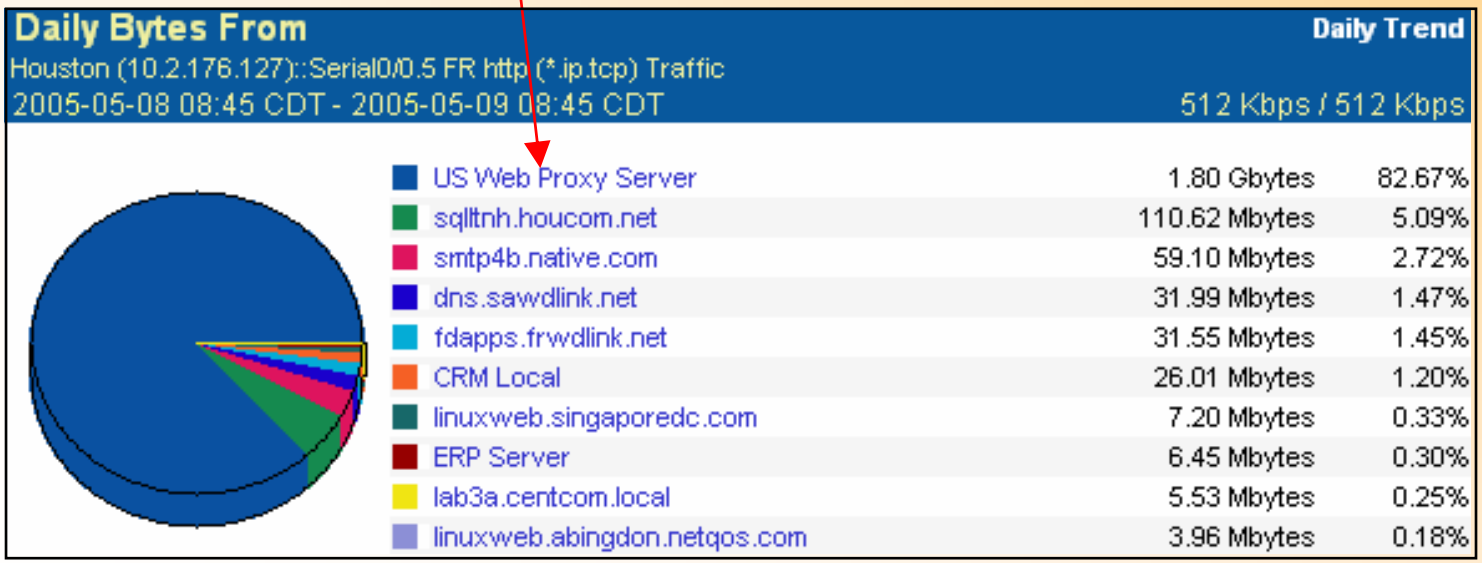


Caso práctico: Planificación de ancho de banda

El servidor proxy "US Web Proxy Server" es el dispositivo que más tráfico HTTP recibe/genera en el enlace a Singapur.

Esto no debería ser así pues los empleados en Asia tienen su propia salida a Internet.

Conclusión: alguién modificó la configuración proxy en los exploradores web para tener un acceso a Internet más rápido.



Caso práctico: Planificación de ancho de banda

El problema se pudo resolver en unos pocos minutos.

En este ejemplo real ReporterAnalyzer ahorró en un único incidente €120.000.

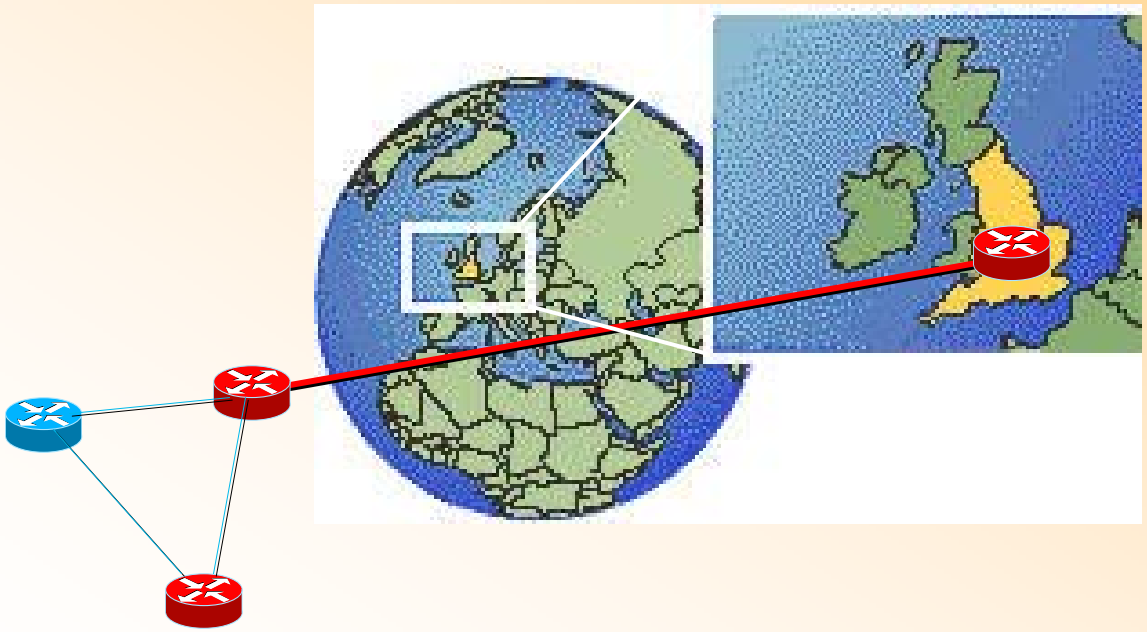
Además ayudó a prevenir futuros incidentes de éste tipo al sentirse los usuarios advertidos y saber que el departamento de comunicaciones puede conocer el tráfico en la red.

Case Study: Traffic Analysis

Caso práctico: Detección de virus

Caso real ocurrido en un cliente:

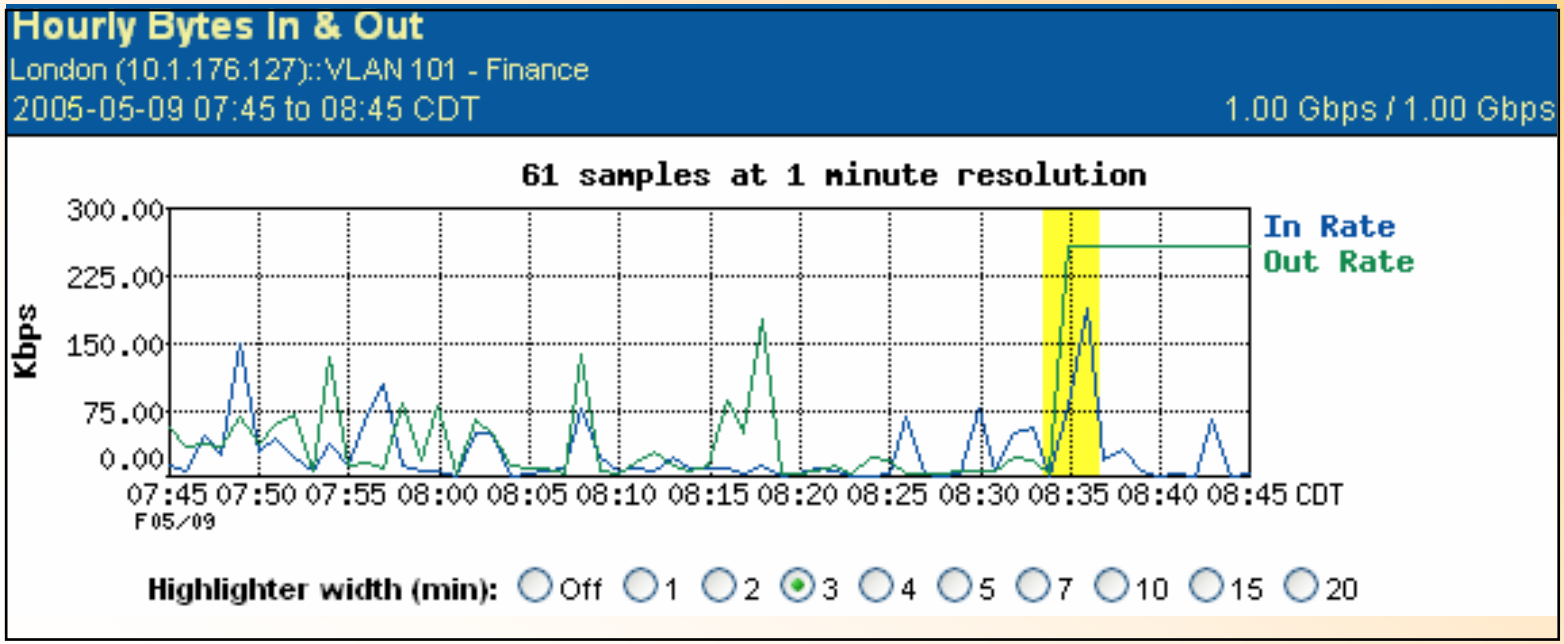
Los usuarios de repente empiezan a quejarse de que no pueden acceder a la red y a sus aplicaciones críticas de negocio ubicadas en un CPD en Londres.



Caso práctico: Detección de virus

Seleccionamos los informes en tiempo real y visualizamos en enlace Con Londres.

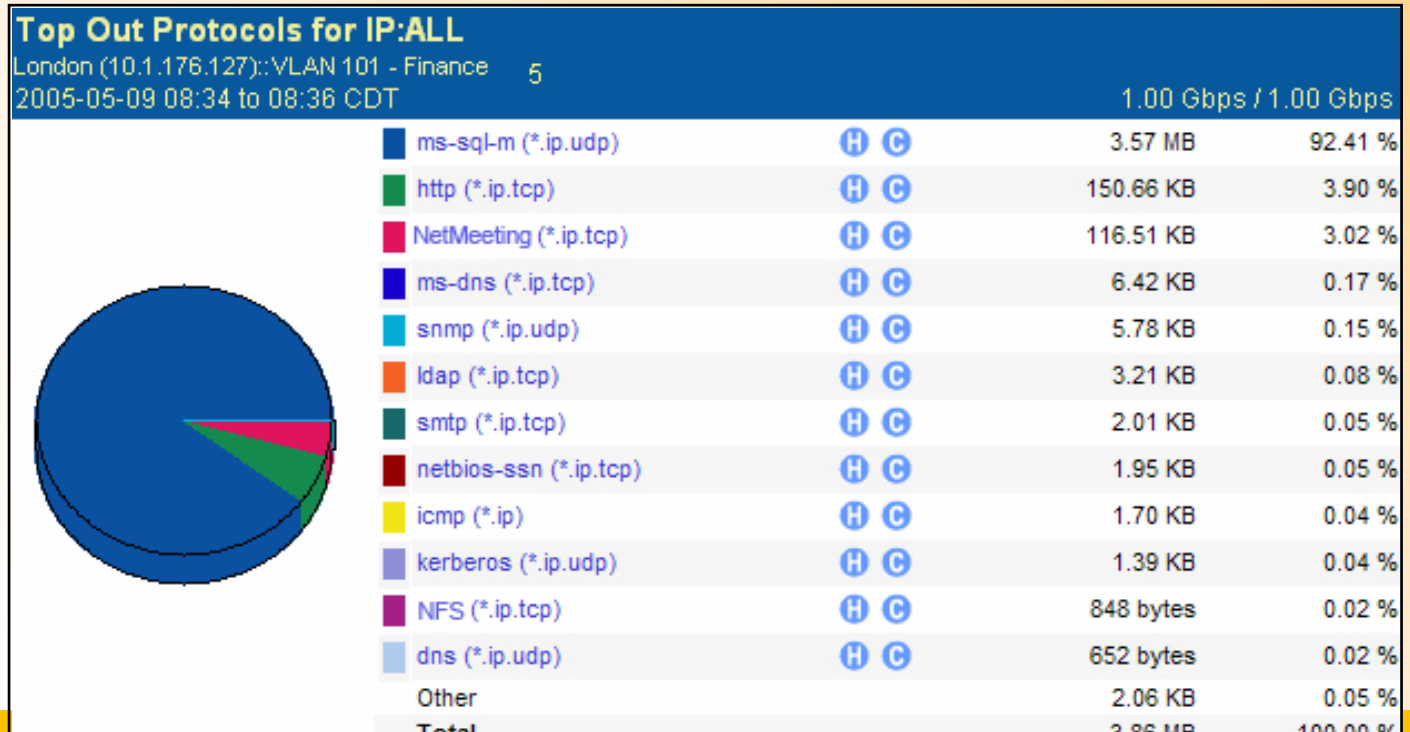
Detectamos un incremento drástico de ancho de banda hace apenas 10 minutos - > Clic para más detalles.



Caso práctico: Detección de virus

Durante el intervalo de 3 minutos seleccionado el protocolo principal causante del tráfico fué ms-sql-m, originando un 92% del consumo.

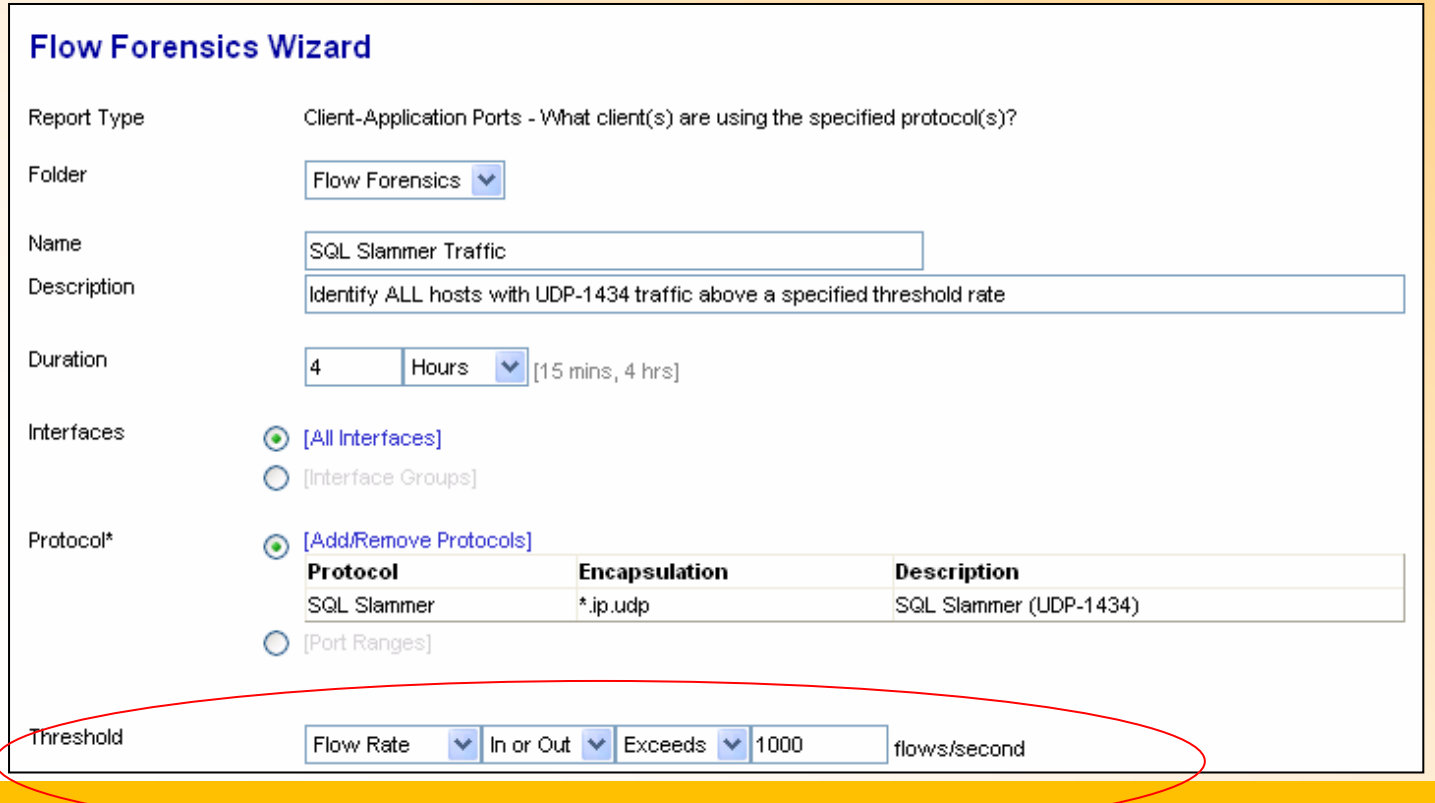
Una rápida búsqueda en la web nos informa que el protocolo en realidad es un virus, el SQL Slammer virus.



Caso práctico: Detección de virus

Detectada la razón de los problemas debemos ahora identificar los usuarios infectados.

Utilizamos las herramientas Flow Forensics de ReporterAnalyzer para generar un informe con los infectados.



Caso práctico: Detección de virus

El informe nos muestra todos los usuarios que en las últimas 4 h han generado tráfico ms-sql-m con una tasa anormalmente alta.

SQL Slammer Hosts

Show all SQL Slammer Hosts that have been active for the last 4 hours

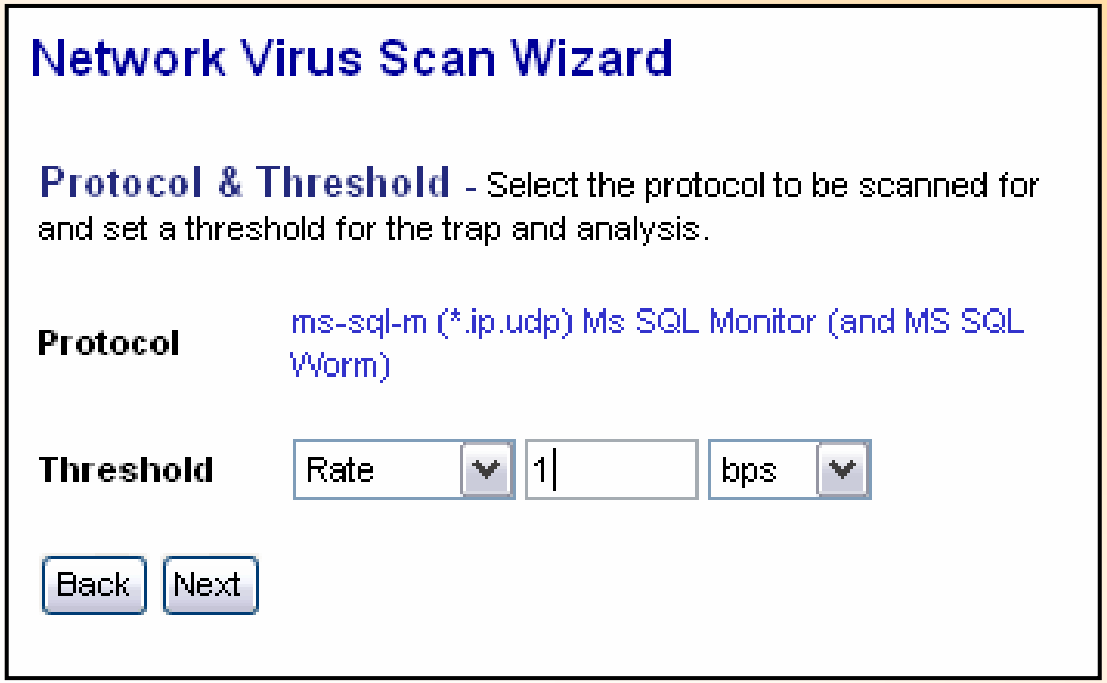
2005-05-09 03:45:00 CDT to 2005-05-09 07:45:00 CDT

Client	Client Name	Flows In	Flows Out	Flows Total	Bytes In	Bytes Out	Bytes Total	Packets In	Packets Out	Packets Total
72.14.226.5	appsql04.houcentlb.com	7.30 K	119.17 K	126.46 K	230.00 K	3.81 M	4.04 M	38.66 K	638.34 K	676.99 K
72.11.160.226	abcsql01.houcentlb.com	3.71 K	113.54 K	117.25 K	115.00 K	3.63 M	3.75 M	19.33 K	608.26 K	627.58 K
72.14.226.32	nqsql02.houcentlb.com	2.43 K	108.16 K	110.59 K	76.67 K	3.46 M	3.54 M	12.93 K	579.71 K	592.64 K
72.12.113.47	nqsql05.houcentlb.com	1.92 K	102.91 K	104.83 K	57.50 K	3.29 M	3.35 M	9.73 K	551.30 K	561.02 K
72.12.113.198	appsql11.houcentlb.com	1.54 K	97.54 K	99.07 K	46.00 K	3.12 M	3.17 M	7.81 K	522.75 K	530.56 K

Caso práctico: Detección de virus

Para prevenir próximas infecciones y vigilar la posible propagación de este virus se programa una alerta.

Recibiremos un trap SNMP de forma automática cuando se detecte de nuevo un exceso de tráfico de éste protocolo.



Caso práctico: Detección de virus

Utilizando la información en tiempo real se pudo detectar la causa del problema, identificándolo como un virus.

Se localizaron los usuarios infectados para aislarlos y eliminar el virus. Además se programó una alerta para avisar de próximas infecciones.

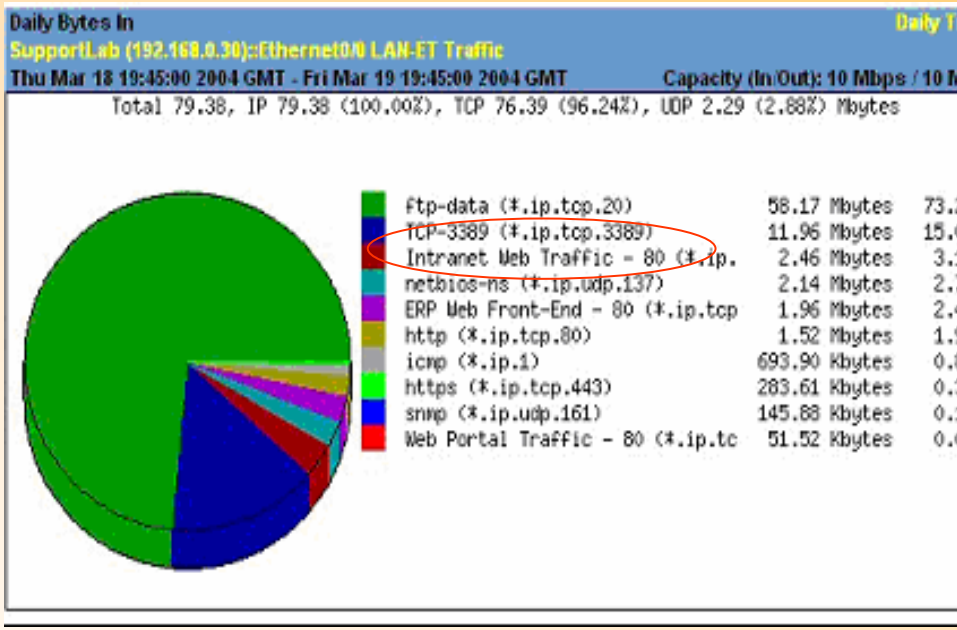
ReporterAnalyzer permitió una rápida resolución del problema, previniendo una posible perdida de datos y de productividad de los empleados.

¡Un poco de customización ofrece nuevas posibilidades! (1)

Un poco de customización permite mejorar la representación de los datos.

A menudo aplicaciones como web tienen diversos usos dependiendo a donde vayan.

Por ejemplo si salen a Internet o van al proxy lo lógico es poner "Internet Web" como descripción. Sin embargo si va a la Intranet, lo lógico sería utilizar "Internet". Finalmente si fuese el interfaz de usuario de una aplicación de negocio lo más útil sería ponerle ese nombre.



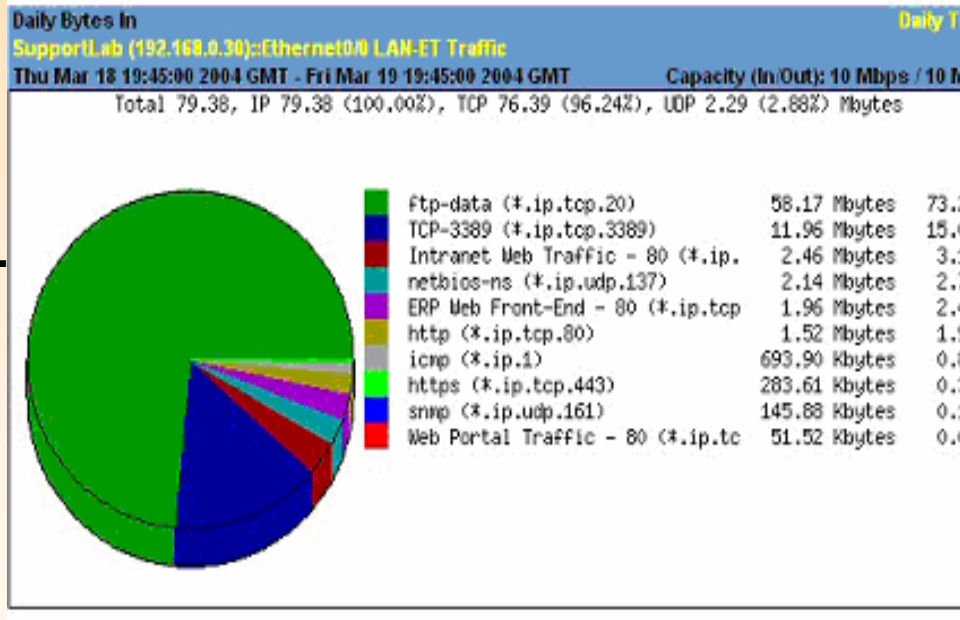
De ésta forma aparecerán como aplicaciones separadas y será más fácil identificarlas.

¡Un poco de customización ofrece nuevas posibilidades! (2)

Algunas aplicaciones no utilizan todo un rango de puertos customizados. Estos puertos incluso podrían ser utilizados por otra aplicación en otro servidor para otros usos.

Podemos mapear el tráfico hacia un servidor a una descripción que elijamos.

De esta forma será sencillo identificar el tráfico y tendremos los diferentes protocolos bajo la misma descripción.

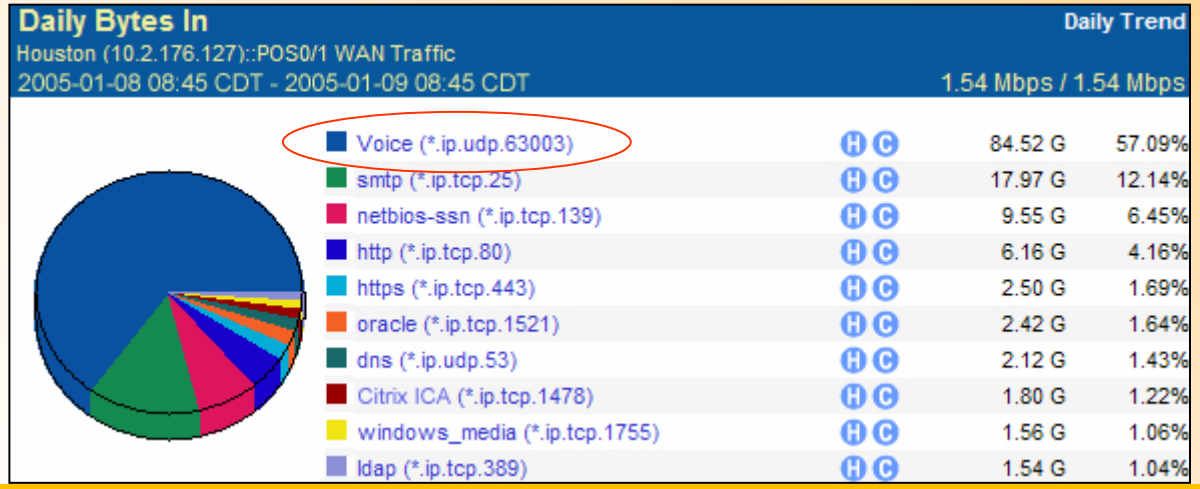


¡Un poco de customización ofrece nuevas posibilidades! (3)

Otras aplicaciones como VoIP no utilizan a menudo unos puertos UDP predeterminados. Pueden utilizar prácticamente cualquier puerto.

En este caso podemos utilizar la información de priorización (TOS – Type of Service) para mapear la aplicación a una descripción.

VoIP suele priorizarse y tiene por lo tanto un TOS diferente con lo que resulta sencilla esta operación.



¿Preguntas?

Les enviaremos por correo el enlace donde podrá descargar esta web.

Demostración real del ReporterAnalyzer

Gracias por participar en este seminario

Le enviaremos por email el sitio donde podrá descargar la presentación

Por favor, no se olviden de rellenar las encuestas

FLUKE networks