TELCO MANAGER

TRAF$_{ip}$

DESCRITIVO TÉCNICO

Telcomanager é uma empresa especializada no desenvolvimento de ferramentas de análise de tráfego e gerenciamento de rede.

Os produtos da **Telcomanager** destacam-se pela tecnologia utilizada, suas funcionalidades amigáveis e, principalmente, por sua eficiência. Por isso, tem atingido sucesso em empresas representativas de vários segmentos do mercado, tais como operadoras de telecomunicações, lojas de varejo, bancos, empresas de logística, indústrias de base e provedores de conteúdo, dentre muitos outros.

Sempre que uma rede for parte importante do dia-a-dia, os produtos **Telcomanager** farão a diferença.

Não há dúvida de que o ambiente de rede está cada vez mais complexo e que sua gestão é um grande desafio. Nesse cenário, saber o que está passando por esta importante infraestrutura é um ponto crítico para qualquer administrador de rede.

O TRAFip é uma poderosa ferramenta de coleta e caracterização de tráfego de rede IP, que vem resolver este problema de forma definitiva.

Através da coleta de dados, via protocolo NetFlow (ou equivalente), o TRAFip oferece uma completa visualização do tráfego da sua rede. Permite identificar cada pacote e associá-lo a usuários, aplicações, servidores, workstations, protocolos ou diversos outros critérios à sua escolha.

Com as informações fornecidas pelo TRAFip você consegue respostas para fazer o correto diagnóstico de problemas que podem estar afetando sua rede, além de entender e clarificar o uso que cada área da empresa faz da rede.

Por que usar?

Tráfego alta sem justificativa

O TRAFip consegue identificar facilmente qual o usuário e a aplicação que estão gerando determinado tráfego na sua rede, apontando inclusive o site e o servidor usados.

Aplicações não homologadas

Com o TRAFip é possível verificar se existe alguma aplicação que não foi homologada gerando tráfego na rede.

Classes de serviço configuradas corretamente

Saber se somente as aplicações planejadas estão usando determinada classe de serviço é fundamental para qualquer gestor de rede. Com o TRAFip, é possível identificar todas as aplicações que estão usando as classes de serviços configuradas na rede.

Localidades que mais consomem recursos da rede

O TRAFip permite visualizar quais as localidades, regiões ou departamentos demandam mais recursos da rede ou do datacenter. Essa informação é fundamental quando se deseja fazer algum tipo de rateio de custo.

Aplicações que mais consomem recursos da rede

O TRAFip pode ser usado para visualizar quais as aplicações que mais consomem recursos da rede. E isso pode ser de extrema importância para planejamentos de mudanças de serviços para “Cloud Computing”, por exemplo.

Solução Appliance

O TRAFip é um appliance, com hardware e software perfeitamente integrados. Uma solução confiável e robusta, com baixo custo de instalação e manutenção.

Não há necessidade de instalação e otimização do sistema operacional, instalação de softwares, risco de vírus, falta de memória, instalação de banco de dados e muito menos ter que se preocupar com a manutenção de todos esses componentes.

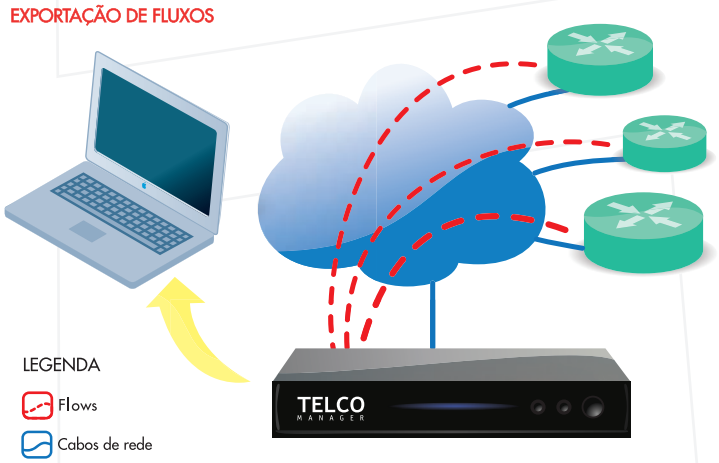
Mecanismo de Coleta

Para realizar seu trabalho, o TRAFip precisa capturar informações sobre o tráfego. A forma mais eficiente de fazer isso é utilizando uma tecnologia baseada em exportação de fluxos.

Essa tecnologia está disponível na maioria das plataformas de nível 3 e em muitas de nível 2 presentes no mercado, variando o nome de acordo com o fabricante (Cisco Netflow, Juniper JFlow, Huawei Netstream, etc).

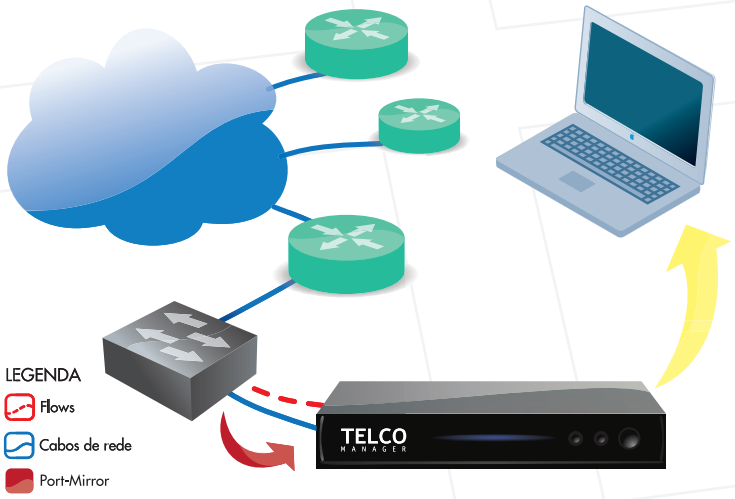
Utilizando a tecnologia de exportação de fluxo, informações relativas ao tráfego são passadas ao TRAFip, que então as analisa. O resultado desta análise é uma classificação deste tráfego por diversos parâmetros, como por exemplo: origem do tráfego, destino do tráfego, aplicação em uso, ASs de origem e destino e muitas outras.

Uma vez com o tráfego identificado, torna-se fácil saber como, quando e quem está consumindo a banda de sua rede.



Mesmo quando não há a tecnologia de fluxo disponível, o TRAFip, através de um switch com port-mirror ou mesmo através de uma porta de HUB, é capaz de realizar suas análises. Neste caso, deve-se ligar o appliance diretamente em um ponto da rede onde ele possa ter acesso direto ao tráfego a ser analisado.

PORT - MIRROR

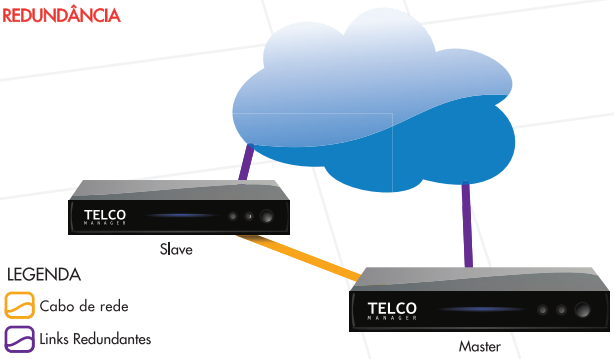


Redundância

Quando o monitoramento é considerado de missão crítica e não pode ser interrompido, a Telcomanager oferece uma opção de ativar dois appliances em redundância. Neste modo de operação, ambos os aparelhos se mantêm sincronizados tanto nas suas configurações definidas quanto com relação aos dados coletados e análises realizadas.

A redundância Telcomanager opera sob um regime hot-standby, não havendo necessidade de intervenção humana. Quando um dos equipamentos para de operar, o outro assume todas as funções automaticamente.

REDUNDÂNCIA



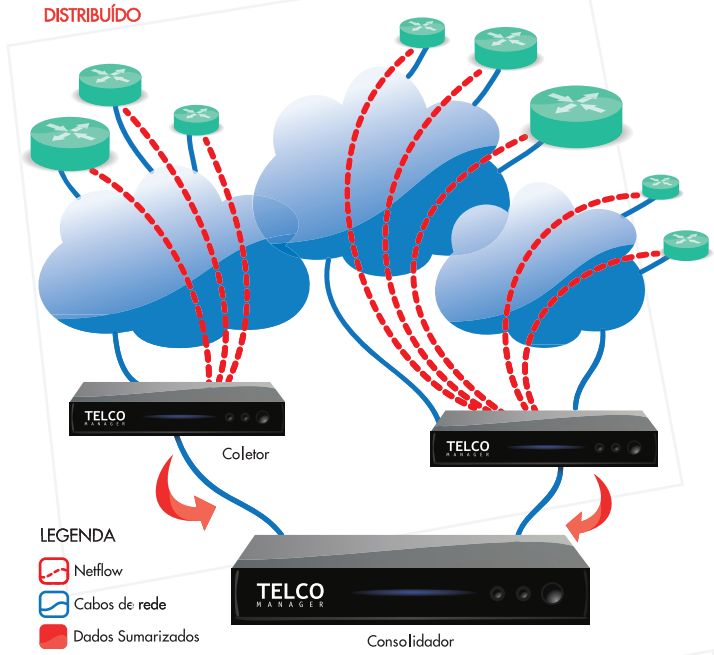
Arquitetura Escalável

O TRAFip pode ser configurado para trabalhar com diferentes tamanhos de rede. A Telcomanager dispõe de appliances com capacidade para monitorar redes com mais de 1000 dispositivos, bem como appliances de pequena capacidade, com custo efetivo, focados em redes com poucos dispositivos.

Utilizando-se um cluster de coletores e pré-processadores de tráfego, que enviam as informações coletadas e tratadas para um consolidador central, pode-se expandir a capacidade da instalação para, virtualmente, qualquer tamanho de rede. Atualmente, existem em operação casos de redes com mais de 10000 dispositivos sendo monitorados por uma plataforma composta de menos de 10 appliances, incluindo-se appliances específicos para redundância.

Os coletores da Telcomanager não são simples coletores e repassadores de informação. Eles realizam o processamento de boa parte desses dados, de forma que a adição de novos coletores não expande apenas a capacidade de coleta, mas também a performance geral do sistema.

DISTRIBUÍDO



Segurança, Autenticação e Autorização

O TRAFip utiliza um modelo clássico de usuário/senha para o controle de acesso. Este sistema pode usar senhas armazenadas no próprio appliance ou integrar com um servidor externo de autenticação Tacacs ou Active Directory.

Pode-se configurar no TRAFip o uso do protocolo HTTPS para um maior grau de confidencialidade e segurança.

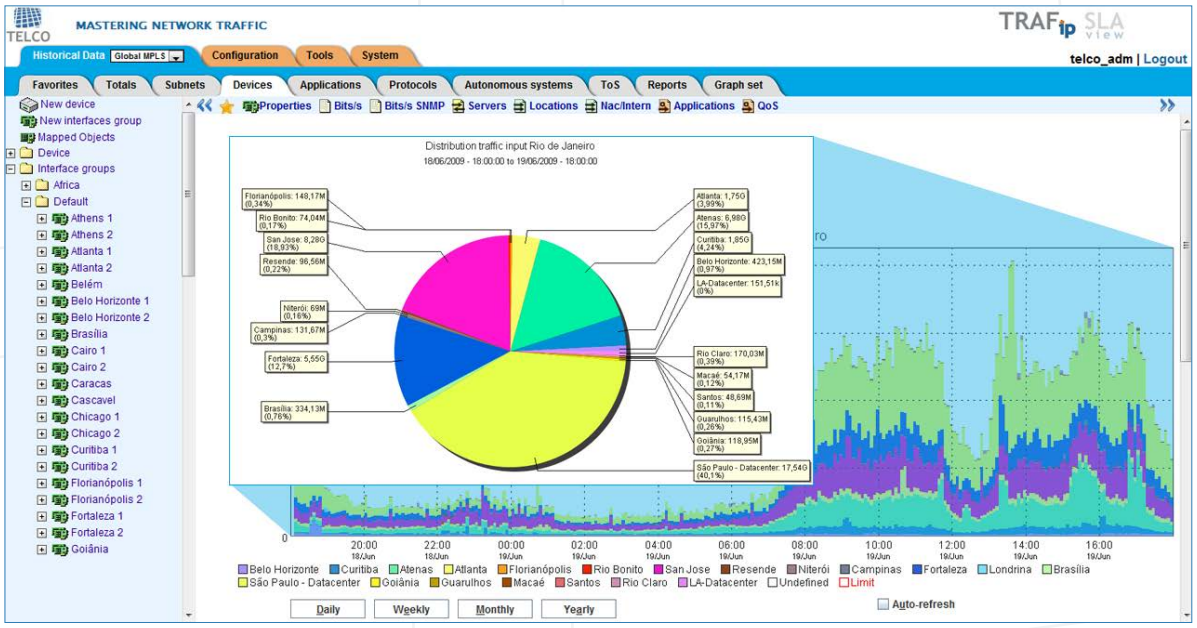
Interface WEB

As funcionalidades do sistema estão reunidas em uma interface WEB, que possibilita rápida navegação através do sistema de abas e menus.

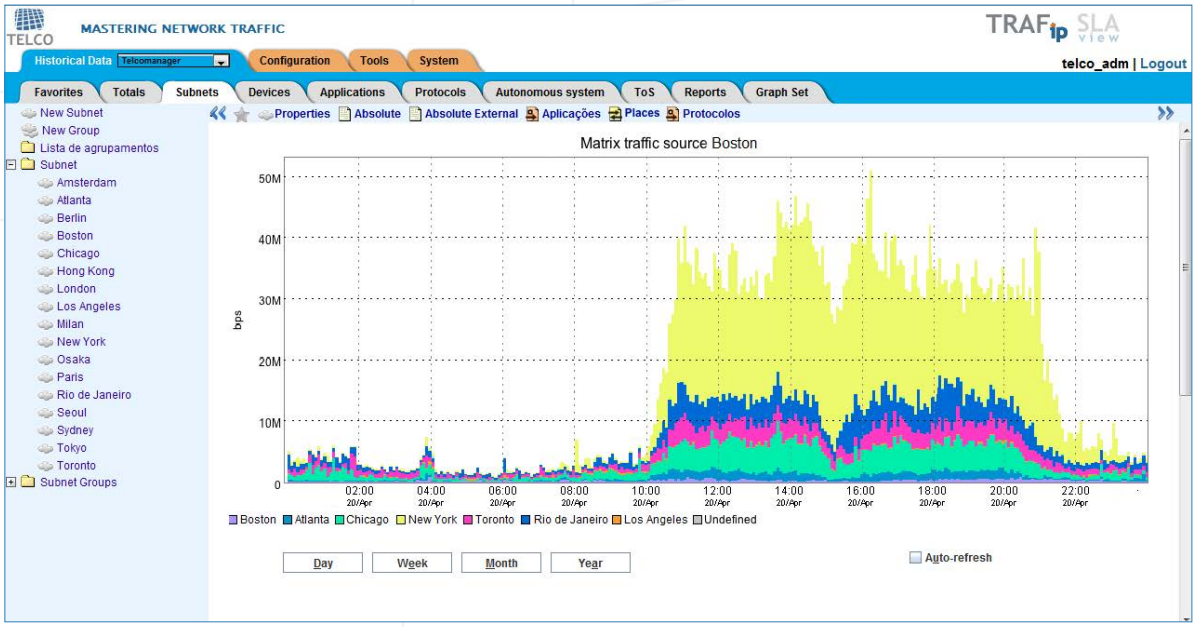
A interface WEB facilita a requisição e coleta de informações para o gerenciamento autônomo da rede, com o uso de recursos em HTML, Java Scriot e Applet Java para gerar gráficos e relatórios.

Existem diversas formas de visualizar e analisar os dados dos dispositivos cadastrados no sistema. Em poucos cliques, gráficos e relatórios personalizados são disponibilizados.

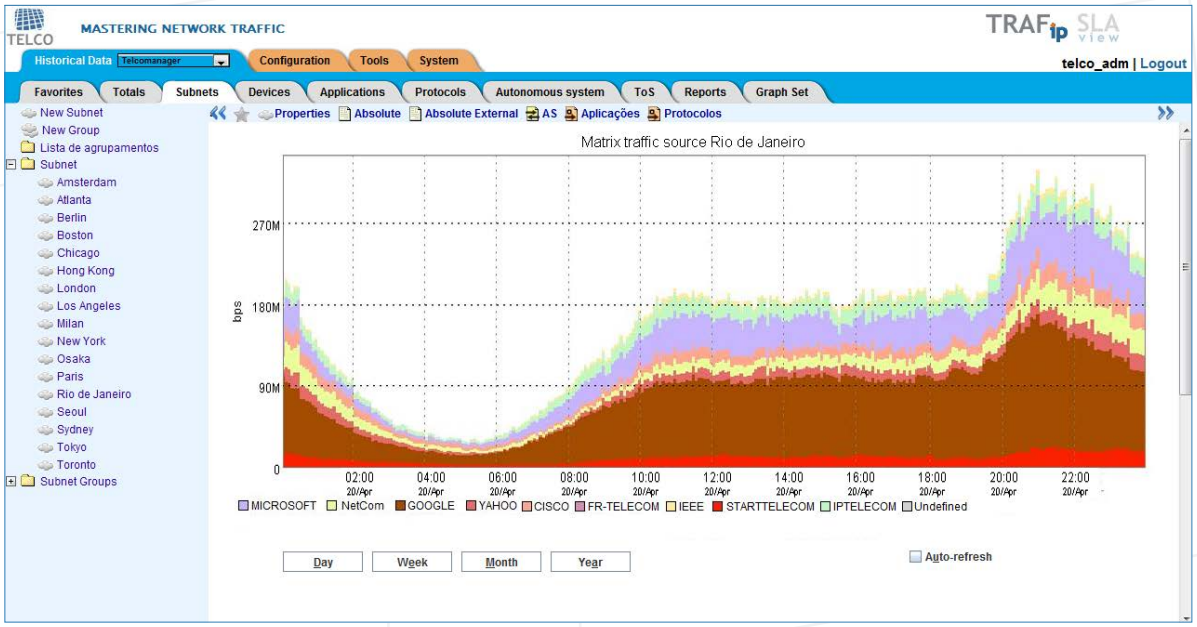
Link x Localidade



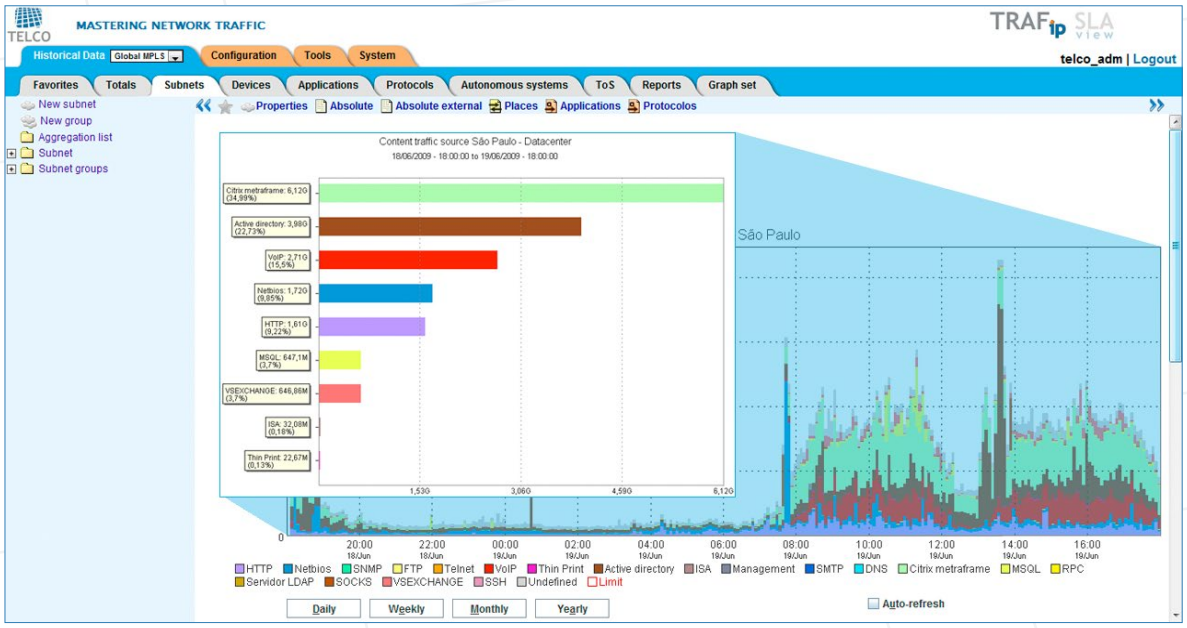
Localidade x Localidade



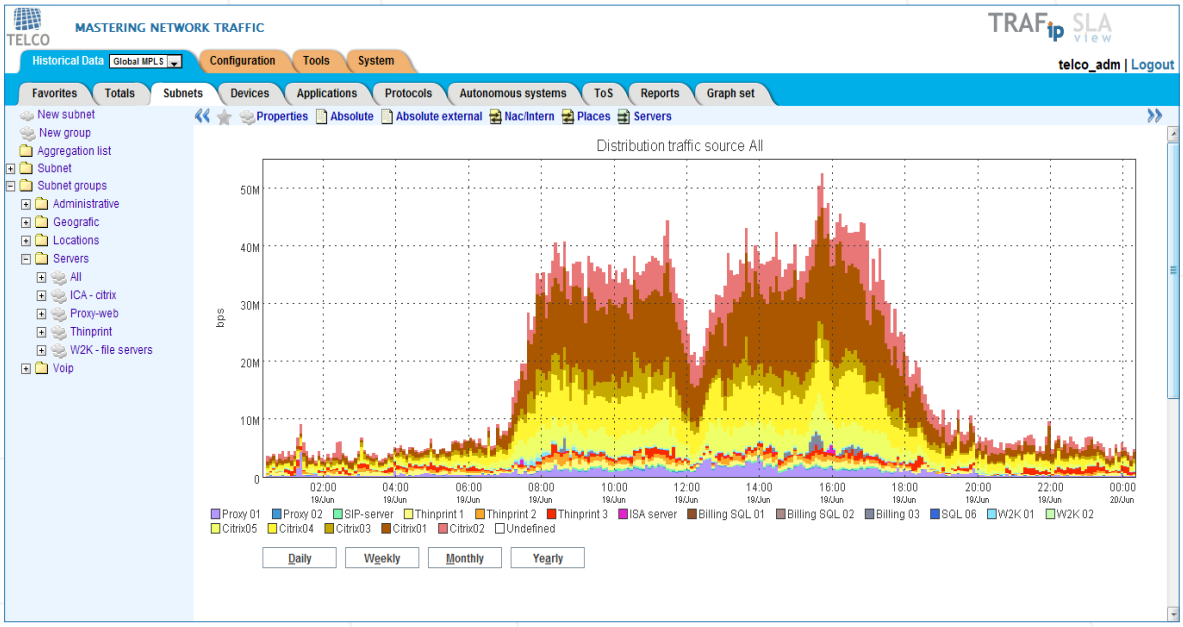
Localidade x AS



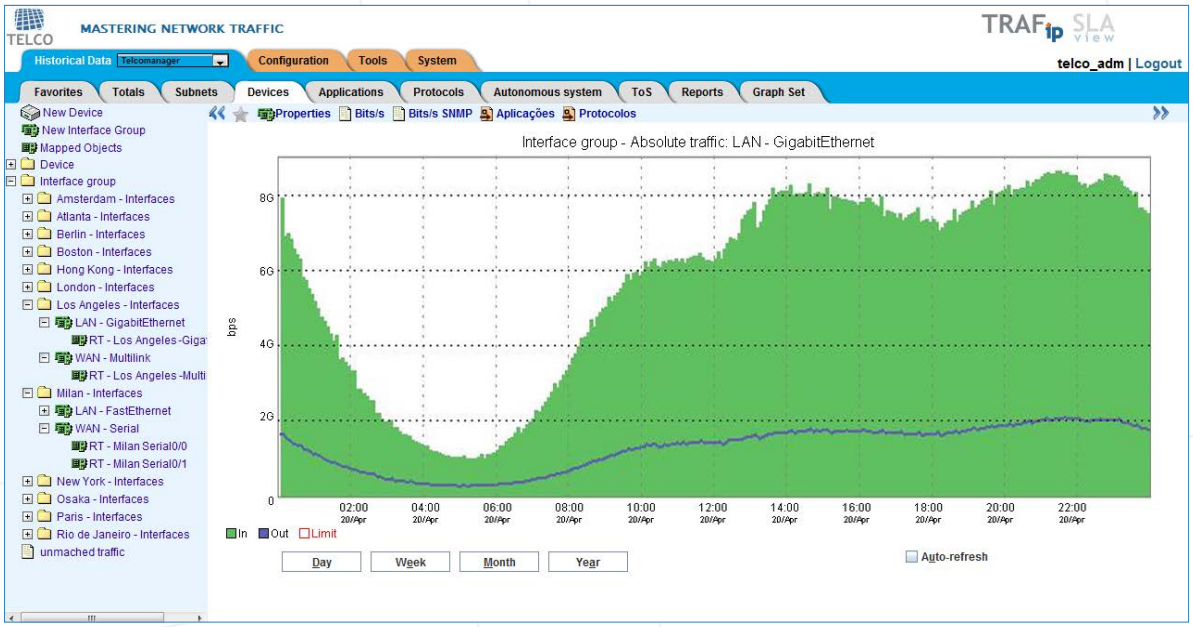
Localidade x Aplicações



Tráfego de Servidores



Grupos de Interfaces



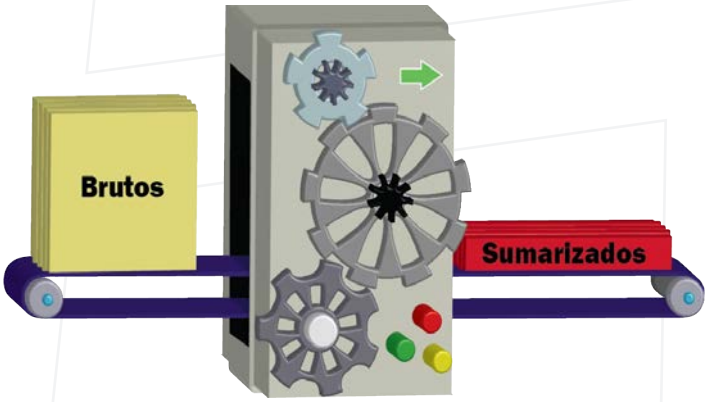
Longo Tempo de Retenção

O TRAFip processa online o enorme volume de dados brutos recebidos, agrega esses dados e gera uma forma compacta de armazenamento que denominamos dados sumarizados.

Devido à grande eficiência do sumarizador e de um método proprietário de armazenamento de seqüências históricas, os dados sumarizados ocupam muito menos espaço que os dados brutos originalmente coletados. Essa relação chega à proporção de 1 para 100. Com essa característica é possível manter online longos períodos de tempo de dados sumarizados.

Tipicamente, os appliances Telcomanager, em sua configuração mais básica, conseguem reter pelo menos um ano de dados sumarizados online para consulta, com frequência chegando essa retenção a mais de 5 anos, neste mesmo appliance, sob condições ideais de uso.

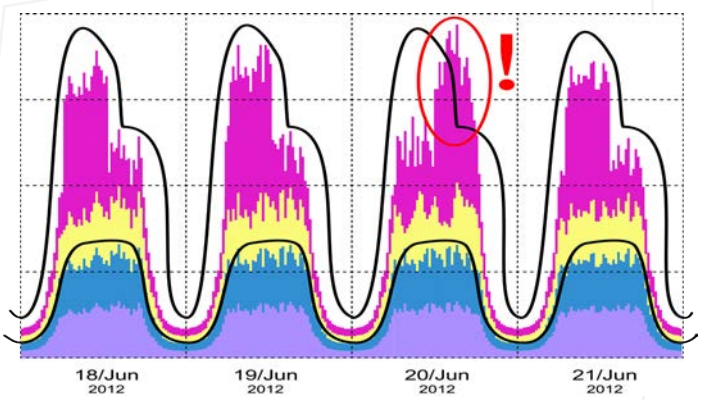
Um longo tempo de retenção não representa apenas um aumento de eficiência e conforto para o operador que se vê livre de ter que localizar dados antigos para análise. O longo tempo de retenção permite funcionalidades mais avançadas como análise de tendência e análise de mudança de comportamento, apresentadas mais à frente.



Mudanças de Comportamento

Para tráfegos de rede que apresentam uma grande variação de valores ao longo do dia, valores fixos não são uma solução adequada, e muitas vezes uma fórmula pode se tornar bastante complexa para representar.

Para essas situações o TRAFip dispõe do módulo de mudança de comportamento, sendo este um verdadeiro “auxiliar” do administrador de rede. Este módulo é capaz de analisar o tráfego e estabelecer regras adaptativas que consigam representar as variações típicas deste tráfego, gerando alarmes apenas quando esse comportamento característico não for observado.



Alarmes

O TRAfip pode ser configurado para gerar alarmes segundo critérios estabelecidos pelo administrador da rede. Esses critérios podem ser definidos de forma simples através de limites fixos ou percentuais. Critérios mais sofisticados podem ser expressos sob a forma de fórmulas, conjugando diversos valores coletados.

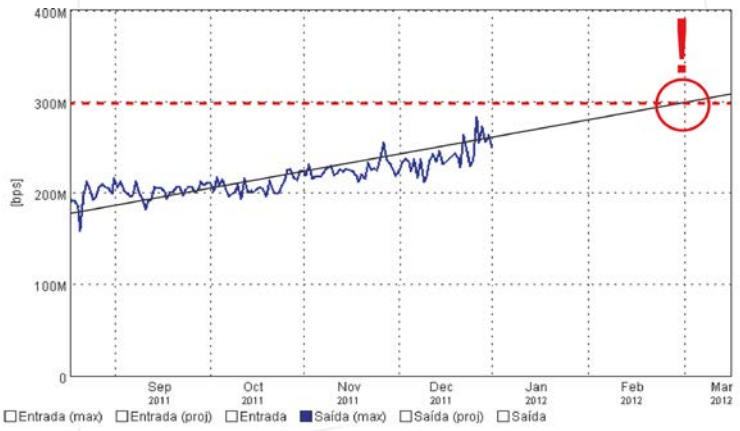
Análise de Tendência

Utilizando os dados coletados e sua enorme capacidade de retenção, o TRAFip consegue realizar previsões sobre a capacidade e os limites de sua rede. Por exemplo, ele pode dizer antecipadamente quando um link necessitará de upgrade ou ainda qual o tráfego estimado para uma determinada data.

As redes de dados atendem a necessidades dinâmicas de uso. Sabemos que infelizmente não basta dimensionar sua capacidade uma única vez e não se preocupar mais. As redes atendem uma demanda crescente de necessidades corporativas de tráfego de informação e frente a esse cenário são frequentemente expandidas. E a pior coisa que pode acontecer é o administrador se dar conta da necessidade somente quando ela já está instalada e gerando problemas.

O módulo de análise de tendência foi criado tendo em mente as necessidades de um administrador de rede em agir proativamente em relação ao planejamento de capacidade e expansão da rede. Ajudando a definir, com muita antecedência, quando essas expansões serão necessárias.

Concentre-se na estratégia de expansão ou na seleção dos parceiros e novas tecnologias enquanto o TRAFip faz o trabalho pesado e repetitivo de calcular e projetar dados!



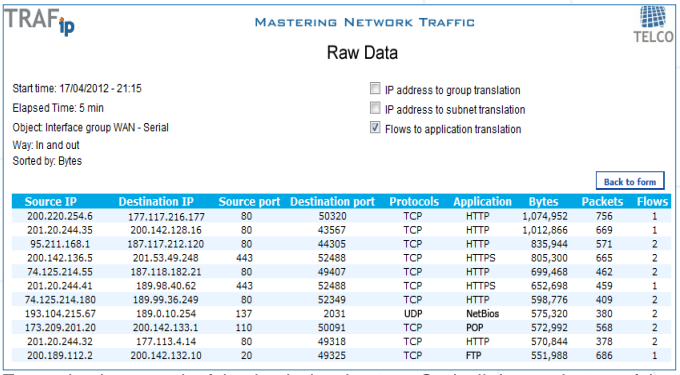
Relatórios

O TRAFip permite a geração de diversos relatórios detalhados, onde um rico conjunto de informações como IP origem, IP destino, porta origem, porta destino, entre muitas outras informações, podem ser obtidas.

O usuário pode personalizar um relatório e ainda agendar para uma futura execução periódica.

O TRAFip pode gerar os relatórios em HTML, CSV, TSV e PDF.

Dados Brutos



TRAFip — MASTERING NETWORK TRAFFIC — TELCO

Raw Data

Start time: 17/04/2012 - 21:15
Elapsed Time: 5 min
Object: Interface group WAN - Serial
Way: In and out
Sorted by: Bytes

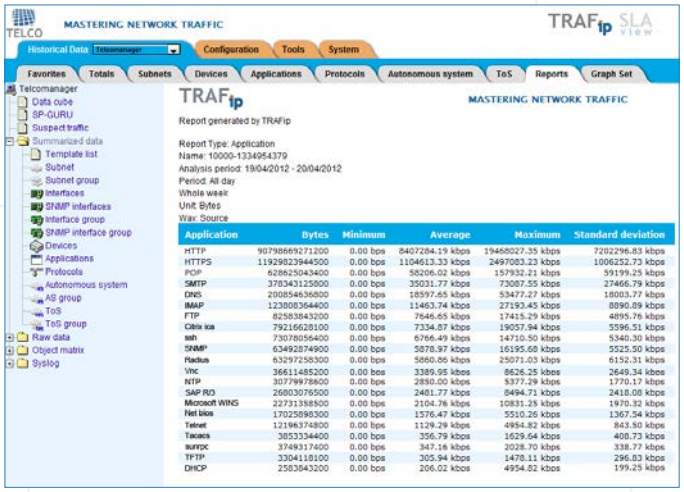
IP address to group translation
IP address to subnet translation
Flows to application translation

Back to form

Source IP	Destination IP	Source port	Destination port	Protocols	Application	Bytes	Packets	Flows
200.220.254.6	177.117.216.177	80	50320	TCP	HTTP	1,074,952	756	1
201.20.244.35	200.142.128.16	80	43567	TCP	HTTP	1,012,866	669	1
95.211.168.1	187.117.212.120	80	44305	TCP	HTTP	835,944	571	2
200.142.136.5	201.53.49.248	443	52488	TCP	HTTPS	805,300	665	2
74.125.214.55	187.118.182.21	80	49407	TCP	HTTP	699,468	462	2
201.20.244.41	189.98.40.62	443	52488	TCP	HTTPS	652,698	459	1
74.125.214.180	189.99.36.249	80	52349	TCP	HTTP	598,776	409	2
193.104.215.67	189.0.10.254	137	2031	UDP	NetBios	575,320	380	2
173.209.201.20	200.142.133.1	110	50091	TCP	POP	572,992	568	2
201.20.244.32	177.113.4.14	80	49318	TCP	HTTP	570,844	378	2
200.189.112.2	200.142.132.10	20	49325	TCP	FTP	551,988	686	1

Exemplo de um relatório de dados brutos. Cada linha pode ter várias traduções, como: aplicações, subredes e grupos de subredes.

Dados Sumarizados



MASTERING NETWORK TRAFFIC — TRAFip SLA view

Historical Data — Configuration — Tools — System

Favorites — Totals — Subnets — Devices — Applications — Protocols — Autonomous system — ToS — Reports — Graph Set

TRAFip — MASTERING NETWORK TRAFFIC

Report generated by TRAFip

Report Type: Application
Name: 10000-1334954379
Analysis period: 19/04/2012 - 20/04/2012
Period: All day
Whole week
Unit: Bytes
Way: Source

Application	Bytes	Minimum	Average	Maximum	Standard deviation
HTTP	90798669271200	0.00 bps	8407284.19 kbps	19468027.35 kbps	7202296.83 kbps
HTTPS	11929823944500	0.00 bps	1104613.33 kbps	2497083.23 kbps	1006252.73 kbps
POP	628625043400	0.00 bps	58206.02 kbps	157932.21 kbps	59199.25 kbps
SMTP	378343125800	0.00 bps	35031.77 kbps	73087.55 kbps	27466.79 kbps
DNS	200854636800	0.00 bps	18597.65 kbps	53477.27 kbps	18003.77 kbps
IMAP	123808364400	0.00 bps	11463.74 kbps	27193.45 kbps	8890.89 kbps
FTP	82583843200	0.00 bps	7646.65 kbps	17415.29 kbps	4895.76 kbps
Citrix ica	79216628100	0.00 bps	7334.87 kbps	19057.94 kbps	5596.51 kbps
ssh	73078056400	0.00 bps	6766.49 kbps	14710.50 kbps	5340.30 kbps
SNMP	63492874900	0.00 bps	5878.97 kbps	16195.68 kbps	5525.50 kbps
Radius	63297258300	0.00 bps	5860.86 kbps	25071.03 kbps	6152.31 kbps
Vnc	36611485200	0.00 bps	3389.95 kbps	8626.25 kbps	2649.34 kbps
NTP	30779978400	0.00 bps	2850.00 kbps	5377.29 kbps	1770.17 kbps
SAP R/3	26003076500	0.00 bps	2481.77 kbps	8494.71 kbps	2418.08 kbps
Microsoft WINS	22731358500	0.00 bps	2104.76 kbps	10831.25 kbps	1970.32 kbps
Net bios	17025898300	0.00 bps	1576.47 kbps	5510.26 kbps	1367.54 kbps
Telnet	12196374800	0.00 bps	1129.29 kbps	4954.82 kbps	863.80 kbps
Tacacs	3853334400	0.00 bps	356.79 kbps	1629.64 kbps	408.73 kbps
sunrpc	3749317400	0.00 bps	347.16 kbps	2028.70 kbps	338.77 kbps
TFTP	3304118100	0.00 bps	305.94 kbps	1478.11 kbps	296.83 kbps
DHCP	2503843200	0.00 bps	206.02 kbps	4954.82 kbps	199.25 kbps

Exemplo de um relatório de dados sumarizados que pode ser gerado por tipos de objetos, interfaces, subredes, dispositivos, aplicações e assim por diante.

Agendamento de Relatórios e Templates

O TRAFip permite o agendamento de relatórios de tráfego e o seu envio automático por e-mail. Para isso, basta salvar um template de relatório e indicar a hora do envio e a frequência. Assim, pode-se estabelecer um processo de pontos de controle de qualidade.

O agendamento evita a necessidade da repetitiva atividade de um operador, economizando o tempo deste profissional e evitando erros na geração de relatórios deste ponto de controle de qualidade.

Análise e Auditoria de QoS

O TRAFip recebe em cada fluxo a marcação de tipo de serviço, isso permite analisar como as classes de serviço estão sendo utilizadas. É possível identificar quais aplicações foram efetivamente encaminhadas para cada classe, o uso de banda de cada classe ou o uso de banda de cada aplicação dentro de sua própria classe de serviço.

O TRAFip possibilita uma perfeita visão de quão efetiva é a atual configuração de QoS ele ainda permite a identificação de erros de marcação e inadequações no dimensionamento das classes de QoS.

O TRAFip é um poderoso aliado que permite que você tire o máximo de sua rede.

Tráfego Suspeito

O TRAFip dispõe de um módulo específico para análise de tráfego suspeito. Esse módulo quando ativado realiza análises diretamente sobre os dados brutos coletados tentando encontrar padrões de tráfego que possam representar um DDoS, DoS ou ainda a propagação de um vírus pela rede. Além desses tráfegos clássicos, o módulo pode alarmar quando detecta um excesso de tráfego entre dois hosts da rede. O módulo pode ser parametrizado pelo operador de forma a evitar alarmes desnecessários e adequar-se às características específicas de sua rede.

Integração

O TRAFip pode ser integrado, no mesmo appliance, com o SLAview e o CFGtool. Outras informações sobre esses produtos podem ser encontradas em suas descrições técnicas.

www.telcomanager.com

tel.: +55 21 3211-2223
info@telcomanager.com
Av. Presidente Vargas, 962 - grupo 1201
20071-002 - Rio de Janeiro - RJ - Brasil

v7.2.2