BROADBAND TESTING

Kemp Flowmon: Uniting Netops And Secops

A Broadband-Testing Report

First published July 2021 (V1.0)

Published by Broadband-Testing

E-mail : info@broadband-testing.co.uk
Internet: HTTP://www.broadband-testing.co.uk

@2021 Broadband-Testing

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors.

Please note that access to or use of this Report is conditioned on the following:

1. The information in this Report is subject to change by Broadband-Testing without notice.
2. The information in this Report, at publication date, is believed by Broadband-Testing to be accurate and reliable, but is not guaranteed. All use of and reliance on this Report are at your sole risk. Broadband-Testing is not liable or responsible for any damages, losses or expenses arising from any error or omission in this Report.
3. *NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY Broadband-Testing. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY Broadband-Testing. IN NO EVENT SHALL Broadband-Testing BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.*
4. This Report does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products, or that the products will meet your expectations, requirements, needs or specifications, or that they will operate without interruption.
5. This Report does not imply any endorsement, sponsorship, affiliation or verification by or with any companies mentioned in this report.
6. All trademarks, service marks, and trade names used in this Report are the trademarks, service marks, and trade names of their respective owners, and no endorsement of, sponsorship of, affiliation with, or involvement in, any of the testing, this Report or Broadband-Testing is implied, nor should it be inferred.

TABLE OF CONTENTS

BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do… The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process.

Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

EXECUTIVE SUMMARY

- Network performance and security are not isolated instances of IT; they directly impact on each other and are completely interactive. However, historically network operations (Netops) and security operations (Secops) have effectively been siloed, which is both inefficient and counter-productive

- Networks in the cloud era are becoming increasingly complex in terms of topologies, as the hybrid (On/Off Premises) approach becomes increasingly common. In turn, this makes it more difficult to manage, secure and optimise those networks.

- In the event of either a performance or security issue arising, on a hybrid network especially, locating the problem can take days, weeks or even months, or is simply untraceable without the right tools to hand. In the event of it being performance-related, this can result in significant down-time, meaning $$$$$. If, however, the problem is a security breach, then by the time the problem has been identified, it may have resulted in business-damaging data loss or worse.

- For this reason, Kemp Technologies, whose technology is used to optimise application and data delivery globally, recently acquired Flowmon, providing the company with these very tools. So, this report is focusing on exactly what the Flowmon technology offers with some sample use cases.

- From capacity planning to application delivery optimisation, the Netops element of the Flowmon technology provides 24x7 monitoring and analysis, with real-world use of the over-hyped Artificial Intelligence (AI) at the heart of this, rather than AI simply being a marketing offensive.

- Tied directly in with the network monitoring and analysis is the Secops element – alerting on network behaviour anomalies and possible cyber-attacks, with the ability to deep dive into the problem and rapidly identify a threat or other cause of behavioural change.

- In bringing together the worlds of Netops and Secops, not only is the Flowmon technology providing the means to optimise and secure the network 24x7, but it also results in de-duplication of IT time, effort and expenditure, thereby reducing bottom line spend. It's what you might call the ultimate win win scenario! More to the point, it also shows how, what was once seen as a "nice to have" or "insurance policy" is now essential technology, as those networks grow ever more complex.

UNITING NETOPS AND SECOPS

It's not being over the top to say that, in many cases, IT has got itself into something of an unholy mess.

The bolt-on approach to building networks over the best part of the past three decades has brought with it many problems, not least visibility. Many companies - regardless of size, geographical spread and status - simply do not know what applications, devices and even users are on their network. They don't necessarily even know where their extended network actually is, not least due to all forms of outsourcing over those decades, culminating in cloud-based deployments in the past few years. This immediately presents two obvious dangers: potential performance nosedives and security vulnerabilities – and, with them, a seemingly invisible network to track. Add in the Work From Home/Anywhere factor that the pandemic has forced on companies and the gravity of the situation is deeper than ever.

At the same time, and for far too long, IT has been creating islands of technology and resource, so tasks and data that should be shared are split between different teams and individuals who seldom communicate with each other. The result is a huge void in terms of visibility and understanding of what is on the network and how to manage and secure applications and data between the different IT teams – Netops, Secops, Devops… Not only does this create major potential problems in optimising and securing the network; it also results in duplication of effort, a lack of synchronisation and potentially excessive IT spend – all the while actually making the end user experience worse!

The reality is that network performance and security do not work in isolation but, instead, directly impact on each other. They therefore need to be managed as one, and not on an "as needed" basis, but 24x7 – IT never stops nowadays. Additionally, the landscape of IT – network topologies – are changing out of all recognition. A constant fear for companies currently is an inability to manage what appears to be a dramatic infrastructure change. Think back to IT of the 70s and early 80s – one or maybe two mainframe/midrange computers hosting a number of terminals and perhaps a smattering of PCs… That was not difficult to manage, even though in-fighting between what was then Datacomms and Telecoms made it harder than it should have been. Regardless, contrast that infrastructure with today's ever-changing hybrid structures, increasing numbers of remote users, any number of different endpoint devices, multiple xSPs.

Networks in the cloud era are becoming increasingly complex in terms of topologies, as the hybrid (On/Off Premises) approach becomes increasingly common. In turn, this makes it more difficult to manage, secure and optimise those networks – no one could even pretend that kind of contemporary IT footprint was easy to manage. It isn't; simply optimising and securing what might appear to be a healthy network is hard enough, but in the event of a performance or security issue arising? Panic, lots of finger-pointing and an inability to readily remediate the problem is a common scenario. In a best-case scenario this is likely to create expensive downtime and a reduction in productivity; the worst-case scenarios can potentially be business-threatening, especially in an era where many companies have been forced to reinvent themselves – digital transformation, adapting to new customers and new or different needs as a result of the pandemic – as if that weren't hard enough in its own right.

© Broadband-Testing 1995-2021

So, IT needs solutions; a hero technology to dig them out of these holes or, even better, make sure they are never formed in the first place. With Flowmon, Kemp Technologies' recent acquisition promises to potentially be that IT lifesaver, so let us take a look at what it offers those despairing Netops and Secops teams.

PRODUCT OVERVIEW

The basic premise behind the Flowmon technology is to provide a near instant way of monitoring and analysis of the network, from both a Netops and Secops perspective, using a combination of AI/Machine Learning (ML), heuristics and analytics, in order to both improve network performance and alert on incidents and potential threats.

Let's get straight to the point here. There have been many attempts in the past to provide some elements of what Flowmon is offering but, all too often, these potential solutions have taken weeks, or even months, to deploy, by which time it's simply too late. Basic deployment of the Flowmon solution takes no more than an hour from download. At that point it starts to monitor and analyse the network, taking a copy of everything flowing across it. With this baseline in place, it can then start to get smart and proactive – identifying any anomalies and alerting them, both for unencrypted and encrypted traffic. Basic tasks include the like of calculating the bidirectional round-trip time ((RTT) for a TCP SYN-ACK (request-response) to test for any latency and/or jitter in a connection, server response times and the retransmit rate. For example, simply by analysing the RTT versus the server response time, you can see whether a problem is manifesting itself on the network or at the server (or even both).

It is important to note that Flowmon does not inject unwanted additional synthetic traffic into the network in order to measure it, but simply uses the real traffic. Where it gets smart is where it uses the gathered performance date to apply network metadata run through ML algorithms to show anomalies such as attacks, misuse and strange behaviour patterns, including at the network perimeter, where the firewalls may have missed something – and they do. It also has full DDOS protection (in either notification or mitigation modes) and is effective up to 400Gbps. Traffic can be redirected to 3rd party scrubbing centres for cleaning if required. Equally, that "blue sky" between the perimeter firewalls and endpoints, that is all too often ignored, is covered off.

Again, it is important to note that this analysis is out of band, so there is no additional traffic or agents consuming resource – just complete transparency. However, the system can handle multiple data feeds making it ideal for MSPs managing a multi-tenant environment. At the same time, a simple deployment can all run on a single Virtual Machine (VM). Indeed, in smaller environments Flowmon might provide most of the required SIEM and APM elements itself. Everything runs on a purpose-built, hardened version of Linux, meaning no update requirement complications.

As is common nowadays, a central dashboard approach is used as the primary access to all the data and analysis which, by default, is kept for 30 days. Multiple dashboards – and reports – are available and all totally customisable. Reporting is interactive and based on a classic "drill down" approach to get deeper information. And there is plenty being collected – for example, DNS info alone has over 250 different fields to analyse.

While Flowmon performs the primary analysis, there are occasions where full packet capture and analysis is required; rather than this going 24x7 and generating unusable (and impossible to store) amounts of data, Flowmon uses an event-based, just in time packet capture approach, on an "as needed" basis, after which the PCAP can be downloaded and analysed with the ubiquitous Wireshark.

In addition to the intelligent collection and analysis, the system also simply black-list sites – there are seven databases in all and the lists are updated every six hours. Background information is also provided on all black-listed elements, such as a host or a URL. Data can also be fed into other systems with Syslog. Finally, Flowmon can carry out Deep Packet Analysis on a range of protocols, including DNS, DHCP, SMB, HTTP and SIP.

KEMP FLOWMON: USE CASES

Secops – Ransomware (anomaly detection)

No security threat has been more talked about over the past couple of years than ransomware. It has effectively become a multi-billion-dollar (or bitcoin!) industry in its own right and targets the most valuable commodity in the modern world – data.

Flowmon's secops' capabilities extend to identifying ransomware attacks, such as the following scenario which was based on a real customer case. It involves a compromised device after an attack on a Samba server for which an attacker has accessed a network via an RDP (Remote Desktop Protocol) server vulnerability, gained valid user credentials from a keylogger on a Windows server, in order to access the Samba server and grab data. The attacker then extracts the data in multiple chunks using the ICMP (ping) protocol, then encrypts the data still residing on the Samba server – classic ransomware. In the real-world case, the attacker then, naturally, fires off an email demanding a ransom payment, usually attaching a sample of the captured file as proof.

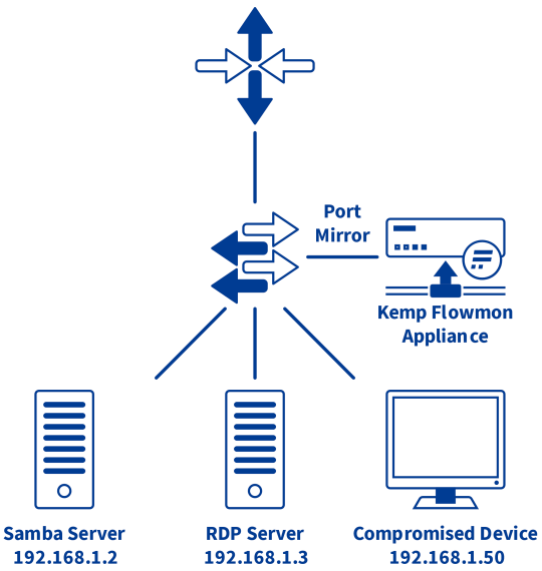

Figure 1 – Ransomware Scenario

So how does Flowmon capture this attack? First, using the Flowmon ADS (Anomaly Detection System), carrying out an ARP (Address Resolution Protocol) scan reveals an

event showing an ARP coming from an infected device (192.168.1.50) from the ARP scan table. There follows a Vertical TCP SYN scan to show discovered targets that might have vulnerable services that can be compromised.

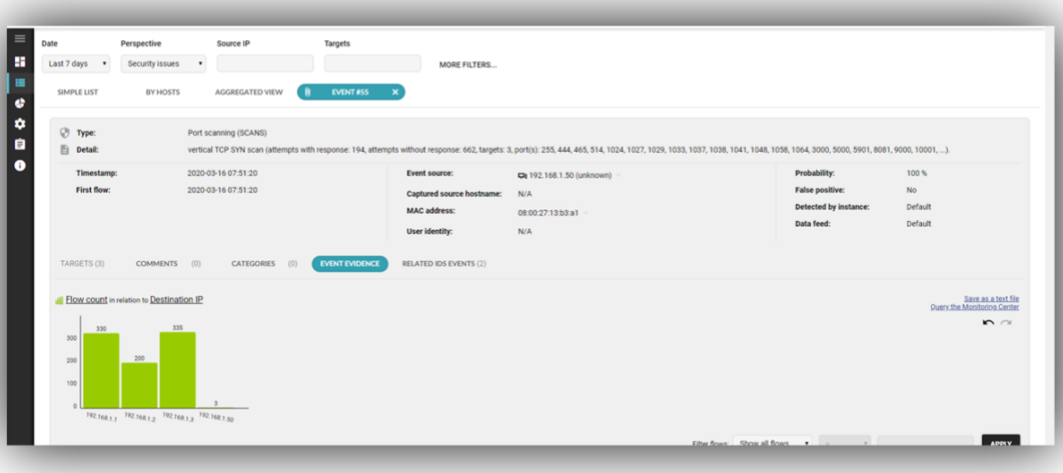

Figure 2 – Vulnerable Targets From Vertical TCP SYN Scan

Furthermore, an attack on the Windows RDP is discovered with a logged event relating directly to this. Deep diving into more detail, related intrusion detection triggers reveal an exploitation of the known BlueKeep security vulnerability on the RDP server.

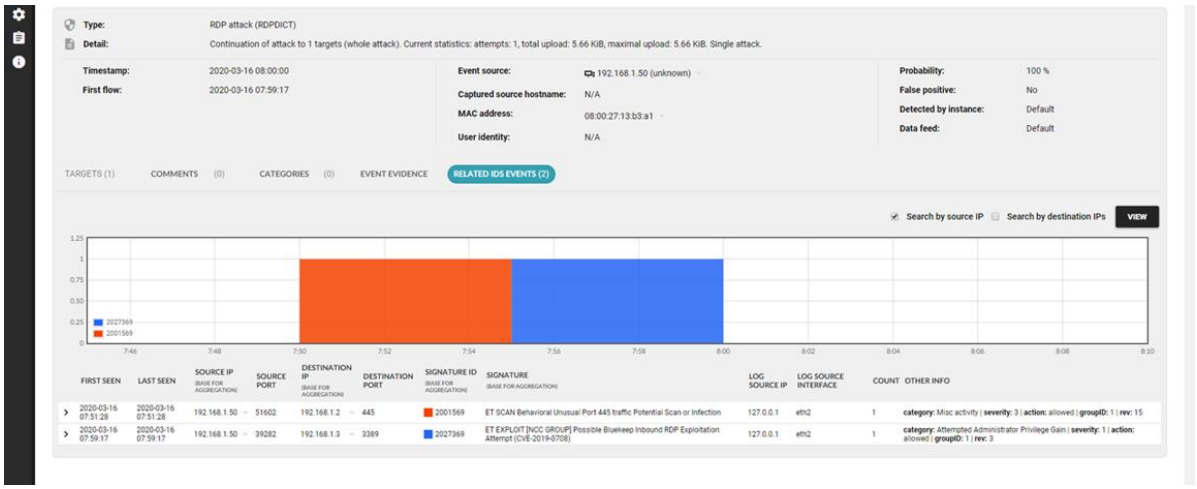

Figure 3 – RDP BlueKeep Vulnerability Revealed

In terms of the data extraction, it is noted that several different methods were triggered; a data upload anomaly, and an ICMP traffic anomaly (ICPM traffic with a payload – as the data was extracted – is an obvious anomaly to the Flowmon ADS, even though the packets were quite small and easily missed using purely manual analysis.

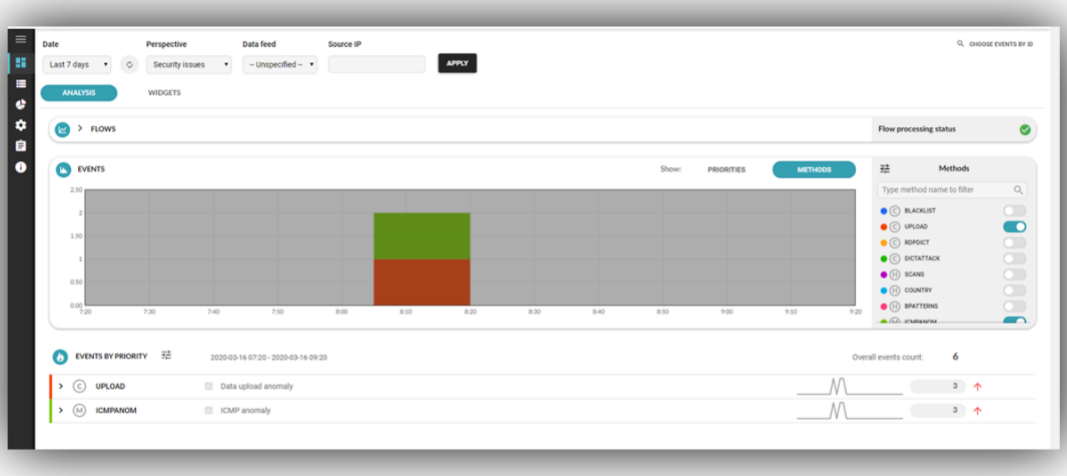

Figure 4 – Anomalous Behaviour Signals

However, as we now know there has been illegal access, we can use the aforementioned capabilities to use full packet capture and analysis on an "as needed" basis, using Wireshark to analyse the packet contents in full. This, in turn, reveals the actual content elements, including the filename and data contents.

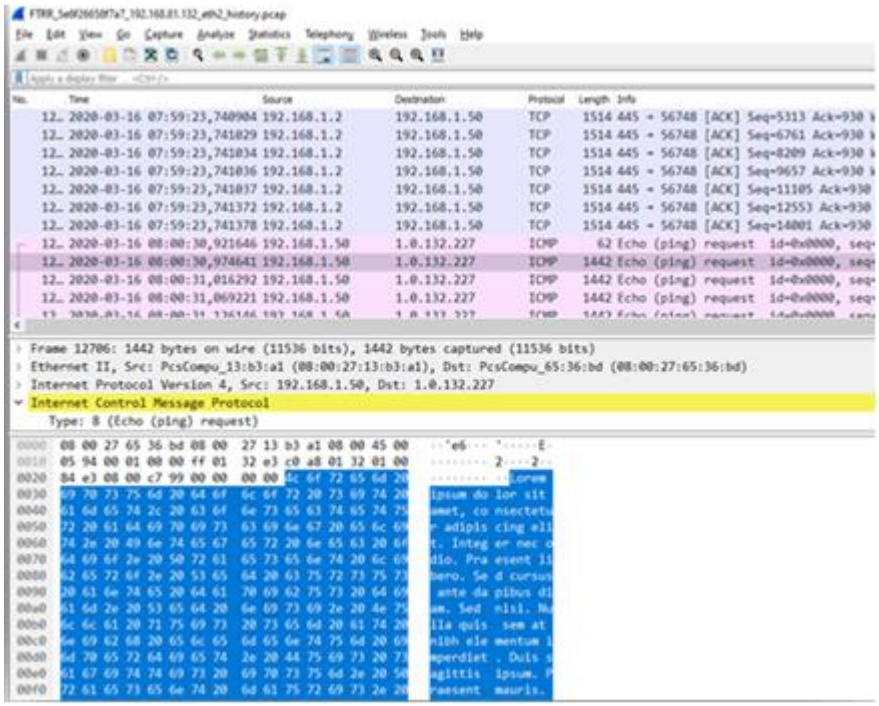

Figure 5 – Wireshark Packet Capture: Payload Content Analysis

It should be noted that all these events can be viewed on a timeline, which makes it easy to understand the processes involved in the attack and help prevent similar attacks in the future – that being the primary point of the analysis, of course.

© Broadband-Testing 1995-2021

Netops/Secops – Encrypted Traffic Analysis

One major potential problem area for companies is encrypted traffic; often given levels are mandatory for use within an enterprise, but how do you monitor and analyse that encrypted traffic to a) guarantee compliance and b) resolve those potential problems?

For these reasons, Flowmon provides an Encrypted Traffic Analysis (ETA) dashboard which we will now use to analyse – as an example – some TLS (Transport Layer Security) traffic. TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and VoIP.

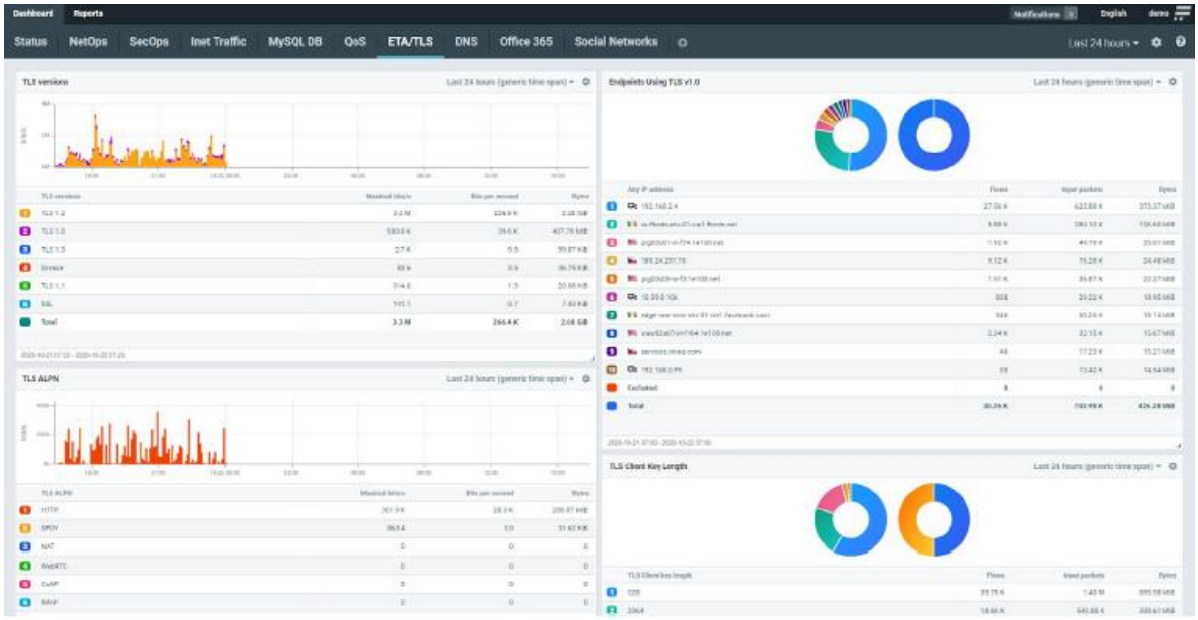

Figure 6 – Kemp Flowmon ETA/TLS Dashboard

As you'll note from the dashboard layout, the consistency of presentation runs throughout the Flowmon offering so, once you've got the hang of one element, the rest follow logically. In this case, at the top is a graph of TLS protocol usage differentiated by version. Next to it is a list of the top 10 endpoints using outdated TLS 1.0 – in other words, an instant viewpoint of devices using an obsolete, and therefore potentially vulnerable, encryption standard. No support equals vulnerable…

One more, from this top level we can drill down using the **More info** menu to analyse in more detail, for example, the TLS-client key length and a chart of TLS ALPN (Application-Layer Protocol Negotiations).

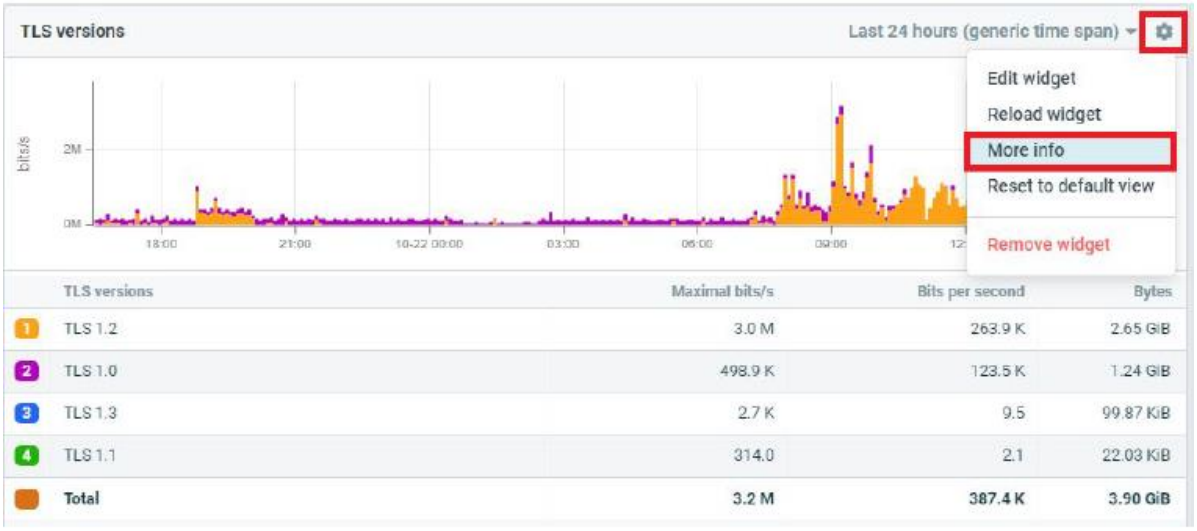

Figure 7 – Kemp Flowmon ETA/TLS Dashboard: Analysis of key length and ALPN)

Here we can see exactly what versions of TLS are in use and to what extent. Using the **Advanced analysis** mode once more, we can then examine the potential problem area – the TLS 1.0 usage. By filtering on TLS 1.0, the results indicate that there is a device using the IP of 192.168.2.4 in the company using the obsolete TLS standard.

Obviously, not is this kind of discovery only important from a security standpoint, but also from a compliance perspective. Given the full TLS application-layer visibility, we could equally examine other potential problem areas such as the validity of TLS certificates, TLS issuer name and encryption algorithms. In each case, the search procedure is the same, just the content being analysed changes. Again, this emphasises the ease of use with the software; yes, ease of use is always a benefit, but when analysing traffic that might include ticking time bombs, saving seconds through speed of data discovery could be precious.

Netops – Bandwidth Monitoring (traffic spikes)

Traffic spikes are a common indicator of unusual or specific (time/day) behaviour patterns that need to be dealt with, since they are a primary cause of outages – note the household name casualties that have been much documented during the pandemic.

With Flowmon, our starting point to investigate potential spikes – in this case with Internet traffic – is naturally the dashboard. In this instance, the bottom half of the screen is showing top sources and destinations of inbound and outbound Internet traffic while the top half readily indicates a massive traffic spike that occurred between 15:00-16:00. Being so out of line with regular traffic flows, this would naturally merit investigation, for the reasons stated above.

© Broadband-Testing 1995-2021

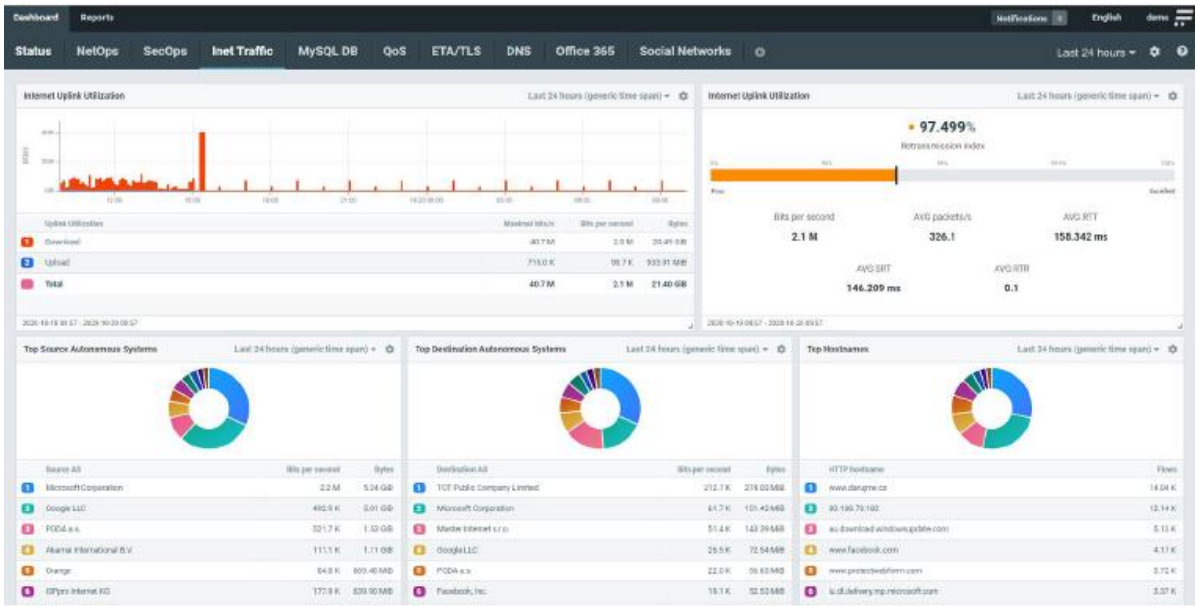

Figure 8 – Kemp Flowmon Dashboard: Bandwidth Monitoring

At this point we can drill down, selecting a **More info** option from the drop-down menu, into analysis mode, where we can focus in on that spike and see that it is a result of an excessive number of downloads.

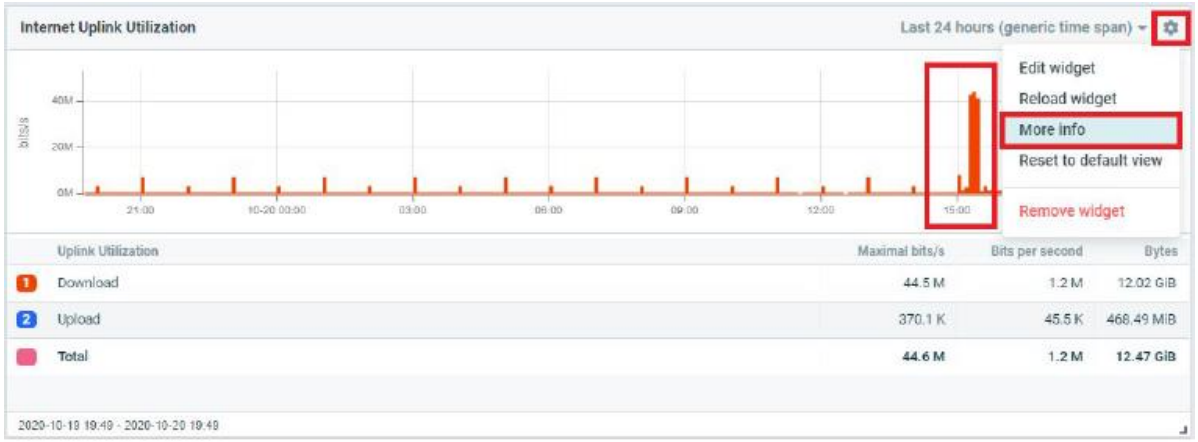

Figure 9 – Kemp Flowmon Dashboard: Drilling Down Into More Info

In the **Advanced analysis** window, a chart showed the first 10 IP conversations (i.e., aggregated connections between two hosts) in order of bytes transferred. From this, it was clear that communications between the pair of IP addresses **172.217.23.193** - **192.168.70.80** resulted in over 4GB of traffic being generated within three flows/connections. Simply right-clicking on one of the IP addresses gave us access to every single connection related to this communication, from which we chose **First 20 flows** from the dropdown menu.

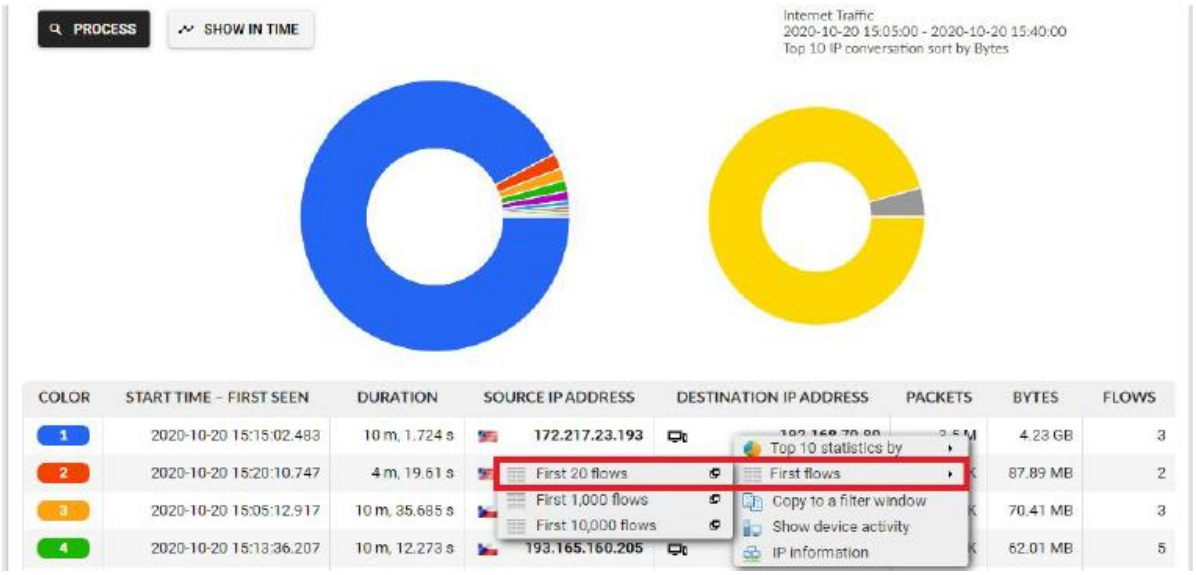

Figure 10 – Kemp Flowmon Dashboard:Identifying Spike Source

From the list it was easy to see that the internet traffic spike was caused by a large download from an HTTP server. However, to short-cut the process further, we could have configured the system to alert us about any unusual situation arising, and this case would have resulted in an alert, as soon as that link saturated. Simply using **Alert view** we could review that spike as it happened in real-time, in greater detail. Essentially, what level of detail you wish to drill down into is all covered off – the more you dig, the more you find!

Netops – DNS Errors

Another major cause of application and data connectivity issues are DNS errors. From a user perspective especially, being unable to connect to regular application or site is both confusing and expensive in terms of potential loss of productivity. The classic scenario is the service management (helpdesk) team receiving a call or message to say a user cannot access an application or site – AKA a specific server in many instances. In this type of scenario, Flowmon provides a DNS dashboard, from which we can dig down into the problem.

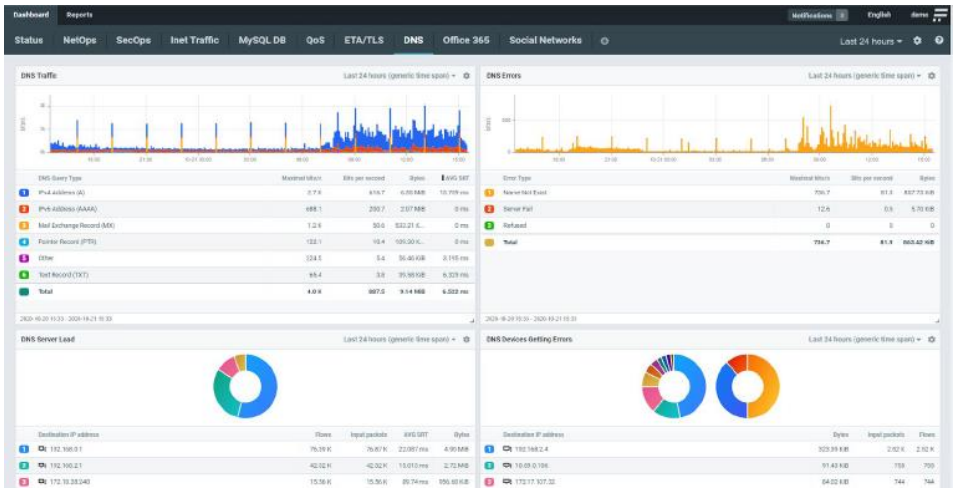

Figure 11 – Kemp Flowmon DNS Dashboard

This dashboard gives us an overview of DNS traffic and DNS errors, with a breakdown of DNS servers handling the greatest load, devices getting the most DNS errors, and related information. In this instance we wish to investigate a potential server problem, so – in a similar fashion to the first scenario – we once again can drill down, selecting a **More info** option from the drop-down menu (DNS Errors in this case).

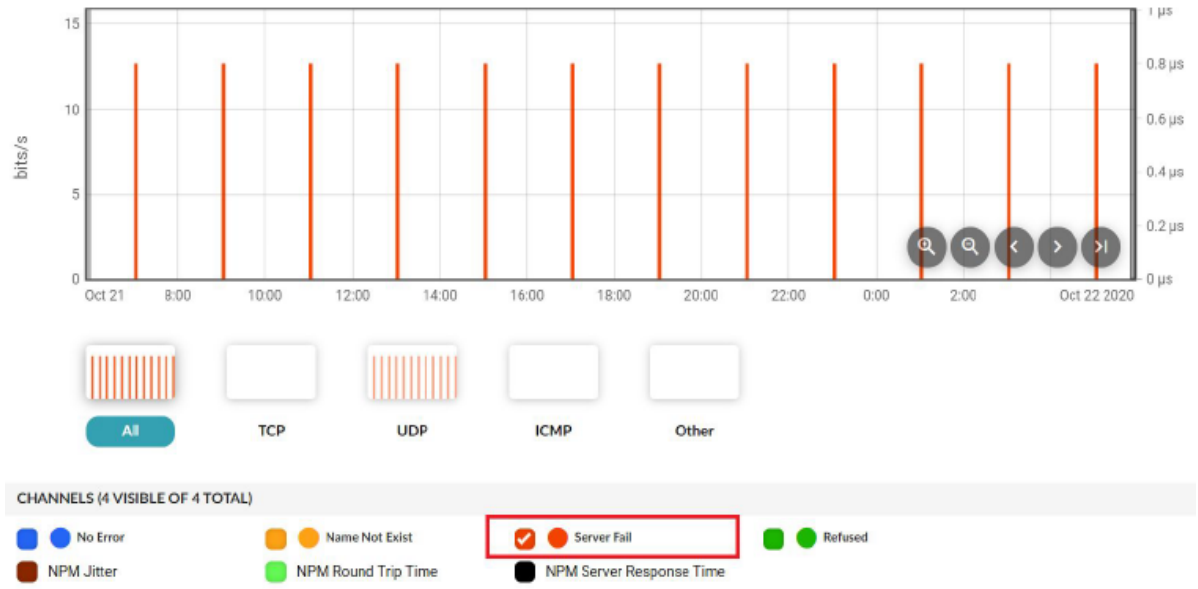

Figure 12 – Kemp Flowmon DNS Errors Highlighted

From the drill-down graph we can clearly see that the majority of errors are resulting from an attempt to connect to non-existing domains (orange) with periodic server failures (red). To analyse these errors in more detail we can then access a **First flows** menu, from which we can choose **First 20 flows** revealing a table of the flow data. In turn, from this we can see that seemingly the DNS server leasing the IP of 172.18.28.240 is the one experiencing the issues.

START TIME – FIRST SEEN	DURATION	PROTOCOL	SOURCE IP ADDRESS	SOURCE PORT	DESTINATION IP ADDRESS	DESTINATION PORT	TCP FLAGS	TOS	PACKETS	BYTES	FLOWS
2020-10-22 01:00:49.212	0 s	UDP	172.18.28.240	domain	172.17.107.32	27555	.....	Best Effort & Default	1	57 B	1
2020-10-22 01:01:38.281	0 s	UDP	172.18.28.240	domain	172.17.107.32	11829	.....	Best Effort & Default	1	54 B	1
2020-10-22 01:01:43.830	0 s	UDP	172.18.28.240	domain	172.17.107.32	56229	.....	Best Effort & Default	1	64 B	1
2020-10-22 01:01:46.906	0 s	UDP	172.18.28.240	domain	172.17.107.32	32314	.....	Best Effort & Default	1	55 B	1
2020-10-22 01:01:47.149	0 s	UDP	172.18.28.240	domain	172.17.107.32	23376	.....	Best Effort & Default	1	65 B	1
2020-10-22 01:01:59.260	0 s	UDP	172.18.28.240	domain	172.17.107.32	41142	.....	Best Effort & Default	1	67 B	1
2020-10-22 01:02:07.437	0 s	UDP	172.18.28.240	domain	172.17.107.32	54986	.....	Best Effort & Default	1	54 B	1
2020-10-22 01:02:18.056	0 s	UDP	172.18.28.240	domain	172.17.107.32	15899	.....	Best Effort & Default	1	58 B	1
								Flows 8		Bytes 474 B	Packets 8

Figure 13 – Kemp Flowmon DNS Flow Analysis

Digging deeper into the communications, we can dive into Layer7 stats, providing us with more DNS-related information including the type of the DNS message, the payload of those messages, and, at the heart of the problem, the DNS question names, which the DNS server has not been able to deliver

START TIME - FIRST SEEN	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	DNS QUERY/RESPONSE	DNS QUESTION TYPE	DNS QUESTION NAME	DNS RESPONSE NAME	DNS RESPONSE DATA
2020-10-22 01:00:49.212	172.18.28.240	172.17.107.32	Response	MX	tmoc.org.sg		
2020-10-22 01:01:38.281	172.18.28.240	172.17.107.32	Response	MX	bmed.com		
2020-10-22 01:01:43.830	172.18.28.240	172.17.107.32	Response	MX	bestdealsalert.com		
2020-10-22 01:01:46.906	172.18.28.240	172.17.107.32	Response	MX	cl.uh.edu		
2020-10-22 01:01:47.149	172.18.28.240	172.17.107.32	Response	MX	canariastelecom.com		
2020-10-22 01:01:59.260	172.18.28.240	172.17.107.32	Response	MX	eproauctionreport.com		
2020-10-22 01:02:07.437	172.18.28.240	172.17.107.32	Response	MX	f-mp.com		
2020-10-22 01:02:18.056	172.18.28.240	172.17.107.32	Response	MX	ida-dtek.com		

Flows:

Figure 14 – Kemp Flowmon DNS Detailed Analysis

IN CONCLUSION

Too many products and services within the world of IT are the classic invention of a solution looking for a problem.

In the case of Kemp Flowmon, we have the exact opposite. It exists because all the potential – and absolute – problem areas it targets and addresses already exist. In other words, it does what it says on the tin. And very efficiently too. The reality is that the contemporary hybrid network is unmanageable and impossible to secure using traditional methods. What the Flowmon technology brings to the table is what is required now – in 2021 – and onwards., as the IT infrastructure revisions continue apace for some years to come yet.

Moreover, it brings together the isolated worlds of Netops and Secops to create a far more secure, resilient and efficient way of managing a network. In so doing, helps enormously with the never-ending task of optimising and securing the network 24x7, reducing the excess of duplication in IT and thereby saving budget to boot. If that sounds like a must-have, then you'd be right on the money – highly recommended.