NETFORT
know your network

UK MSP Uses NetFort AWS Traffic Visibility to Troubleshoot a DDOS Attack on Their Website

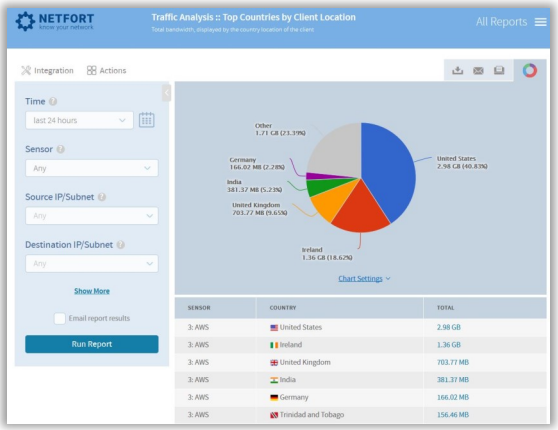
As organizations move to the cloud, like any network, the requirement for visibility to troubleshoot an 'urgent' issue must eventually be addressed. But this is easier said than done as network administrators are often severely hindered by tools and a lack of real time traffic visibility offered by public hyper-cloud providers. It is not possible to simply *walk up to the cloud* and take a packet capture.

The Initial Problem – 'our website is slow'

"At approximately 10 am Tuesday morning, a developer updating the blog on our website hosted on AWS, complained it seemed really slow and was making updates almost impossible," according to Stephen, the CTO of a UK MSP with less than 60 employees. After a few minutes, the website was down and unavailable.

Troubleshooting – getting to the root cause

Standard AWS tools revealed that the CPU utilisation was very high but, it did not provide further drill down or detail. The MSP was a beta site for the new LANGuardian AWS VPC Flow log sensor, it was deployed in AWS and monitoring all traffic to and from the website.



AWS VPC Flow Logs

AWS VPC Flow Logs provide 'Cisco Netflow-like' data about the IP traffic traversing the AWS estate and provide data on:

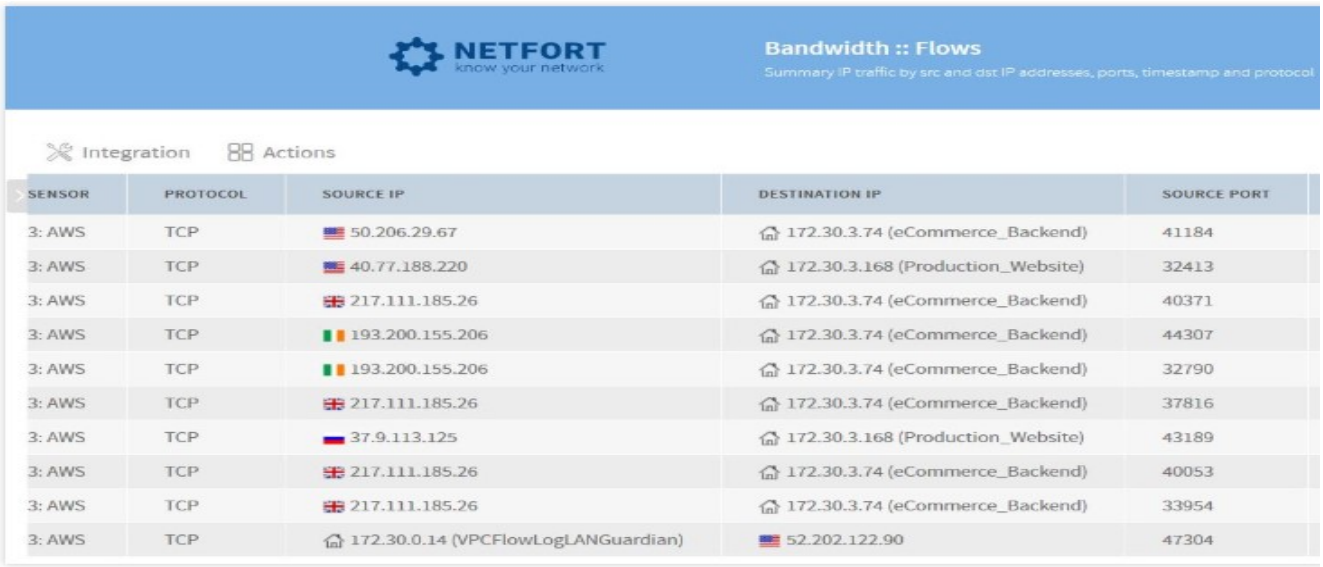
- Source and destination IP addresses and ports
- Protocol, sent packet and byte counts
- Interface and AWS accountID
- Allowed or Denied indicator
- Number of packets and bytes transferred
- Start and end time

VPC Flow Logs are processed by LANGuardian, generating similar metadata to NetFlow. The VPC Flow Logs are merged into sessions, Geolocation information is then added and saved into the NetFort database.

Results - the final 'drill down'

Upon running a 'Top Users' report, one IP was immediately highlighted. It was registered in Holland, using a script to automate registration attempts of a form used for membership and access to white-papers on their site.

"Now that we had the IP address and understood what was happening, we were able to do a WHOIS lookup search to find the ISP and contact them. We sent them our report, the proof, and they immediately disconnected the user, the whole process took less than 5 minutes but clearly illustrates the value of real time traffic visibility of your AWS estate," according to the CTO.


NETFORT
know your network

Bandwidth :: Flows
Summary IP traffic by src and dst IP addresses, ports, timestamp and protocol

Integration Actions

SENSOR	PROTOCOL	SOURCE IP	DESTINATION IP	SOURCE PORT
3: AWS	TCP	50.206.29.67	172.30.3.74 (eCommerce_Backend)	41184
3: AWS	TCP	40.77.188.220	172.30.3.168 (Production_Website)	32413
3: AWS	TCP	217.111.185.26	172.30.3.74 (eCommerce_Backend)	40371
3: AWS	TCP	193.200.155.206	172.30.3.74 (eCommerce_Backend)	44307
3: AWS	TCP	193.200.155.206	172.30.3.74 (eCommerce_Backend)	32790
3: AWS	TCP	217.111.185.26	172.30.3.74 (eCommerce_Backend)	37816
3: AWS	TCP	37.9.113.125	172.30.3.168 (Production_Website)	43189
3: AWS	TCP	217.111.185.26	172.30.3.74 (eCommerce_Backend)	40053
3: AWS	TCP	217.111.185.26	172.30.3.74 (eCommerce_Backend)	33954
3: AWS	TCP	172.30.0.14 (VPCFlowLogLANGuardian)	52.202.122.90	47304

Summary

- Cloud is no longer a *blind spot* with real time visibility of traffic in AWS
- Detection of suspicious activity
- Instant drill down to the granular detail
- Reports for third parties with actual proof
- Access to forensic data to investigate historical issues

Who uses NetFort?

NetFort is used to monitor, troubleshoot and report on everyday network and user activities for customers like these: