

IOTA Use Case

QUICKLY ISOLATING CLOUD-BASED APPLICATION ISSUES



PROBLEM

Users at a remote office experience poor application performance with a cloud-hosted application.

CLAIM

The IT organization feels the server is under resourced. The provider says the problem is the client network. Neither side has proof.

Information needed

The server ping roundtrip time seems to be ok, at least when engineers run occasional tests from the central office. However, this test only validates the network path between the client network and the cloud environment. They needed packet-level detail of the problem while it was happening. This was difficult to get because the problem was not always happening while engineers were onsite. They needed a way to simply and persistently capture traffic from the client side so the problem could be caught in the act.

The application was recently migrated to the cloud, so the network engineering team no longer had access to capture on the server side.

Once the problem was properly captured during a problem period, statistics like the network roundtrip time, server response time, TCP retransmission frequency, and other TCP outliers can be measured to isolate the true problem domain – whether client, network, or cloud-server.

IOTA Made Things Easy

IT engineers were able to install the IOTA at the remote site by putting it inline between the client network and the edge router. This vantage point allowed them to see the activity of several clients, not just one. They could contrast client activity between problem periods and times with good performance.

After a few hours, clients reported that they again experienced the performance problem. Engineers were able to immediately access the IOTA using the web-based interface from the central office and begin troubleshooting. Within minutes they had access to the core details needed to isolate the problem domain.

Step 1 - Getting the right timeframe

First, engineers needed to filter on the period of time that the issue happened. From the starting screen in the Home dashboard, they could sweep across the time frame when the problem occurred and see the IP conversations during that time. They observed both the problem client and the server addresses in play.



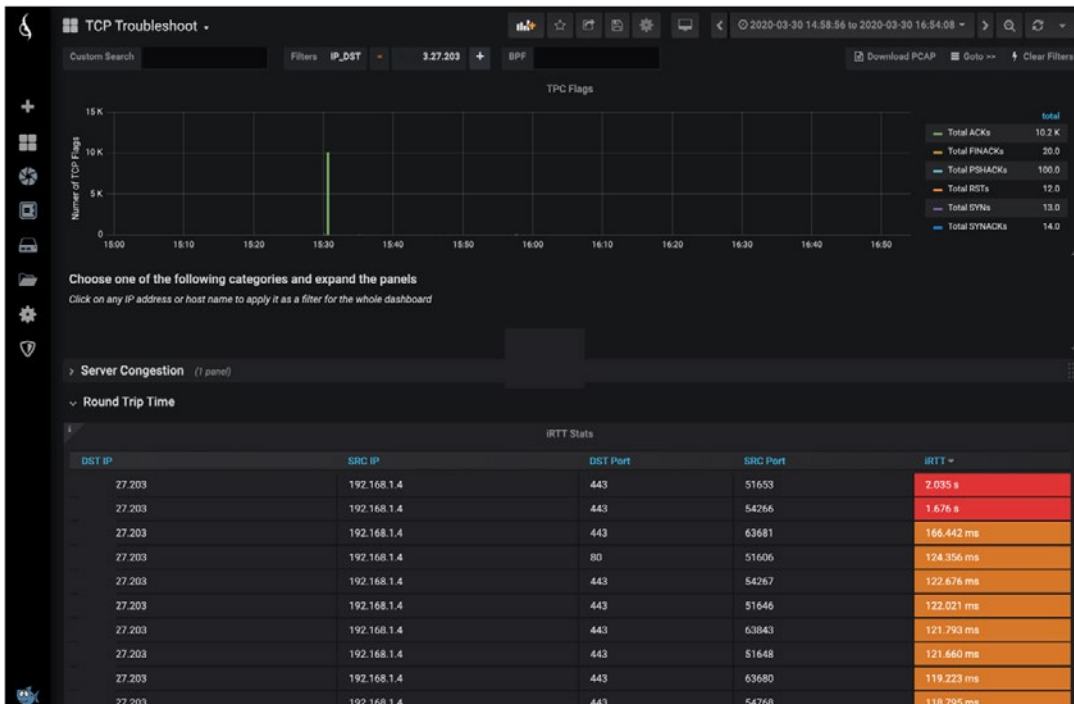
Step 2 - Checking server response times

Now that they had the right time frame, they needed to look at the health of the client conversations with the server. Using the User Experience – Application Latency dashboard, they could measure the application response time of the server, even though the traffic was encrypted. They noticed that the maximum latency of the server response time was 206 milliseconds. Comparing this to normal periods of performance, there was no significant change in this measurement. The server was responding like normal, even during the problem period.

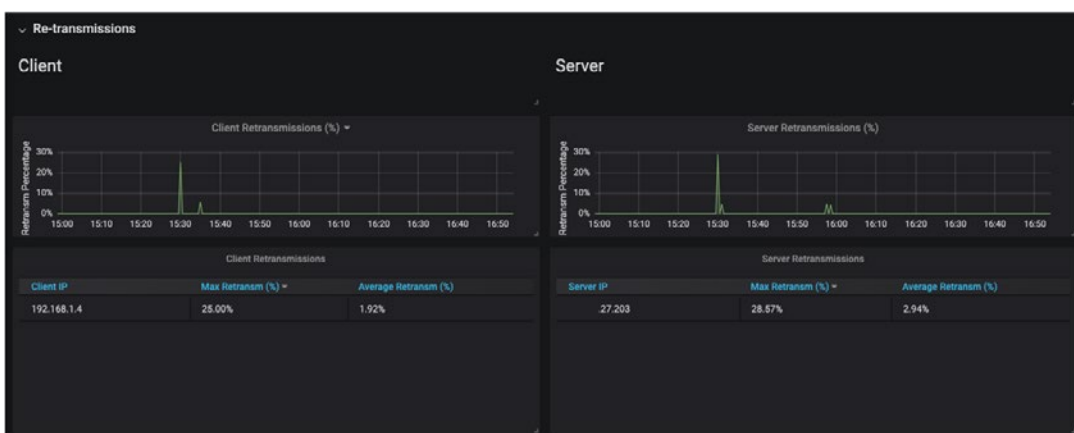
Step 3 - Troubleshooting TCP

Next, the engineers were able to look at the health of the traffic flow itself using the TCP Troubleshoot dashboard, setting a filter on traffic to and from the server IP.

This is where the problem could be seen. At certain points, the network roundtrip time between client and server would spike up to over two full seconds! The retransmission statistics also showed a high number of lost packets during this problem period.



Comparing this data with packet statistics during normal performance, the engineers could see that when the clients had a good experience, the network roundtrip time was low and there were no retransmissions.



This helped them to see that the network was dropping traffic and latency was high during the performance issue. Typically, this is caused by network congestion or an errored link.

What else could they do to track down the root cause?

Step 4 - Checking application bandwidth

During the problem period, the engineers were able to investigate the usage of the network for the network site overall. Using the Bandwidth dashboard set to the same timeframe as the performance problem, engineers were able to see a spike in the utilization of a specific application – Microsoft 365. This same activity happened at a previous time when the problem hit as well.



Within a few clicks, they were able to see which user was transferring so much data to 365 and how often it was happening. They saw that this spike of traffic was present for every client complaint of slow performance.

Conclusion

Using these dashboards pointed engineers to the leading symptom of the problem (packet loss and high latency, caused by network congestion) which steered them to the root cause (someone had accidentally configured their machine to do a full backup to Microsoft 365 every hour!)

The IOTA provided the right data, at the right time, with a simple workflow, allowing engineers to simply and remotely access the data they needed to resolve it.

**BRINGING CLARITY
INTO YOUR NETWORKS.
ANYTIME,
ANYWHERE.**



Profitap develops and manufactures hardware and software solutions that help you get complete access and visibility into your network. These network visibility solutions are designed with the security, forensics, deep packet capture and network & application performance monitoring sectors in mind.

Profitap network solutions help eliminate network downtime, add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7.

As we are experts in our field, we have developed our products to set new standards in an industry where the definition of excellence is constantly being challenged.


With more than 1,000 clients from 55 countries, Profitap has become a must-have solution or many important businesses, many of which are among Fortune 500 companies.

**PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS**

sales@profitap.com
www.profitap.com

 Profitap

 @Profitap

 profitap-international