CASE STUDY

Detect SIP Fraud

with ServicePilot

www.servicepilot.com
+1 (954) 446-9010
info@servicepilot.com

Note: Due to the nature of the information presented in this document, the client has asked that the data be anonymized.

CHALLENGE

One of our customers, a major European car manufacturer, uses SIP and Oracle SBCs to deliver high-quality VoIP service to its 80,000 employees.

Even though SIP is now used by many large companies, and considered as one of the most used VoIP signalisation protocols, it suffers from security loopholes which make them vulnerable to hackers.

Before starting to use ServicePilot, this customer had been the victim of several attacks, causing heavy financial losses (unusually high phone bills and indirect costs due to denials of service).

SOLUTION

ServicePilot's solution, aside from allowing the car manufacturer to better understand its infrastructure and troubleshoot service degradations faster, has helped it stop and prevent VoIP attacks.

1) Collecting SIP traffic using the SBCs

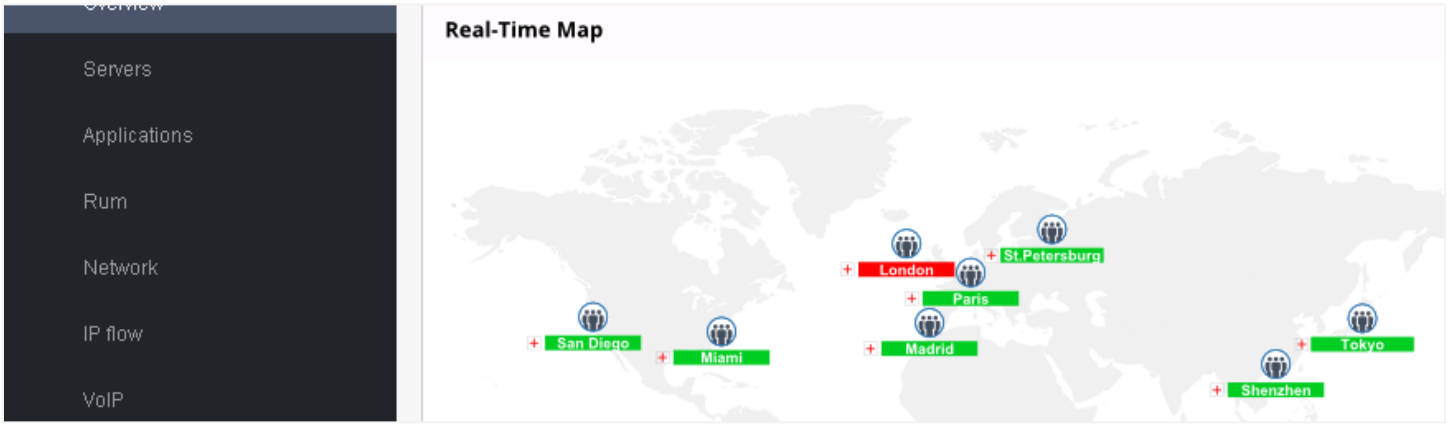
First, it is important to know that ServicePilot collects numerous indicators on the customer's entire infrastructure (Alcatel-Lucent, Cisco, Skype for Business, Oracle, and Sonus).

In particular, the client is able to collect CDR information on SBCs and PBXs concerning the volume of call placed.

2) Setting zones and custom alerts

Moreover, using ServicePilot's web interface the client was able to quickly create geographical zones in order to organize the display of collected data.

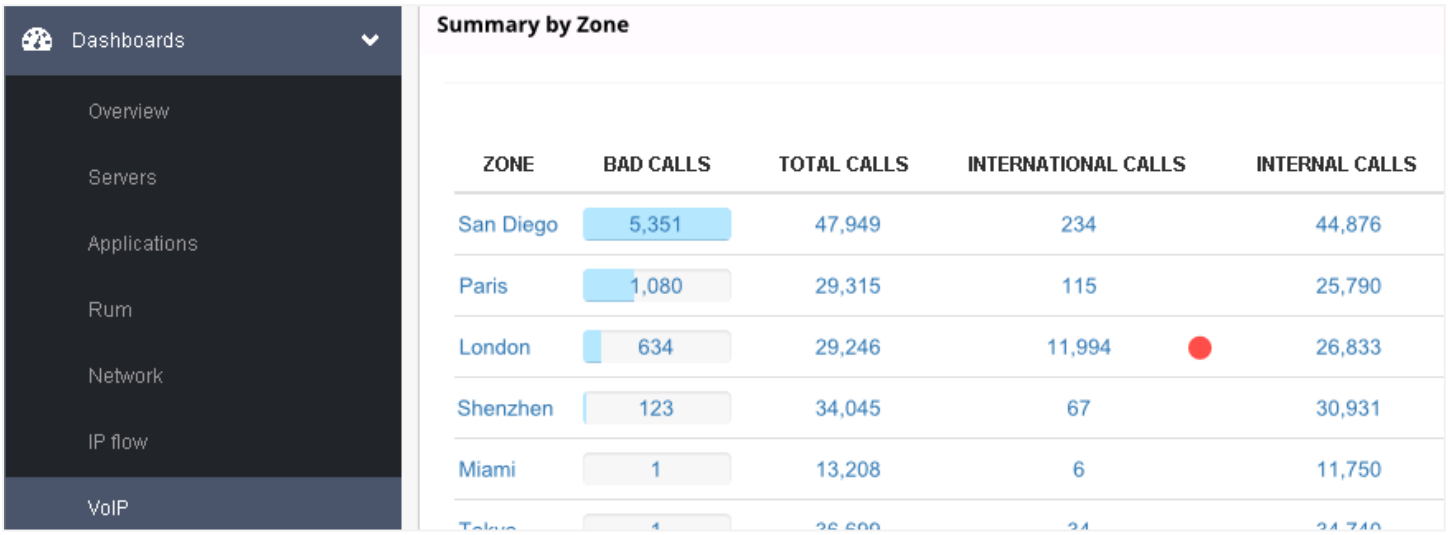
Additionally, new alerts were created, each with a custom threshold, in order to detect unusual traffic volumes.



3) Detecting attacks with custom alerts and dashboards

Soon after having deployed ServicePilot, the Voice team received an alert indicating that one of the SBCs was experiencing a sudden surge in traffic, exceeding the threshold that had initially been configured.

Using ServicePilot's dashboard they were able to identify an unusual increase in the number of outgoing international calls (see zone “London” below), as hundreds of international calls were being placed by an unusual IP, all from one of their Oracle SBCs.



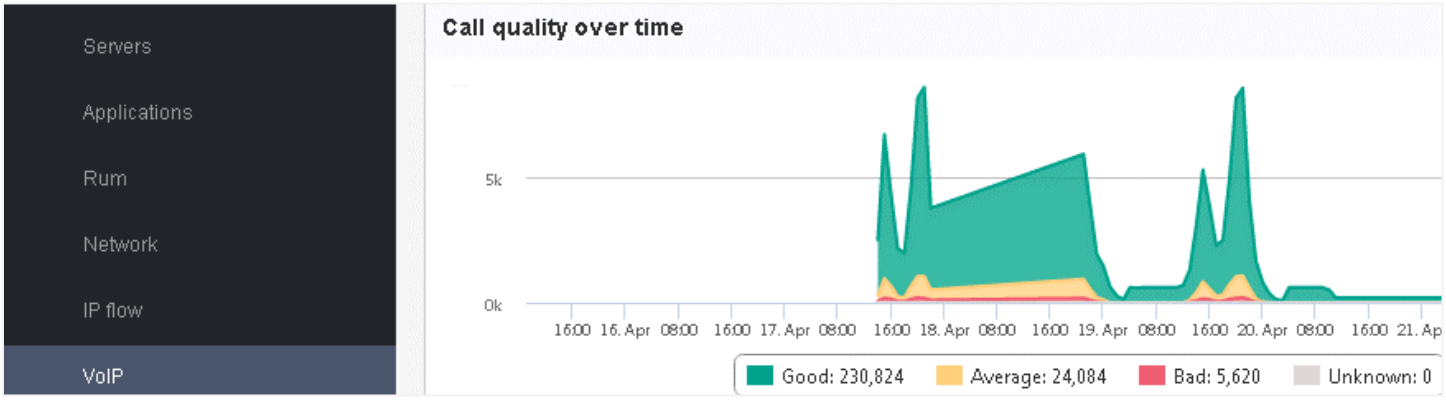
4) Stopping the attack and preventing future fraud

Having diagnosed the issue with precision, they were able to update their SBC configuration and block the hacker.

BENEFITS

By reacting quickly, this car manufacturer was able to:

- limit the financial impact of the attack as well as preventing future occurrences,
- avoid denials of service and maintain high-quality VoIP service for its users.



According to its Director of Telecommunications:

"ServicePilot's custom alerts and dashboards made it really easy for us to notice patterns caused by VoIP hackers. It also allowed us to avoid a very costly phone bill and many user complaints."

www.servicepilot.com
+1 (954) 446-9010
info@servicepilot.com