

Customer



Area of Activity

Financial services

Challenges

- ▶ Absence of tools for a detailed overview of what is happening in the network
- ▶ Solution using the existing Cisco Nexus 7000 devices
- ▶ Saving statistics at min. one month
- ▶ Automatic anomaly detection

Benefits of the solution

- ▶ More effective management and network monitoring
- ▶ Increasing the security of computer networks
- ▶ Recording statistics to the 2TB virtual collector

Deployed products

- ▶ Flowmon Collector VA
- ▶ Flowmon ADS Business

In cooperation with



U Plynárny 1002/97
101 00 Praha 10
Česká republika

www.alefnula.cz
sales@alef.com

About the company

Raiffeisenbank is one of the largest and most important banks on the Czech market. It offers a wide range of services both in the area of personal finance and corporate finance. It takes pride primarily on the quality of services and professional approach to clients. In 2008 it was declared to be the best bank in the Czech Republic.

Requirements from the IT department of Raiffeisenbank

Raiffeisenbank faced the problem of monitoring data flows in its data centres. This problem lay in a missing tool for a detailed overview of what was happening in the network at the level of communications. The customer required a solution involving the use of existing devices in the network and their supported protocols. For collecting and evaluating information it was possible to use the virtualized data centre and thus the gained computing performance. The requirement for storage of statistics about all communications was minimally one month. Among other requirements there was the ability to automatically detect and track anomalies in traffic and consequently alert these anomalies.

Solution

The ALEF NULA company, in cooperation with Flowmon Networks, designed a solution that uses the NetFlow protocol running on the existing network elements Cisco Nexus 7000. They used protocol NetFlow version 9 and the existing preconfigured templates for IPv4 traffic. The selected L2 VLAN networks were configured with monitoring traffic towards the entry of data into the L2 VLAN.

All traffic information is sent to Flowmon collector with a capacity of 2TB, which is deployed in a virtual data centre environment. Flowmon collector stores, displays and analyses network statistics in the NetFlow format and provides users with detailed information about network communications and their progress. In addition to the basic module for analysing the data collected, the collector has been extended with the module Flowmon ADS (Anomaly Detection System) in the option Business, which over the data network performs the automatic detection of anomalies in the network and warns of any suspicious activity and network communications. Therefore the deployed solution serves not only to increase the security of the computer network and the detection of security anomalies, but also to detect operational problems and network events.

Customer quote

Jan Krtička, head of network infrastructure in Raiffeisenbank, states:

"In such a sensitive environment, like a bank's data network, you need to have control over of the security threats, data flows, and anomalies. It is Flowmon which brought us this control and greater safety. In the configuration with an existing Cisco infrastructure and computing power in data centres we have gained a cost-effective solution that allows us a detailed overview of network operations, the possibility of reverse engineering and streamlining administration. Flowmon ADS is also a benefit that allows the detection of incidents and threats, detection of infected workstations and operating problems."