Ensure Security across Entire Network using Software Defined Networking

Document Purpose

The number of cyber threats is growing constantly. They have become more sophisticated, precisely targeted and can overcome traditional security solutions for the data network perimeter. If these attacks break the security mechanisms, they can easily infiltrate the internal network of organizations, leaving limited options for defence. They usually target sensitive data, systems or specific individuals with the aim of stealing intellectual property or even secret information of corporate and government institutions. By doing this, attackers may gain an unfair competitive advantage in both commercial and public sectors.

This document describes:

- The key challenges in today's complex network infrastructures.
- The architecture of Allied Telesis and Flowmon Networks combined solution for security in SDN environments.
- The major benefits of the joint solution.

Challenge

Increased complexity due to the rising number of devices, inconsistent policies across networks or the inability to scale-out according to current business needs are the biggest challenges for traditional networks. Software Defined Networking addresses these challenges and brings the same agility that abstraction and virtualization have brought to server infrastructure.

Modern cyber threats are a serious risk to the assets of every organization. Network Behavior Analysis allows a way to detect such threats, undesirable network communication and other traffic anomalies which cannot be detected by traditional solutions deployed on the network perimeter or end points. Combining Network Behavior Analysis and Software Defined Networking technologies enables a way to protect even the largest network infrastructures and organizations.

Solution Architecture

The integrated solution architecture consists of **Flowmon ADS** (Anomaly Detection System) for network anomaly detection based on flow data (NetFlow, IPFIX or other compatible) and Network Behavior Analysis and **Allied Telesis SES** (Secure Enterprise SDN) solution for the dynamical determination of access policies across the whole network architecture based on detected network events (anomalies).

The joint solution for addressing security challenges in Software Defined Networking combines the following features:

- **Flow data export** from **Flowmon Probes** to provide visibility into network traffic. Probes connected to TAP or SPAN/mirror ports generate flow statistics from all communications in the network and exports them to Flowmon Collector.
- **Flowmon Collector** with module **Flowmon ADS** stores, processes, analyses and reports network traffic information. Network Behavior Analysis technology of Flowmon ADS allows a way to detect undesirable network communication, traffic anomalies and other operational and security incidents. Script triggering or sending a syslog message upon event detection and REST API allows a way to integrate with third party solutions like Allied Telesis SES SDN controller and to provide it with detailed information about security incidents and to configure and enforce network policies.
- **Allied Telesis SES** SDN controller for centralized automation of policy-based application profiles. The controller automates the deployment and compliance checking of network policies across the entire network. Highly programmable open APIs allow a way for integrating with third-party solutions like Flowmon ADS and to create innovative network services and applications to fuel business growth.

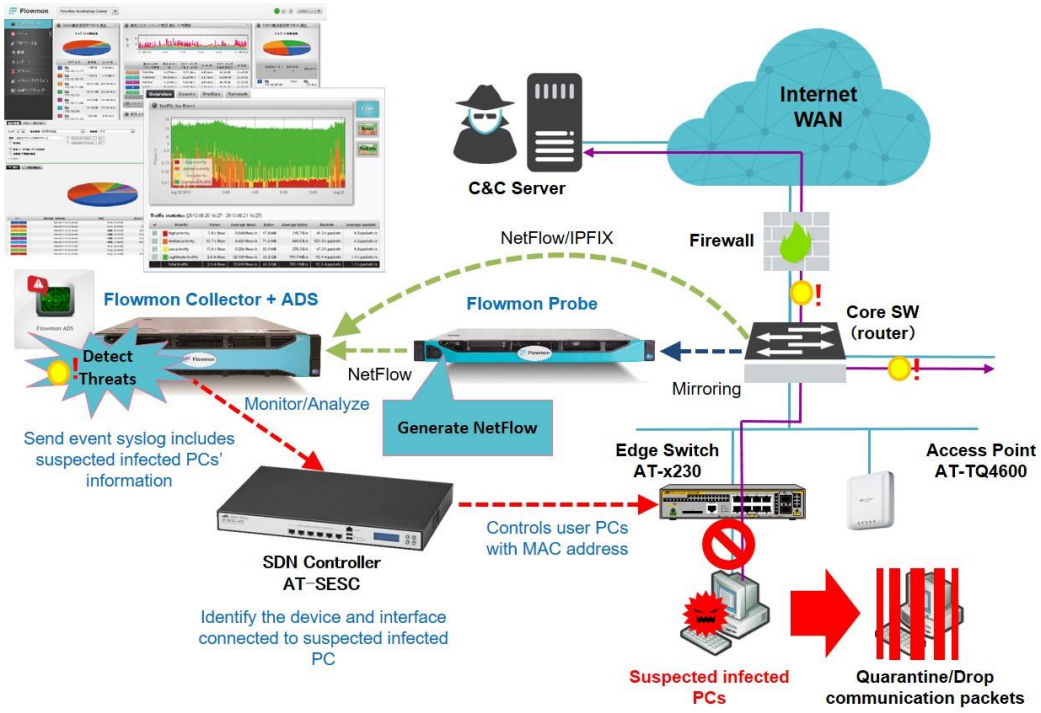

Figure 1: Integration architecture.

Flowmon ADS detects anomalies in network traffic and reports every detected security threat. Upon detection, Flowmon ADS sends information about malicious hosts to Allied Telesis SES. Using the provided information, Allied Telesis SES sets up a new access policy to reconfigure the SDN switch to which the malicious host is connected. Based on the policy, the host can be disconnected from the network, moved to quarantine, etc.

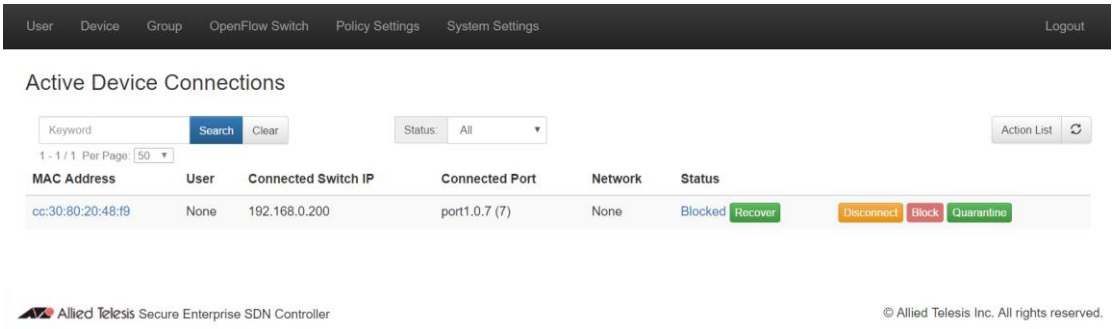

Figure 2: Infected host is blocked from the network.

The network / security operator is notified by an alert from Flowmon ADS and can analyse attack details to get more information about the attacker and its victims. From event details in Flowmon ADS, the operator immediately sees detailed information about the attack and also each individual flows on which the event was detected.

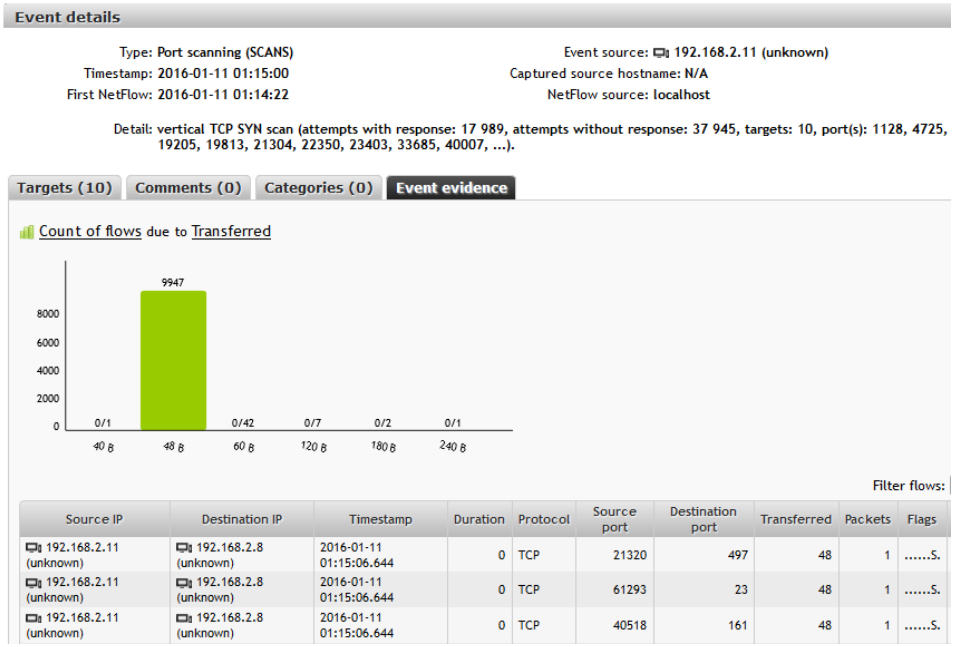

Figure 3: Event details in Flowmon ADS.

Solution Benefits

The joint solution aims to provide a detailed insight into an internal network, to detect operational and security incidents in the network and to troubleshoot network issues and reactively protect the network infrastructure against cyber threats and network attacks. The major benefits of the solution are:

- Active protection against cyber threats and network attacks using and applying policies across entire network infrastructure.
- Saves significant investments in scripting language or tools that can automate configuration changes.
- Eliminates time needed to discover and troubleshoot incorrect manual entries for a given device.
- Operational-security incidents can be processed without the need of manual reconfiguration of network access points.

For More Information

For more information, contact your Allied Telesis or Flowmon Networks partner.

Allied Telesis K.K.

2nd TOC Bldg. 7-21-11 Nishi-Gotanda,

Shinagawa-ku, Tokyo 141-0031,

Japan

www.allied-telesis.co.jp (Global site: www.alliedtelesis.com)

Flowmon Networks a.s.

Sochorova 3232/34

616 00 Brno

Czech Republic

www.flowmon.com