White Paper

Practical Application of Software-Defined Networking (SDN) in Enterprise Networks

Drivers for change in enterprise networks

Enterprise businesses know they need dependable data networks in order to function. A high-performing, reliable network is a necessary cost of doing business these days. For enterprises, a reliable network is as necessary as plumbing. Just like the plumbing, they expect the network to work well, and not cause problems—and the less it costs them, the better.

Before any enterprise business adopts Software-Defined Networking (SDN), they need assurance that the technology is well-proven, low risk, and will help them achieve their primary business goals.

What sort of SDN solution would appeal to a typical, cost-conscious enterprise?

Agility and rapid service provisioning are not key requirements because enterprise networks are not dynamic—once they are installed, they do not change much. Similarly, better link utilization is not a high priority, because if more bandwidth is required the business can simply install it.

However, end-user management can be a major cost as users come and go. Security concerns are present at all times. Users are constantly looking to use new applications, in increasingly more flexible ways.

Enterprises need wired and wireless equipment to provide connectivity for their users, and want to minimize capital expenditure (Capex) and operational expenditure (Opex) invested into this infrastructure. At the same time, they must provide their users with security, reliable connectivity and high performance.

The benefits that enterprise businesses want to achieve are:

1. Improved security
2. Reduced operational costs
3. A better user experience

The next sections explore how SDN can deliver these benefits.

What can SDN deliver to the Enterprise?

1. Improved security

Moving to SDN can deliver security solutions that react immediately to threats right at their source, and can automate user access control and quarantining.

The combination of effective internal network traffic analysis, with direct software control of both the wired and wireless access layers of the network, enables rapid threat detection and immediate threat quarantining, by disconnecting network access at the threat's source on a packet by packet basis.

2. Reduced operating costs

Reducing the operational costs of an enterprise network results from achieving things like:

- facilitating user onboarding
- applying business rules consistently from centralized apps
- simplifying troubleshooting

Bring Your Own Device (BYOD) and "Choose Your Own" programs have resulted in an increasingly mobile workforce, with greater flexibility in choices of user equipment. Achieving the centralized management of user and device identity has become a key challenge in Enterprise networking. When user and equipment databases are combined with user access policy rules, and the resulting information is automatically translated into operational instructions for the network infrastructure, the results include major efficiency improvements, cost savings, and better network security and performance.

3. A better user experience

Users need a network that supports their work and allows them to:

- Enjoy greater mobility, and access business data and applications from anywhere.
- Use the devices that suit them best.
- Access a greater range of applications.
- Combine a variety of communication methods at once, I.e. voice, video and data—with high quality.

Customizing the network to its users' needs is a challenge that can be much more easily met when there is centralized software control of the network.

Allied Telesis SDN initiatives in the Enterprise

Allied Telesis have taken a two-step approach to addressing the need for SDN:

1. Unifying and simplifying the management plane
2. Achieving programmability of the control plane

1. Unifying and simplifying the management plane

Allied Telesis began by focusing on the most pressing need for customers—simplifying management by unifying the management plane—and developed a product called Allied Telesis Autonomous Management Framework™ (AMF). Hundreds of networks worldwide are now enjoying the benefits of AMF's simplified network management, and businesses are reporting cost reductions of over 60% as a result.

2. Achieving programmability of the control plane

Next, Allied Telesis addressed the need for the control plane to be programmable. A simple software upgrade for existing switch products now enables them for OpenFlow v1.3. These products then operate in hybrid mode, allowing customers to choose how quickly they adopt OpenFlow in their network.

Recognizing that enterprise businesses need a combination of wired and wireless access, OpenFlow support is also available on Allied Telesis Wi-Fi Access Points (APs) so customers can gain the benefits of SDN solutions across their entire infrastructure.

In the future, OpenFlow support will be extended across other product lines, such as firewalls, to enable customers to have programmatic control of their WAN gateway infrastructure.

An integrated SDN solution for the Enterprise

Allied Telesis have combined with leading technology partners to develop a new range of SDN solutions, called Secure Enterprise SDN (SES). These deliver the key benefits that Enterprise customers seek.

Secure Enterprise SDN (SES) solution

SES delivers three compelling benefits:

1. Easy user onboarding
2. Easy endpoint security
3. Easy traffic monitoring

1. Easy user onboarding

SES links HR events and user devices to network access policies, via an HR workflow system. This is ideal for mobile workforces in locations such as hospitals, schools, universities, and more.

2. Easy endpoint security

If a user attempts to connect with a device using an old OS version or banned application, the device is forced into quarantine or directed to an update site. This provides a safe network environment, by providing:

- A highly responsive NAC to prevent internal threats.
- Rapid detection, and nullifying, of worms and Trojans.
- Control over which sites and apps can be accessed.

3. Easy traffic monitoring

Network flows from user devices are monitored, looking for suspicious activity and taking preventative action when required. The protection afforded by this is applicable to ANY network device, including MachineToMachine (M2M) equipment, which is useful for hospitals, manufacturing, Smart City infrastructure, and much more.

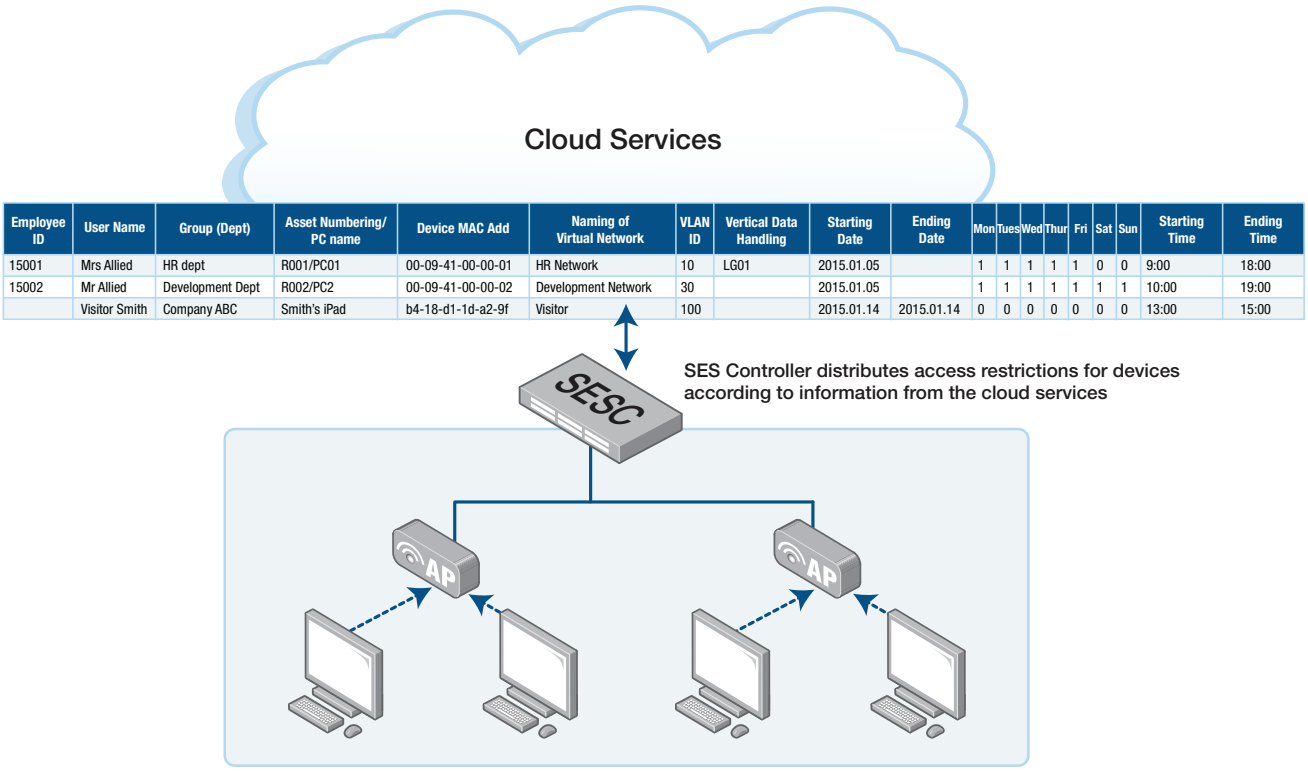
SES user onboarding

As a user enters the business, their details are entered into a cloud-based HR database:

- Location
- Department
- Device address(es)
- Work schedule

The SDN controller can apply business rules—for example departmental access permissions, degree of mobility, expected hours of access, and so on—to the user information, in order to derive access rules to apply to the edge switches and Wi-Fi APs.

User onboarding

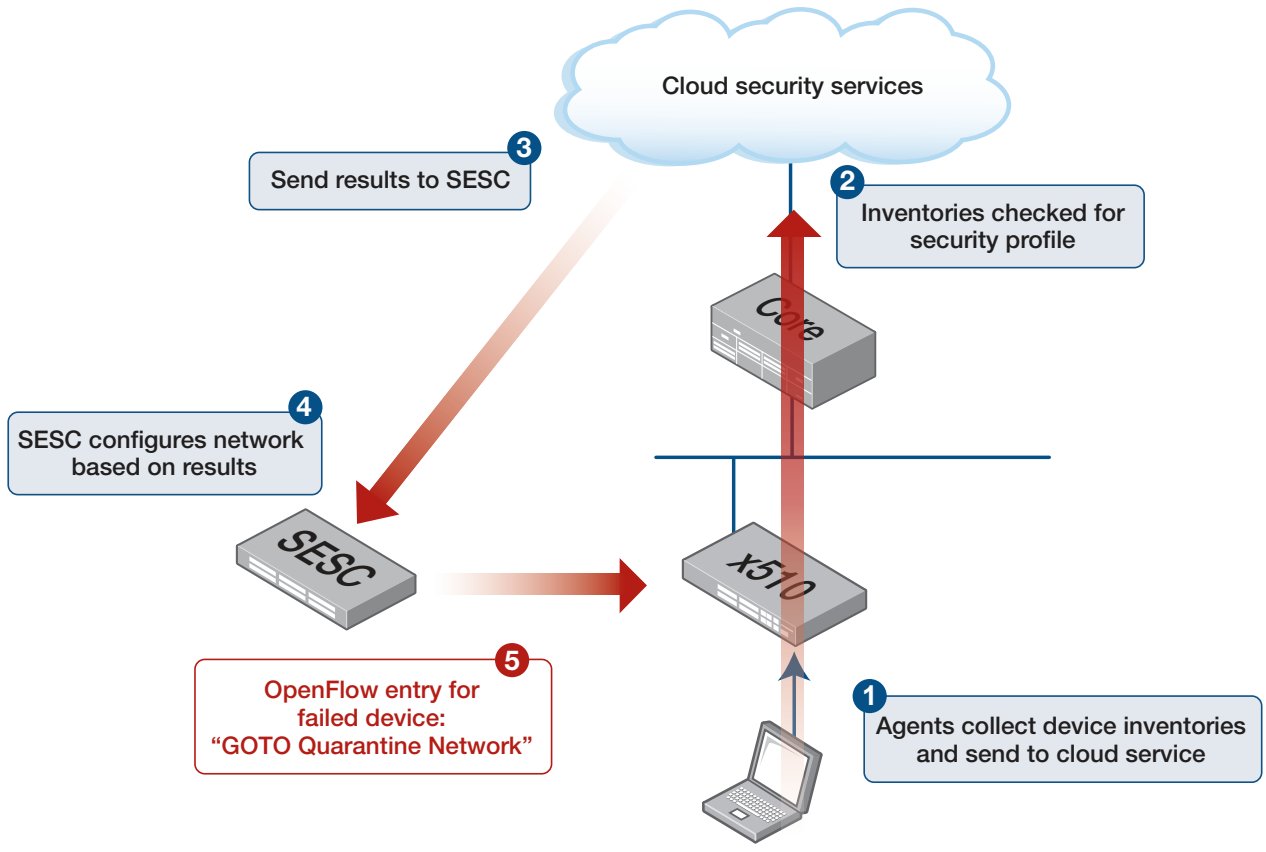


Employee ID	User Name	Group (Dept)	Asset Numbering/ PC name	Device MAC Add	Naming of Virtual Network	VLAN ID	Vertical Data Handling	Starting Date	Ending Date	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Starting Time	Ending Time
15001	Mrs Allied	HR dept	R001/PC01	00-09-41-00-00-01	HR Network	10	LG01	2015.01.05		1	1	1	1	1	0	0	9:00	18:00
15002	Mr Allied	Development Dept	R002/PC2	00-09-41-00-00-02	Development Network	30		2015.01.05		1	1	1	1	1	1	1	10:00	19:00
	Visitor Smith	Company ABC	Smith's iPad	b4-18-d1-1d-a2-9f	Visitor	100		2015.01.14	2015.01.14	0	0	0	0	0	0	0	13:00	15:00

SES–easy endpoint security: checking device status

Local agents collect device information and send to cloud service to check for vulnerabilities. The results of those checks are sent to the SDN Controller through published Application Program Interfaces (APIs). The SDN Controller instructs OpenFlow switches to direct vulnerable devices to a Quarantine Network

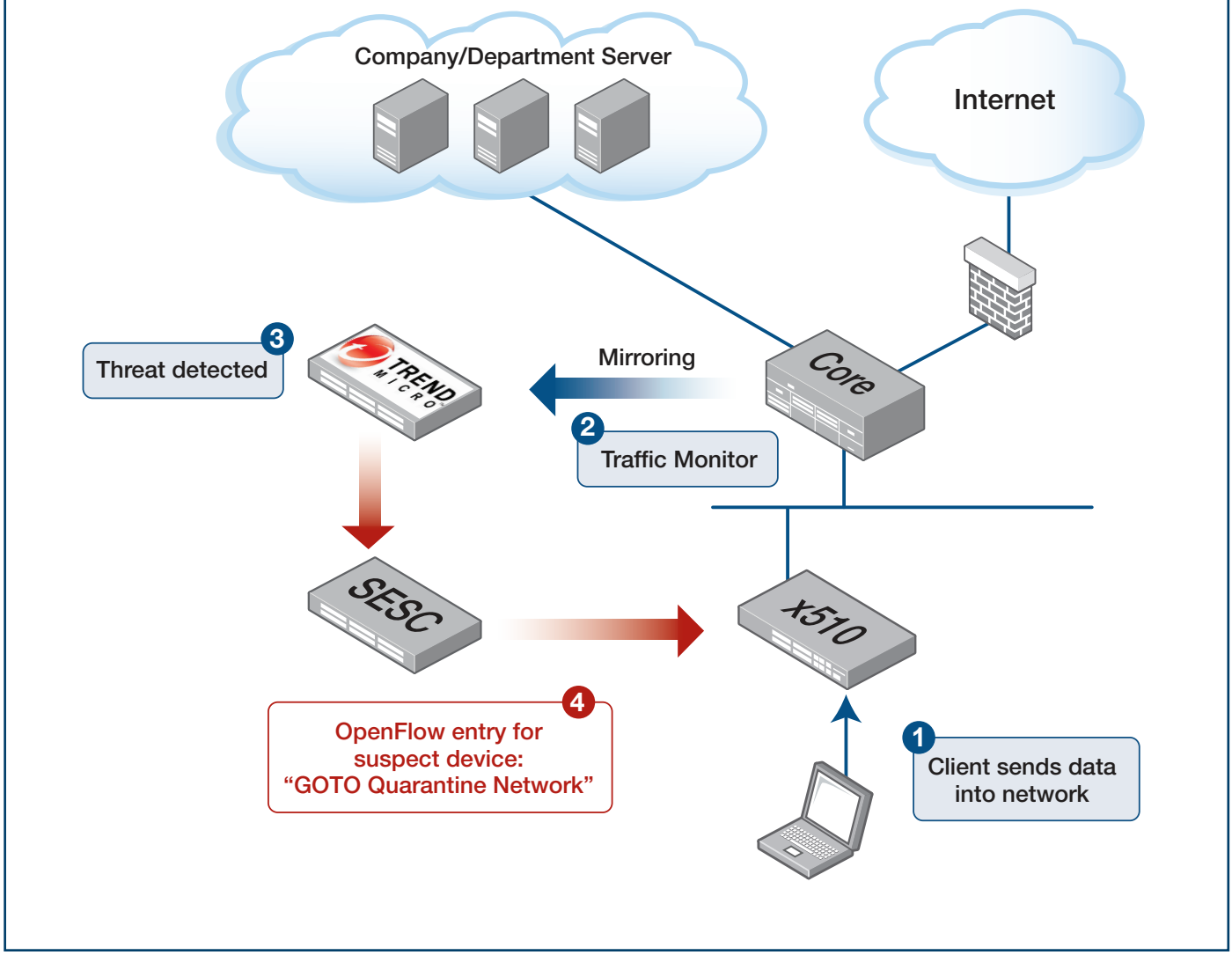
Checking device status



SES—easy endpoint security: detecting suspicious traffic

A core switch mirrors traffic to the Trend Micro Deep Discovery platform, which checks this internal traffic for threats. If threats are found, the SDN Controller is advised via an API and network configuration is dynamically changed. OpenFlow switches block "Suspected Threat" user devices, or isolate them into a quarantine network.

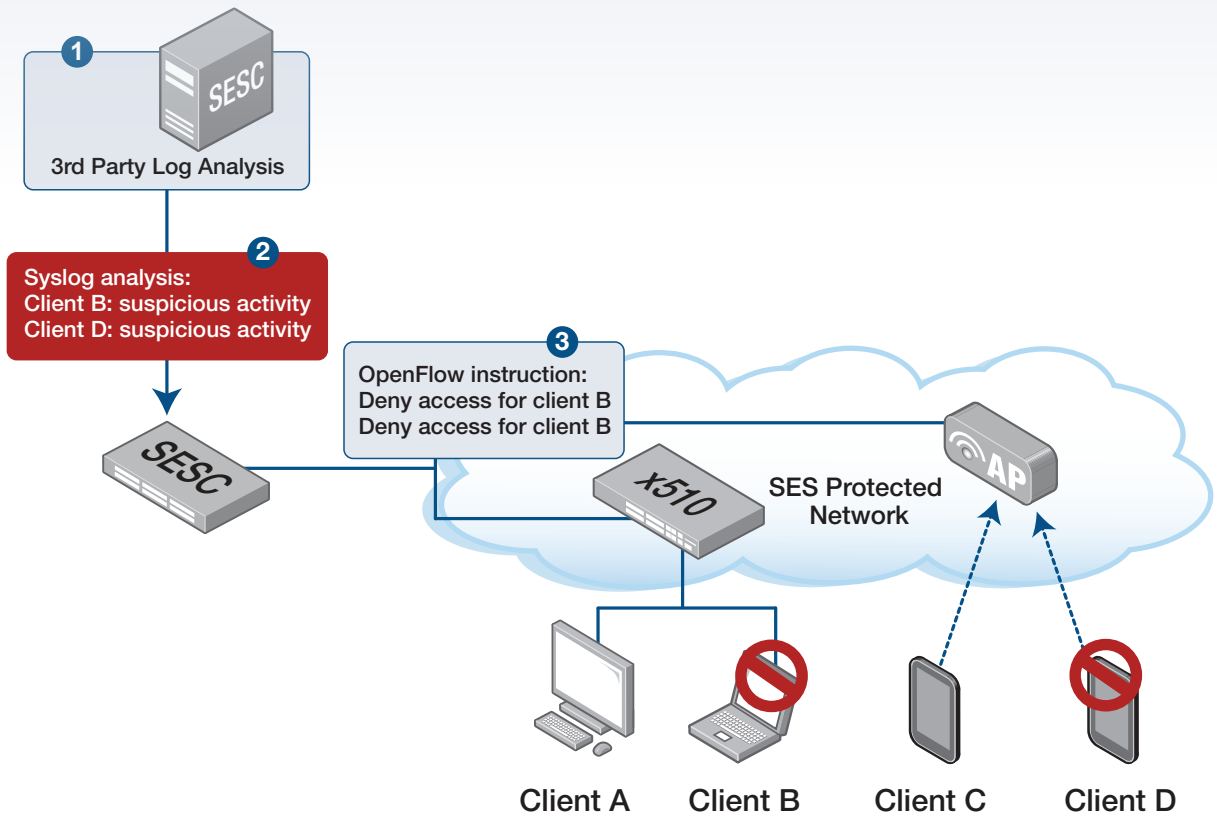
Detecting suspicious traffic



SES–easy traffic monitoring

A Syslog Interpreter can provide a way for 3rd party applications to integrate with SES. For example, a Security application supplier can identify suspicious client behavior by analyzing the network logs. Upon detecting such behavior, the application can inform the SDN Controller to block certain user devices.

Log analysis



Summary

The drivers for introducing SDN into enterprise networks are quite distinct from the drivers for introducing SDN into data centers.

Allied Telesis understands the needs of enterprise networks extremely well, and have been introducing SDN into the Enterprise market in a manner that addresses that market's needs.

The Secure Enterprise SDN solution is the practical application of SDN to the Enterprise network in a way that delivers significant benefits.

C613-08034-00 RevB