# Wedge Networks: Transparent Service Insertion in SDNs Using OpenFlow


EXECUTIVE SUMMARY

In this paper, we will describe a novel way to insert Wedge Network's multiple content security services (such as Anti-Virus, Anti-Spam, Web Filtering, Data Loss Prevention, Advanced Persistent Threats and Mobile Security) into an existing SDN network with minimal operational impact while providing maximum security. Using SDN and OpenFlow, we show how traffic can be dynamically steered towards a transparent malware detection platform, allowing non-intrusive insertion of security services within a cloud service provider or enterprise datacenter.


The SDN method has advantages over traditional methods using WCCP, policy-based routing, direct insertion or proxies. In particular, the value for cloud providers and datacenter are that this novel method is:

- Transparent: Non-intrusive insertion of value-added security services
- Efficient and high-performance: Ability to pick up only relevant flows to direct to the platform while leaving other flows untouched, and using high-performance switches with fast fabrics means no unnecessary load on routers (compared to WCCP and PBR)
- Dynamic and flexible: Service providers can dynamically decide which flows to direct to the platform and reconfigure on the fly as required on a per customer basis

SDN provides a new way for cloud service providers and enterprise data centers to insert valuable services into the data stream. As an innovative provider of L4-7 security services, Wedge Networks has demonstrated a viable technique of transparent service insertion using SDN and OpenFlow that service providers and enterprise infrastructure teams should consider.

## Introduction

With today's business requirements for security and flexibility while maintaining reliability and transparency, CISOs are looking for ways to improve their security capabilities without impacting user productivity or adding unnecessary complexity to their network. The constantly increasing number of malware attacks, spam, and phishing activities has organizations and service providers scrambling to find ways to secure their networks. Historically, adding security services into a user network required downtime to orchestrate a topology change while the network was reconfigured, a new security appliance inserted, and multiple content security services turned on and debugged. However, with the advent of software-defined networking (SDN) and OpenFlow-enabled switches, there is now a better way.

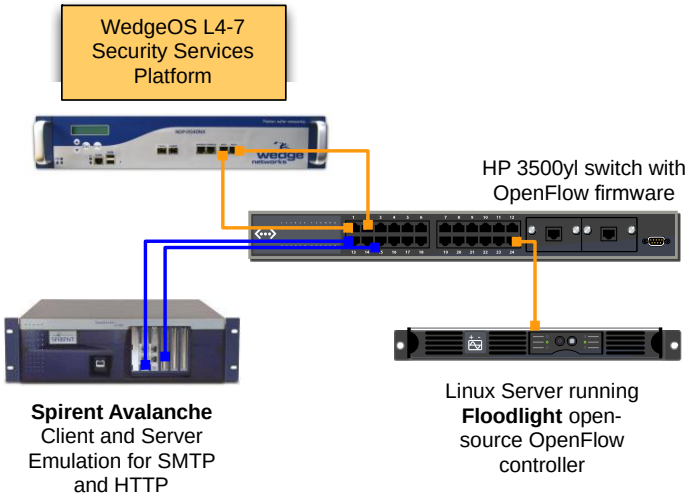
Specifically, we will be using OpenFlow to pick out specific services and direct them transparently in a manner that does not impact the underlying network, without the need to re-cable the physical network

## Setup

The setup consists of an OpenFlow-enabled switch, a WedgeOS platform with Anti-Spam and Anti-Virus modules running and configured to listen to HTTP, HTTPS, POP3 and SMTP service ports. For our lab setup, we have chosen to use the HP 3500yl switch, with OpenFlow firmware dated February 2012. There are multiple other providers of OpenFlow-enabled switches as well including Juniper, Brocade, IBM, NEC and Pica8. The techniques used in this setup will work with any OpenFlow 1.0-compliant switch.

For traffic generation, we used Spirent's Avalanche L4-7 traffic generation product as both client and server, acting as source and sink for TCP service ports 80, 110 and 25 representing HTTP, POP3 and SMTP.

The following shows the topology of the setup:

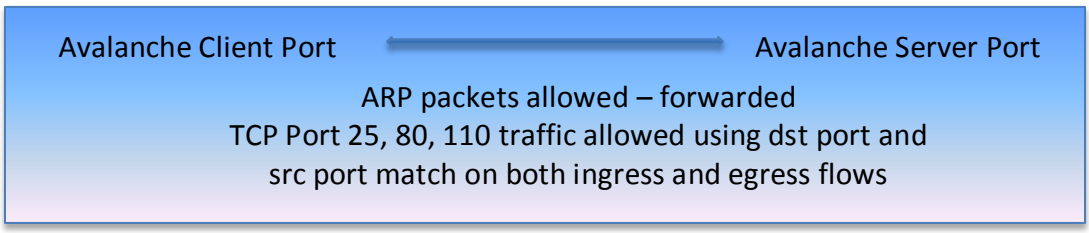



The HP switch was connected to a server running the open-source Floodlight controller, and the rules were configured via scripts calling the RESTful interface on the Floodlight controller.

We inserted the appropriate flow rules to allow the testbed baseline traffic to be run:

- Flows to allow ARP requests and responses to pass between the appropriate ports that need to communicate. Initially, this was between switch ports connected to the client interface and server interface of the Avalanche.

- Allowed specific flows on the appropriate TCP ports 80, 110 and 25 to be forwarded from the client interface of the Avalanche to the server interface, setting up bi-directional flows using TCP destination and source port matches.

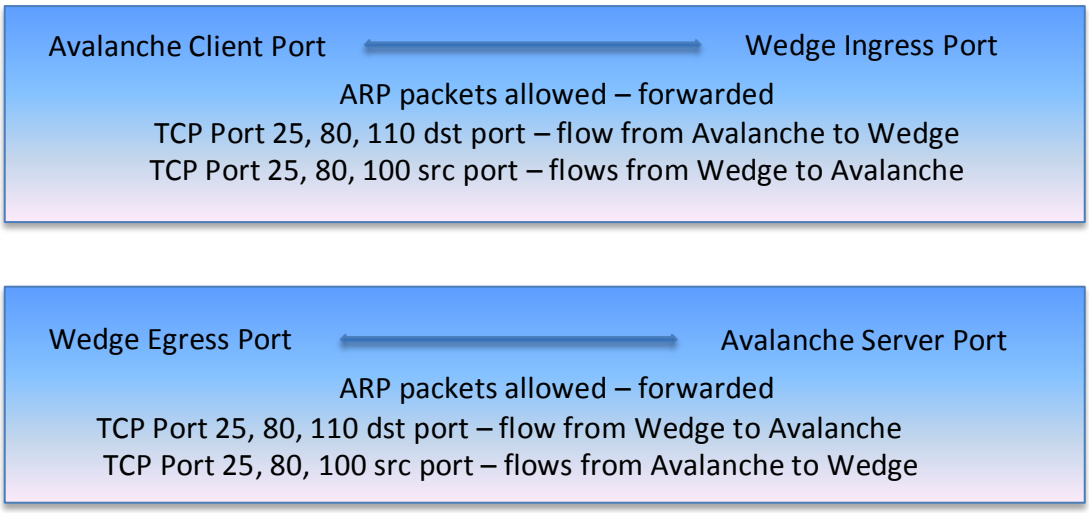



## Transparent Service Insertion

Once traffic was flowing smoothly between the Avalanche client and server ports, simulating a regular datacenter network, we invoked a set of scripts that triggered the service insertion of the WedgeOS platform to inspect port 80, 110 and port 25 traffic. The WedgeOS platform was placed in transparent mode to provide minimal impact to the data stream.

To achieve the service insertion, the scripts performed the following steps via the OpenFlow controller:

- ARP flows were redirected via the WedgeOS platform. We replaced the previous ARP flows with two pairs of new flows: one between the client interface of the Avalanche and ingress interface of the Wedge appliance and another between the egress interface of the Wedge appliance and the server interface of the Avalanche
- TCP port matching rules for ports 80 and 25 were pushed down to the switch, redirecting incoming flows destined for TCP ports 80 and 25 to the WedgeOS platform ingress port, and directed the same flows out of the egress port to the Avalanche server interface
- A set of return flows (with TCP source ports 80 and 25) were configured from the Avalanche server interface, through the WedgeOS egress port first, then the ingress port back to the Avalanche client




## Results

There was no perceptible negative impact, latency or otherwise, on the traffic flows on ports 80 and 25 when the WedgeOS platform was inserted to inspect the traffic. The flows continued seamlessly while the WedgeOS inspected traffic on ports 80 and 25—as evidenced by live statistics on the WedgeOS Web GUI.

This technique can be extended to directly select TCP flows into any type of transparent service infrastructure to perform security scanning and monitoring services. If large payloads were involved with executable content, there could possibly be latency introduced due to scanning services, but the key value-add of this approach is complete transparency to the data streams.

## Benefits of the SDN Approach

Today's conventional deployments of network-based security services fall into several categories:

- **In-line, hard-wired transparent bridge**: requires direct physical connections, inflexible and forces all protocols to run through the device regardless of whether they are being scanned or not. Trying to scale requires load-balancing techniques that are complicated if not all together impossible in practical deployments.
- **Pre-configured explicit proxy**: requires configuration changes, non-transparent and does not allow quick insertion or removal of the L4-7 services. Tends to be very hard to manage.
- **WCCP**: requires edge routers to support WCCP and expensive hardware that can do this without performance or data stream impact
- **Policy based routing (PBR):** requires careful consideration of return path to prevent asymmetric routing loops, and assignment of a dedicated layer 3 subnet for the platforms running the service. Can also degrade performance on routers with additional compute.

The SDN approach described and tested successfully above demonstrates that using OpenFlow to insert L4-7 services can achieve the following benefits:

- **Transparency**: this approach does not require any kind of pre-configuration and can be turned on and off at will. Value-add L4-7 services can be inserted with minimal to no impact on existing topology and live data streams.
- **Efficiency and performance**: this technique provides fine-grained controls to pick up only relevant flows to direct to the services platform while leaving other flows untouched. It saves on the services platform having to process unnecessary data and the same technique can also be used to load-balance and direct specific flows to different services platforms. This allows for service differentiation and scaling much better than any traditional method. Furthermore, because OpenFlow switches have high switching bandwidth at low costs, serving even 10s of Gigabits of traffic will not present a problem.
- **Flexibility and dynamism**: the approach allows the service provider to dynamically decide which flows to direct to the platform and reconfigure on the fly. The flexibility could allow for self-service purchase of value-add services, with automated provisioning that can safely and quickly insert new services on-the-fly into production networks.

In summary, SDN provides a new way for cloud service providers and enterprise data centers to insert valuable content security services such as Data Loss Prevention and mobile security in addition to the mainstays such as Anti-Virus, Anti-Spam and Web Filtering that Wedge Networks provides into the data stream. Wedge Networks has demonstrated in this innovative testbed setup that the SDN method can be transparent, efficient and highly agile and dynamic compared to existing deployment topologies. Service providers and enterprise IT infrastructure teams considering deploying new architectures within their datacenters and edge networks should evaluate an SDN-based solution around the architecture we have proven in this testbed.

## About Wedge

Wedge Networks is the leader in real-time Content Security and Compliance solutions for enterprises and service providers. Our patented WedgeOS platform provides the next generation security infrastructure to detect, protect against, and control threats, information leaks, and allows future security functions to run on the network. At its core is our Deep Content Inspection technology, which moves beyond the application layer to allow full access to all content passing through the network in real time. It uniquely provides the most depth in scanning without compromising performance, loading clients, and remaining completely transparent to network traffic. Software systems and hardware appliances running on WedgeOS are deployed globally, delivering security protection for tens of millions of users in Fortune 500 companies, government agencies, internet service providers, and across all industry verticals. For more information, visit www.wedgenetworks.com.