ADVANCED SECURITY MECHANISMS TO PROTECT ASSETS AND NETWORKS: SOFTWARE-DEFINED SECURITY

One of the largest concerns of organisations is how to implement and introduce advanced security mechanisms to protect their assets and networks. This document aims to provide an overview of how an organisation can leverage the emerging technologies of Software Defined Networking (SDN) and Network Functions Virtualisation (NFV) for implementing security, as opposed to using traditional methods, and outlines some of the benefits that can be realised.

INTRODUCTION

Organisations today are evolving and rapidly adopting new technologies in order to offer more flexibility to their employees, such as connectivity and accessibility to corporate resources from anywhere and at any time, as well as new services to their customers, such as self-provisioning of services through portals, e-commerce applications and many more. This has led to redefining the organisational boundaries, but has also increased the risks and the threat footprint of the organisation. In particular, the last couple of years we have seen a huge increase in Distributed Denial of Service (DDoS) and Malware attacks. In order for an organisation to be able to protect their resources and mitigate the risks, it has been necessary to deploy solutions that would protect the network from such attacks. In addition to these trends, the evolution of networking technologies has introduced concepts such as SDN, which decouples the network control and forwarding functions, enabling the network to become directly programmable and the underlying infrastructure to be abstracted for upper layer applications, and NFV, which is allowing for the virtualisation of network functions, that were previously deployed in proprietary vendor hardware appliances, on commodity hardware equipment. These advancements can enable organisations to implement security solutions in a different way and maximise efficiency, whilst minimising cost. The following sections aim to provide an overview of the implementation and architecture differences when deploying an Anti-DDoS or Anti-Malware solution.

TRADITIONAL SECURITY ARCHITECTURE. Today's approach to implementing security in an organisation has been firstly to identify the potential threat (i.e. DDoS or Malware attacks), then assess the risk by calculating the likelihood of the threat and the impact to the business and lastly define a security solution or control mechanism that can be put in place, in order to detect and mitigate the attack when it happens.

In the scenario that an organisation wants to deploy a solution for protecting its network and resources from a DDoS attack or to quarantine an infected host by a malware the following components will need to be deployed:

- A mechanism (i.e. Netflow, anti-malware software) or an appliance (i.e. IPS/IDS), which allows for traffic monitoring and detection of anomalous traffic
- A security application, usually running in vendor specific hardware appliances, for DDoS detection and another for automated malware detection
- A mitigation software or appliance, to clean the traffic or to block the infected host

Usually the mitigation of the attack has to take place at the mitigation software or appliance, which most of the times is deployed in central points of the infrastructure. This results to introduction of delays and latency, due to the fact that the traffic has to be diverted from the original traffic path, to be cleaned and then send it back towards the destination, which is not the optimum solution. In addition to that, for all the diversion and mitigation to be successful a number of other points in the network (i.e. core routers, switches, firewalls) would have to be pre-configured and set, in order to allow for this traffic diversion and mitigation to take place. An example of such scenario is illustrated in Figure 1.

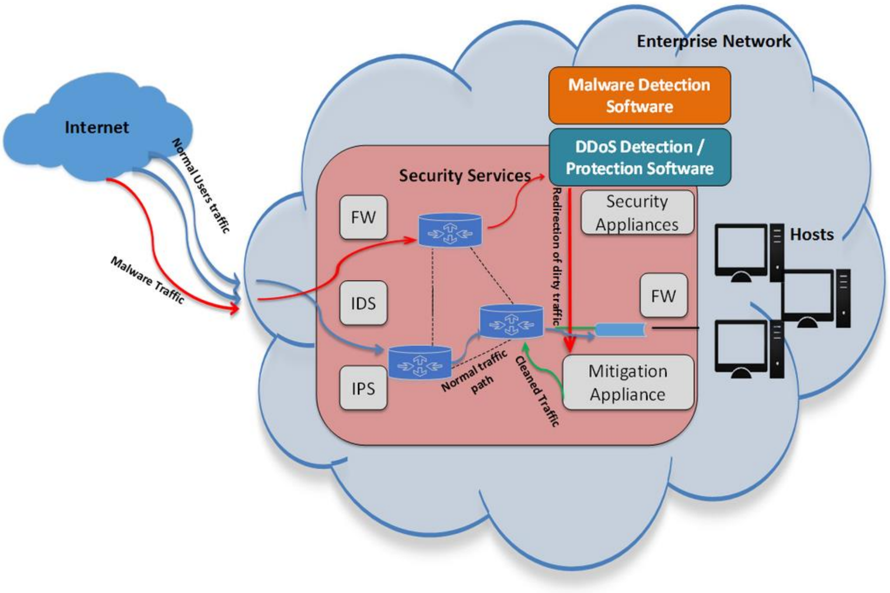

Figure 1: Traditional security architecture for dealing with DDoS & Malware attacks

The configuration of the network nodes is complex and following this approach every single device that takes part in the process will have to be pre-configured, even if an attack is not happening and mitigation is not needed. In addition, if an organisation wants to achieve the most effective security design, they usually select to introduce the specific security appliances inline in the network, which can cause delays in traffic processing and forwarding.

SOFTWARE-DEFINED SECURITY ARCHITECTURE. One of the inherent capabilities of an SDN controller is the fact that it has knowledge of the network topology and infrastructure and it provides visibility of the traffic. Since the introduction of the SDN logic and its architecture, the controllers have now evolved and are also offering integrated security functions. Some examples of these functions are: routing, firewalling policies and service chaining enablement, which allows for the implementation of dynamic security in the network via the controller that is mainly driven by applications and software. As a complement to this approach the SDN controller can make use of the NFV concepts, which allows for the deployment of sophisticated network functions in commodity hardware, and through the application of service chaining dynamically direct the traffic flows to the right network elements, if and when needed. The overall model is described as Software-Defined Security (SDSec).

Following the above architecture concepts, the design of security solutions to protect organisations from DDoS and Malware attacks can drastically change and evolve to a more dynamic and sophisticated implementation. By utilising SDN and NFV the design described in the previous section will transform to the following:

- Existing network devices (i.e. routers, switches, firewalls) are integrated with the SDN environment and an SDN controller has visibility of the topology and also has the capability of managing the devices directly or indirectly (i.e. through integration with their own element managers).
- SDN controllers will have visibility of the traffic flows and the communication between endpoints, which allows security policy to be centrally controlled and managed. In addition the controller will collect and process information about the network and the traffic through analytics.
- Network security application components, which through the use of NFV can now be virtualised and deployed in existing commodity hardware, can integrate through northbound APIs with the SDN controller and utilise the information, in order to detect and respond to potential DDoS or Malware attacks. In some scenarios the application can also be designed as native functionality of the SDN controller itself.
- The mitigation can now be realised in a more dynamic and efficient way:
    - The application can direct the SDN controller to reconfigure the network elements, in order to either divert the traffic to the right network elements, such as a scrubber device to clean the DDoS, or to block and quarantine an infected host for preventing further infection of the network in a dynamic way.
    - The most interesting implementation characteristic of the mitigation though, is the fact that the mitigation can now be applied dynamically at source of the attack, without necessarily the need to fully re-direct the traffic. It is now possible to spin off a virtual instance which runs the anti-malware or DDoS mitigation mechanism and place it nearest to the host from where the attack originated.

Consequently the concept architecture is evolving and leveraging SDN and NFV technologies, for implementing security solutions as depicted in Figure 2.

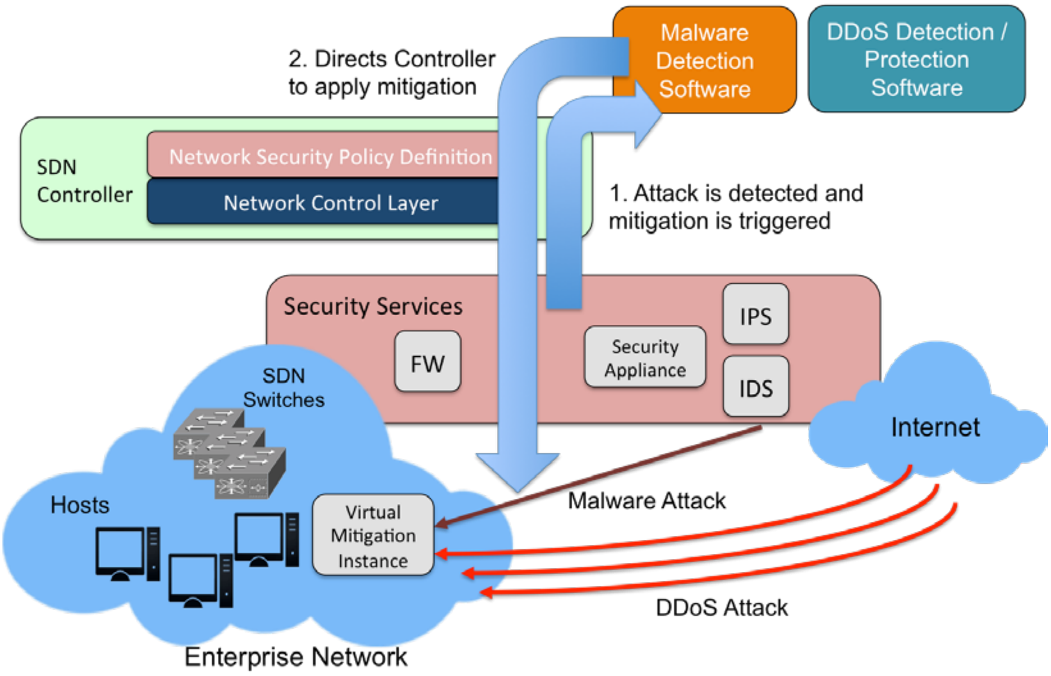
Malware Detection Software
DDoS Detection / Protection Software
2. Directs Controller to apply mitigation
SDN Controller
Network Security Policy Definition
Network Control Layer
1. Attack is detected and mitigation is triggered
Security Services
IPS
Security Appliance
FW
IDS
SDN Switches
Internet
Hosts
Virtual Mitigation Instance
Malware Attack
DDoS Attack
Enterprise Network

Figure 2: Evolved security architecture for dealing with DDoS & Malware attacks

SOLUTIONS. Most of the network security vendors are evolving their products, in order to integrate with the SDN layer and utilise the concepts of NFV. This will allow organisations that have invested in security products to evolve and incorporate such technology integrations at their own pace. In the case that an organisation is looking to invest in introducing an SDN solution, they should be mindful of the integration of such products with the selected SDN controller, since interoperability between different vendors' products is not yet mature or standardised.

At the same time, a lot of Open Source driven security tools and applications have been introduced, which allow for integration with a wide number of solutions. Some of the security solutions, such as DDoS detection and mitigation, have also been incorporated within Open Source driven SDN controller frameworks and it is anticipated that with the evolution of SDN more and more security functionalities will be moved natively into the SDN environment.

BENEFITS & OPPORTUNITIES

By leveraging technologies, such as SDN and NFV, and advancing to an evolved security architecture, an organisation can realise benefits and opportunities that were either not possible in the past, or too expensive to be justified.

Overall some of the benefits that can be realised by introducing SDSec in an organisation are the following:

- **Efficient and dynamic mitigation** of security threats and attacks, since the mitigation can be applied nearest to the source of the attack, relieving the network from having to off-ramp traffic to a central location, and also allowing for dynamic insertion and removal of security points where and when needed.
- **Hardware cost reduction**, due to the virtualisation of the network security applications in commodity hardware, instead of the deployment of specialised vendor appliances.
- **Utilisation of existing network appliances**, even if they do not support advanced traffic monitoring mechanisms.
- **Dynamic configuration of existing network nodes** for the mitigation of an attack, where and when needed, instead of static pre-configured policies that potentially are not being used.
- **Harmonised view of logical security policies**, which exist within the SDN controller model and are not tied to any server or specialised security device.
- **Visibility of information from one source** rather than by introducing network probe elements in different locations of the network, which will then have to be correlated.
- **Integration with sophisticated applications**, which can utilise the existing information around the network, in order to correlate events in a simpler way and respond more effective and intelligently to security threats.
- **Central management of security**, which is implemented, controlled and managed by security software through the SDN controller.

CONCLUSIONS

The evolution of networking through the use of SDN and NFV is introducing tremendous opportunities for organisations to evolve their traditional security architecture and implementation models, realise the benefits of programmability and automation and adopt the Software Defined Security model, in order to respond in a more dynamic, efficient and intelligent way to the continuously increasing security threats that they face today.

SYTEL REPLY’S OFFERING

Through its distinct competencies, Sytel Reply assists clients in realising the benefits and dealing with the impacts of the disrupting technologies on their environments. Sytel

Reply leverages real-world experience in SDN & NFV consulting for the TMT market, having worked with global Telco providers and established strong relationships with all major SDN vendors.

Through active collaboration with various vendors and, by forming partnerships with educational institutions, as well as performing internal research & development, Sytel Reply creates and supports innovative projects around new technologies, such as SDN & NFV.

Some of the more detailed offerings in the area of SDN & NFV include, but are not limited to, the following:

- SDN/NFV Requirements Definition
- Solutions Evaluation (including RoI, TCO)
- Architecture Design and Technical Consulting
- Security Assessments
- Proof of Concepts (PoCs) Design, Plan and Testing

Sytel Reply builds upon this knowledge and partners with its clients to define their strategy and identify the trajectory they should follow towards adopting these disruptive technologies, for future proofing their environments and their investments. Sytel Reply builds on the basis of understanding the customer requirements and selecting the optimal solution towards programmability, service agility, automation and openness in their networks, in a vendor agnostic way.

REPLY
SYTEL

Sytel Reply is part of Reply, a leading Consulting, Systems Integration and Digital Services company specialising in the design and implementation of solutions, based on new communication channels and digital media. Sytel Reply UK is the company of the Reply group that is specialised in the Telecommunication, Media and Technology (TM&T) markets in the UK and Ireland.

Sytel Reply, thanks to its in-depth competence and experience, boasts a team of highly skilled professionals with a mission to support clients in managing technology and business disruptions, which they are facing during business transformation and technology innovation programmes.

Sytel Reply
www.reply.com