Assure
Advanced Performance Management

Solving the East-West Problem

Application focused security

Modern application architectures often rely on hybrid environments, meaning lots of virtual machines, spread across local virtualisation platforms and cloud services. In the past, we could assume that an application would be deployed to a secure zone, protected by a hardware firewall (and, occasionally and Intrusion Prevention System or IPS) to create a Demilitarised Zone (DMZ). Network traffic could be steered through the firewall to implement segmentation and the application of security policies to application traffic. This applied both to inbound traffic from application users on the internet or internal network and to application traffic between servers.

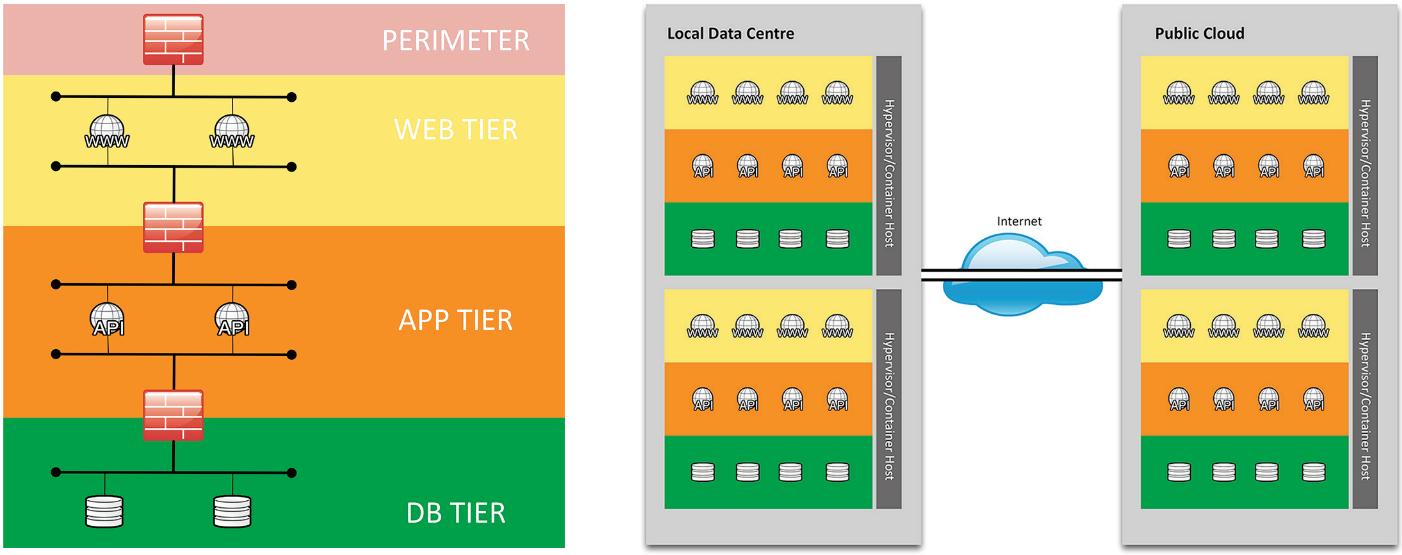

Figure 1 Traditonal Architecture (L) vs Modern Architecure (R)

Nowadays, the situation is almost unrecognisable. Application components may be spread across multiple instances and containers, both on-premises and in the cloud. Network traffic may be moving between logical components without ever leaving a single physical host. This has led to a loss of visibility within the application environment, and it makes it almost impossible to enforce viable security policies using traditional security mechanisms, such as physical or virtualised appliances without applying some seriously over-complex routing and switching logic. We call this the “East-West Problem”.

Moving the security focus

The problem can be summarised as follows:

How can I regain the visibility and enforcement I once enjoyed without losing the benefits of hybrid infrastructure?

The answer is to move the enforcement point closer to the applications, services and data that you are trying to protect. Within an environment where you cannot be certain whether traffic will leave a physical host, the enforcement point must move to the logical component, whether this is a virtual machine or a container. In order for this to be effective, enforcement and definition of the security policy must be simple and as automated as possible. Ideally, it will fit in with your orchestration tools to allow the automatic deployment of fine-grained security policies when new infrastructure components are instantiated. he security policy as defined by the administrator should be high-level, ideally close to natural language. At Assure, we think we’ve found the perfect product to deliver this capability.

Illumio adaptive security platform

Assure has conducted extensive research into how we can help our customers solve this architectural conundrum and has identified the Illumio Adaptive Security Platform (ASP) as a perfect solution for our customers' needs. The ASP works by leveraging the built-in firewall capabilities of Linux and Windows (iptables and Windows Firewall, respectively) via an agent deployed to the workload. ASP allows an administrator to discover and map application data flows before grouping components together using labels.

Once your infrastructure has been correctly labelled, security policies can be defined in high-level language such as the one shown below.

Source	Destination	Service	Encrypt	Action
Internet	Web Servers	Web	No	Allow
Web Servers	Application Tier	Web	Yes	Allow
Application Tier	Database	DB	Yes	Allow

ASP uses graph theory to compute and deploy complex security policies across your entire infrastructure. As an added bonus, the Illumio agent can use the built-in IPSec capabilities on the workload to encrypt traffic between systems.

Summary

Traditional application architectures were simple to secure using network choke points that allowed physical or virtual security appliances to enforce policy. As infrastructure began to spread between corporate data centres and the cloud, security policy became increasingly difficult to apply using traditional security mechanisms and security appliances became increasingly difficult to manage.

Assure can help you solve these problems in partnership with Illumio. Deploying Illumio's Adaptive Security Platform allows you to define simple, yet highly granular micro-segmentation policies across application infrastructure, regardless of the physical location of the workloads involved or the infrastructure that they run on. As an added bonus, the Illumio ASP can help you discover complex application flow information, helping you to fully understand your application infrastructure.