A Trend Micro White Paper | May 2016

Network Security Protection Alternatives for the Cloud

» A technical brief summarizing the deployment options that can be used to deploy IDS/IPS protection for cloud instances

Version: 2.0

PURPOSE OF THIS NOTE

Cloud computing has become extremely popular for enterprises. It helps provide additional computing capacity for their Data Center or in some cases replaces it.

The security model for servers and applications with most cloud providers is referred to as a Shared Responsibility Model. This model requires that both the cloud provider and the customer share responsibilities for providing protection to those servers and applications.

The customer in most cases is responsible for all operating system and application security. Therefore, many of the security mechanisms required in a traditional Data Center are also required in the cloud. From an audit perspective for key industry regulations, such as PCI-DSS, the ability to meet the audit requirements still applies.

Some of the main security mechanisms depended on by organizations today within the Data Center are:

- Firewalls
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Integrity Monitoring
- Anti-Malware
- Log Monitoring and Aggregation
- Identity and Access Management (IAM)

Some of these mechanisms are typically delivered using dedicated hardware security appliances at the network perimeter (Firewall, IDS/IPS). Others are delivered through software on the servers themselves (Anti-malware, Integrity Monitoring). And others are typically delivered by 3rd party software and/or services (Log Monitoring and IAM).

The purpose of this paper is to identify the different options for deploying IDS/IPS functionality to protect cloud instances, and highlight the differences in approaches. IDS/IPS is one of the security mechanisms that most organizations depend on in their Data Centers and is often required to meet compliance requirements and defend against threats.

In particular, the deployment of IDS/IPS using a security virtual appliance (SVA) running at a cloud provider will be compared and contrasted to security software running on the instances themselves.

INTRUSION DETECTION AND PREVENTION (IDS/IPS) OVERVIEW

Security professionals have been utilizing IDS since the first commercial product was introduced in the early 1990's. These systems were normally network based and initially only detected intrusions. About ten years later IPS became popular because of the additional ability to actively block attacks. They systems typically ran on dedicated hardware with the performance and throughput being based on the size of the network interface, CPU and memory.

The widespread use of virtualization on x86 architecture has caused a shift in Data Center security. Many organizations, in order to build scalable "private cloud" environments are augmenting perimeter security with security controls that operate on virtualized servers. This includes IDS/IPS and can be done with security virtual appliances as well as software on the virtual machine.

USING IDS/IPS TO PROTECT CLOUD INSTANCES

A typical deployment of an application in the cloud will utilize multiple application servers and database services. The application servers will often use auto-scaling to add more servers automatically as application load increases.

Using the SVA deployment model there are two methods in which IDS/IPS can be used. One requires software to be deployed to each instance in order to send a copy of the network traffic to the appliance for inspection. The second requires routing configuration changes to be made in order for the security virtual appliance to inspect the traffic. Figure 1 illustrates both deployment scenarios.

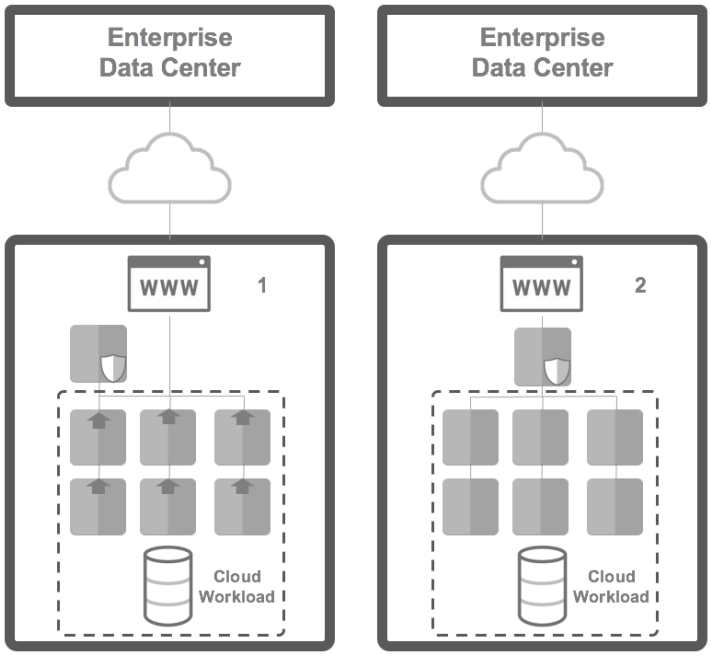

Figure 1: Security Virtual Appliance IDS/IPS

The other option for deploying IDS/IPS is to protect each instance using software this is deployed directly to them. This allows the security polices to tailored to the specific software executing on that server. Which allows for the removal of generic or not-applicable rules running and taking up resources. Features such as “Recommendation Scan” from Trend Micro also help to determine exactly what is needed to protect the server. The challenge of deploying this security software and policy is alleviated with tools such as Chef and Puppet, which most major cloud providers support. There are also native ways such as Cloud-Init, OpsWorks and Azure VM Extensions. This approach is illustrated in Figure 2.

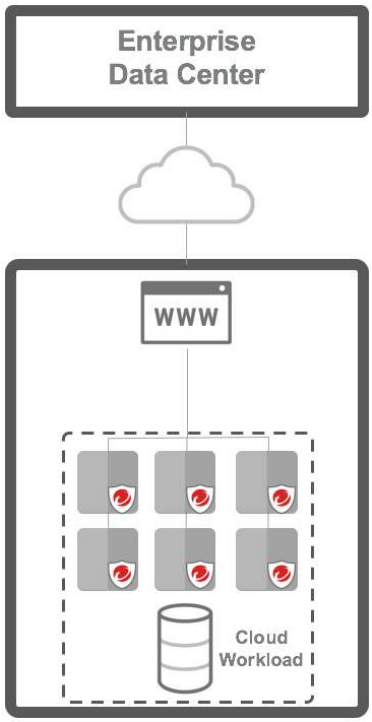

Figure 2: Instance Software

COMPARISON OF OPTIONS

One of the biggest architectural problems with Network based IDS/IPS is the use of encryption to protect network traffic. This security practice protects the contents of network traffic making it difficult and sometimes impossible to analyze and thus attacks cannot be detected. For Host based IDS/IPS, encryption is less of an issue as the host decrypts traffic before it is analyzed.

The following is a summary comparison of the different methods, which can be used to deploy IDS/IPS protection for cloud instances.

Attribute	Security virtual appliance (Method 1)	Security virtual appliance (Method 2)	Instance software
Instance software required	Partial (required to forward traffic to appliance)	No	Yes
Ease of Configuration	Complex	Complex	Straightforward
Network Transparent	Yes	No	Yes
Performance/ Throughput Impact	Difficult to understand impacts on an SVA as instances are added or auto-scaled	Difficult to understand impacts on an SVA as instances are added or auto-scaled	Does not change as instances are added or auto-scale
Scalability & Availability	Potentially Complex availability model	Complex availability model	Same availability model as instances
Rule Efficiency	Inefficient - General rules to cover a broad range of devices	Inefficient - General rules to cover a broad range of devices	Efficient - Specific rules to cover only the device being protected
Audit History	Incomplete	Incomplete	Complete
Ease of additional security mechanisms (Anti-malware, File Integrity Monitoring)	Not possible	Not possible	Straightforward
IDS/IPS protection	Detect only	Detect & Prevent	Detect & Prevent
Analysis of Encrypted traffic	May require additional configuration	Requires additional configuration	May require additional configuration required.

SUMMARY

Although both SVA's and instance software can be used to deliver IDS/IPS for cloud instances, there is a strong argument for instance software being the easier and most cost effective choice. Deployment can be handled with automation tools supported by major cloud providers making it seamless and there is a reduced resource requirement by not having an additional specialized instance. With the added "Recommendation Scan" feature of Trend Micro Deep Security, organizations can also benefit from a more specialized and efficient set of protection rules.

As cloud providers change to provide more sophisticated networking mechanisms which would enable more transparent methods of adding network security functionality to cloud environments, this paper will be update to reflect these changes.

Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.