ENEA

Use Case Datasheet

Data Center Security based on Micro-Segmentation: Protect Traffic between VMs up to the Application Level

Micro-segmentation is a new way to enhance security for east-west traffic within a data center. This new approach requires real-time application-awareness which can be provided by Enea's Qosmos ixEngine®.

Key Facts

- Qosmos ixEngine is a DPI-based application classification & metadata extraction engine
- High recognition rate: ability to identify layers 2 to 7 in the OSI model
- 3000+ protocols classified and continuously updated, 4700 application metadata extracted
- Identifies protocols and applications based on flow pattern matching, session correlation, heuristics and statistical analysis
- Users can develop their own signature plugins
- Modular architecture (flow management, regular expression engine, http parsing, etc.)
- Portable architecture (x86, ARM, Cavium)

Benefits

- Ready-to-use layer 7 visibility for developers of data center security products
- Continuously updated protocols and applications
- Qosmos ixEngine extends vSwitch visibility from layer 1-4 all the way up to layer 7
- Natively integrated with new virtualized architectures and frameworks (e.g. ODL Group-Based Policy)
- Enables automated provisioning and move/add/change of policies + quarantine of infected VMs

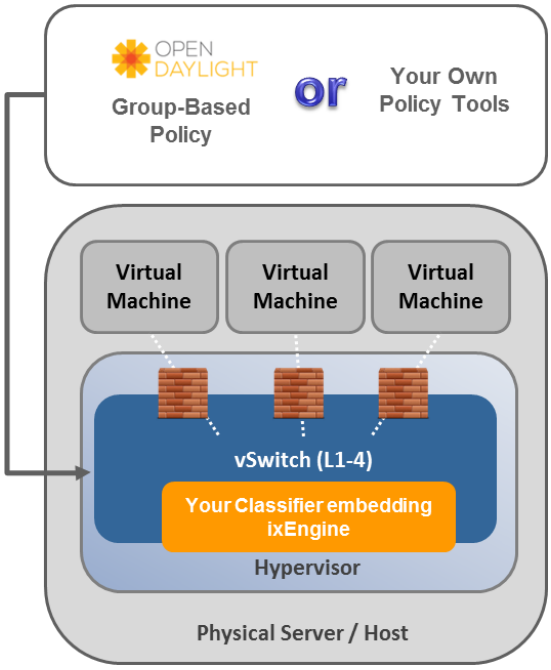
The Challenge

Data centers are typically protected using perimeter security technologies such as firewalls and IDS/IPS. These products focus on north-south traffic, in and out of the data center. While they are very effective at protecting the perimeter, they are not built for securing east-west traffic within the data center. This is becoming an issue since east-west traffic could represent 5x the amount of north-south traffic, due to an increasing number of communicating web, application, and database servers. This means that if a malware penetrates the outer security perimeter, it can launch further attacks inside a vulnerable data center.

The Solution

Micro-segmentation divides the data center into smaller zones which can be protected separately. The advantage is that in case of a breach, the damage can quickly be contained to a small number of compromised devices. This new approach requires a real-time association between applications and security policies. Therefore, east-west traffic between VMs must be analyzed in real-time, up to the layer 7 application level.

Using your own development resources or with the assistance of Qosmos Professional Services, Qosmos ixEngine can be integrated inside the hypervisor and extend vSwitch visibility from layer 1-4 all the way up to layer 7. The vSwitch strengthens access control rules between VMs based on application traffic.



L7 Classifier for vSwitch based on Qosmos ixEngine

Comprehensive Network Intelligence

Qosmos ixEngine® provides the broadest range of protocol and application recognition on the market, based on over a hundred man-years of expertise in the telecom, enterprise and security markets:

- Ability to identify nearly all protocols and applications behind IP flows, on mobile and wireline networks, in any geography
- Fast addition of custom plugins to meet requirements for decoding local, proprietary or legacy protocols
- Tools for users to develop customized signature plugins

Advanced Analysis

Qosmos ixEngine can be integrated inside the hypervisor and extend vSwitch visibility from layer 1-4 all the way up to layer 7. The vSwitch strengthens access control rules between VMs based on application traffic.

The resulting L7 classifier enhances security for east-west traffic within a data center:

- Full application decoding: classification, metadata extraction, content extraction, reconstruction of communications (e.g. Instant Messaging)
- High accuracy rate: advanced techniques like double checking and CRC checking ensure 100% accuracy with no false positives
- Full protocol behavior analysis: for example full http decoding to handle http proxying
- Support of complex networking behavior such as GTP encapsulation, VXLAN and tunnels (GRE, L2TP, etc.)
- Leverages hardware acceleration

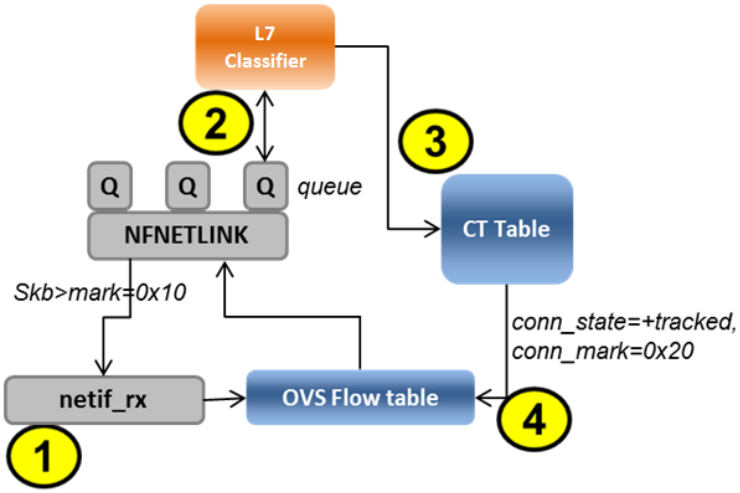
Architecture & Integration Scheme

The Qosmos division of Enea provides the easiest path to L2-L7 flow analysis for embedded software developers, reducing development cycles, costs and risks. Developers can focus on building complete solutions, relying on Qosmos for our domain expertise in protocol, application and metadata extraction:

- Integration with Open Virtual Switch version 2.4 or higher
- Qosmos works with leading switch vendors and the open source community to extend support for additional switches
- Different configuration options enable developers to optimize integration. Qosmos ixEngine is modular and can work, for example, with an external regular expression engine
- Independent core decoding framework and protocol plugin library enable fast protocol updates while preserving software stability. The protocol plugins are hot-swappable
- Switchable IP and TCP flow reassembly process for packet reordering
- Traffic offloading mechanism

Supported Environments

- Open Virtual Switch 2.4 or higher
- Cavium LiquidIO virtual switch



Reference architecture of a L7 Classifier built on Qosmos ixEngine

Find out more on the Qosmos website!

Qosmos, a division of Enea, is the leader in IP traffic classification and network intelligence technology used in physical, SDN and NFV architectures. Qosmos ixEngine software development kit and components are embedded by vendors and integrators into their products sold to telcos, cloud service providers and enterprises. For more information: www.qosmos.com