DYNAMIC CONTAINER NETWORK AND SERVICE MESH POLICY ACTIONS BASED ON MALWARE AND INTRUSION DETECTION

Sanjeev Rampal
DYNAMIC CONTAINER NETWORK AND SERVICE MESH POLICY ACTIONS
BASED ON MALWARE AND INTRUSION DETECTION

AUTHORS:
Sanjeev Rampal

ABSTRACT
A closed loop solution is provided for dynamically enforcing container network and service mesh policies based on dynamic malware detection. This may be integrated with existing enterprise firewalls, intrusion detection systems, and other similar malware detection appliances.

DETAILED DESCRIPTION
An existing network security problem is how to enforce container security policies dynamically in a cloud native environment based on security alerts/triggers that can originate from security devices (such as firewalls or intrusion detection systems) which may be running outside the container cluster. An end-to-end solution for malware detection and dynamic remediation is needed across a mix of containerized and non-containerized workloads/endpoints.

Current container networking and service mesh solutions typically require the static configuration of network segmentation rules, which is often ineffective. In addition, these container networking based policy solutions have no integration with security appliances such as firewalls and intrusion and malware detection systems. The problem is further compounded by the fact that container identities and Internet Protocol (IP) addresses are not typically visible outside of the container cluster due to layers of Network Address Translation (NAT) and dynamically changing pod IP addresses with short lifetimes.

Hence, the problem to be solved is how to provide a clean end-to-end solution that integrates security appliances such as firewalls and intrusion detection/preventions systems with container networking and policy capabilities at both Layer 3 (L3) and Layer 7 (L7) / service mesh layers and enables dynamic remediation and segmentation actions once malware has been detected in a mixed enterprise environment that has both containerized and non-containerized workloads.
Figure 1 below illustrates an example overview of the solution provided herein.

As shown, a security appliance detects malware emanating from some IP address. The security appliance reports this to a remediation gateway module which is configured to know that this range of virtual IP addresses belongs to a certain cluster (e.g., a Kubernetes (K8S) cluster) but does not know details of container networking policies, identities of specific pods behind this virtual service, etc. Therefore, in this example the security appliance calls the K8S Application Programming Interface (API) to trigger a K8S policy (which may be an L3 network policy or an L7 service mesh policy) that has the appropriate segmentation action (e.g., quarantine, redirect, alert, etc.) on the appropriate service IP address(es). This K8S policy is then applied by the K8S control plane resulting in the blocking, segmentation, or other appropriate action on the suspect pod or set of pods using that logical service IP address. The enterprise administrator may thereby immediately mitigate the threat.

By using K8S network policy, these operations may be performed regardless of whether an Application Centric Infrastructure (ACI) physical network fabric is used. It relies purely on standard K8S layer network policy controls, and provides the option to enforce advanced L7 security policies when the service mesh and policy is being used in K8S. Service meshes provide an additional layer of new options for enforcing and monitoring policies within K8S. Finally, once this feedback loop is in place, it enables
additional innovations between security portfolio and container networking and K8S platform products.

The techniques described herein may cover both traditional non-containerized intrusion detection systems as described above as well as future containerized versions of intrusion detection systems.

In summary, a closed loop solution is provided herein for dynamically enforcing container network and service mesh policies based on dynamic malware detection. This may be integrated with existing enterprise firewalls, intrusion detection systems, and other similar malware detection appliances.