May 10, 2018

PORTABLE NETWORK NAMESPACES: TRAFFIC COLORING FOR PORTABILITY

Ian Wells
Cisco Systems, Inc.

Rajiv Asati
Cisco Systems, Inc.

PORTABLE NETWORK NAMESPACES: TRAFFIC COLORING FOR PORTABILITY

AUTHORS:
Ian Wells
Rajiv Asati

CISCO SYSTEMS, INC.

ABSTRACT

Techniques are described herein to add a “color” marker as a namespace to packets per service/microservice/container. This causes the namespace to be used within or between the cloud(s) for additional treatments.

DETAILED DESCRIPTION

Network namespaces within container platforms enforce endpoint identity. Conventionally, containers have access to a namespace with an Internet Protocol (IP) address that they have no power to change. Access Control Lists (ACLs) and routing policy may be applied based on source interface and network address, but the endpoint cannot be moved to another host or cloud.

Accordingly, described herein is a “color” marker for packets. Briefly, every packet generated by a process has a “color”. As with process groups, a process may select a color from a range of colors it is authorized to use, which it inherits from a parent. The first process of a container inherits its range of colors from the orchestrator when initiated. The color is encoded in every packet created from BSD socket calls to the kernel from that process, and may be encoded in a Layer 2 header, Layer 3 header, Layer 4 header, or any combination thereof.

The color may be assigned independent of the IP address and pod location. Thus, the color does not necessarily need to change even if the IP address(es) that is assigned to the function/microservice/container changes due to portability. Color is added to the (payload) packet to indicate the treatment the packet should receive in terms of additional services (e.g., firewall, Deep Packet Inspection (DPI), prioritization, jitter reduction, etc.). This permits policies to be applied anywhere in the cloud network fabric, physical or virtual,

regardless of location. Moreover, the service can be moved and even readdressed to a new subnet local to the new location, without changing this behavior.

This may also be implemented across clouds. Colored packets may be fed via a proxy for each cloud that determines treatment (potentially including a source address rewrite) and appropriate routing to a destination (potentially using non-local Virtual Routing and Forwarding (VRF)). In one example, color may be in an Ethernet or Virtual Extensible Local Area Network (VXLAN) header. In another example, color may use Segment Routing version 6 (SRv6). An SRv6 option header may be added with the targeted address of the packet as the terminal address and an additional address before indicating the treatment the packet should receive.

Conventional SRv6 does not solve this problem because the SRv6 domain can be different from that of the datacenter, and SRv6 might not be plausible on the host / container / Virtual Machine (VM) itself. Also, SRv6 leverages an address/hop based SR header that is tied to a particular domain or cloud. The techniques described herein are broader, and SRv6 may be used in one example. To make use of SRv6, a new Segment Identifier type may be defined with global uniqueness to encode “color”.

In summary, techniques are described herein to add a “color” marker as a namespace to packets per service/microservice/container. This causes the namespace to be used within or between the cloud(s) for additional treatments.