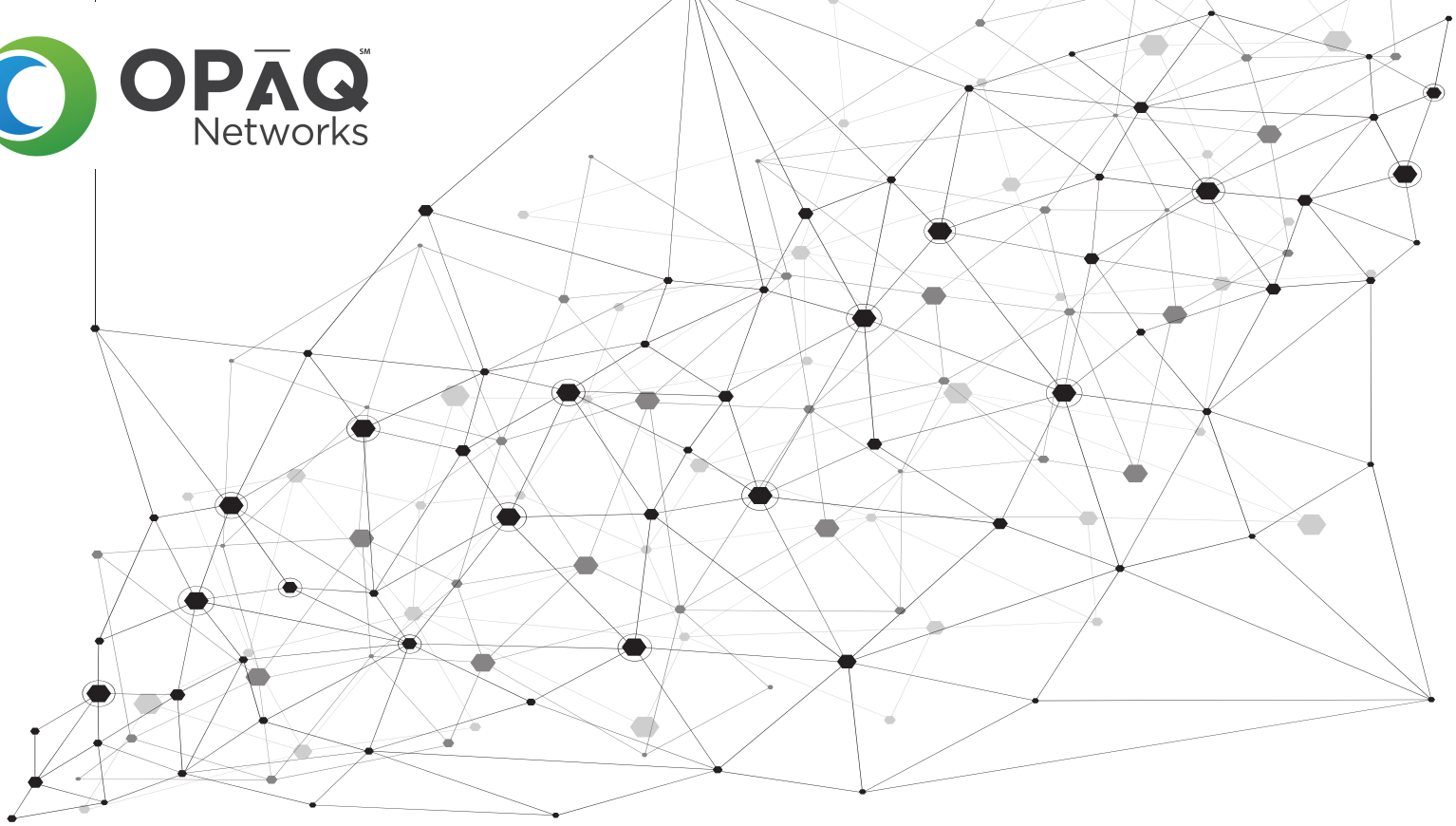


Monitoring and Security for Docker Containers

OPAQ PathProtect™

Abstract

Since its emergence on the market in 2013, Docker has become the clear leader in container technology in the cloud computing era. But even though Docker made containerization easier, it is still not easy. As enterprises now seek to scale container technology from single-host development environments to multi-host cloud production environments, the challenges of monitoring and enforcing a consistent security policy become even more difficult. OPAQ PathProtect™ is a commercially available, next-generation host-based firewall that can provide visibility and control over all your enterprise's workstations, servers, and now containers.

Greg Galloway

1 Overview

Containerization is not new, with its roots going all the way back to 1979 with the introduction of the chroot system call on V7 Unix. But not until Docker emerged on the market in 2013, did interest in containerization really start to take off. Docker made containerization easier, albeit not completely easy. And as a result we've seen the emergence of a number of new projects to address scaling Docker deployment from single-host environments to multi-host environments. While each of these solutions attempt to address one part of the scalability puzzle, they also make monitoring and security a bit more difficult.

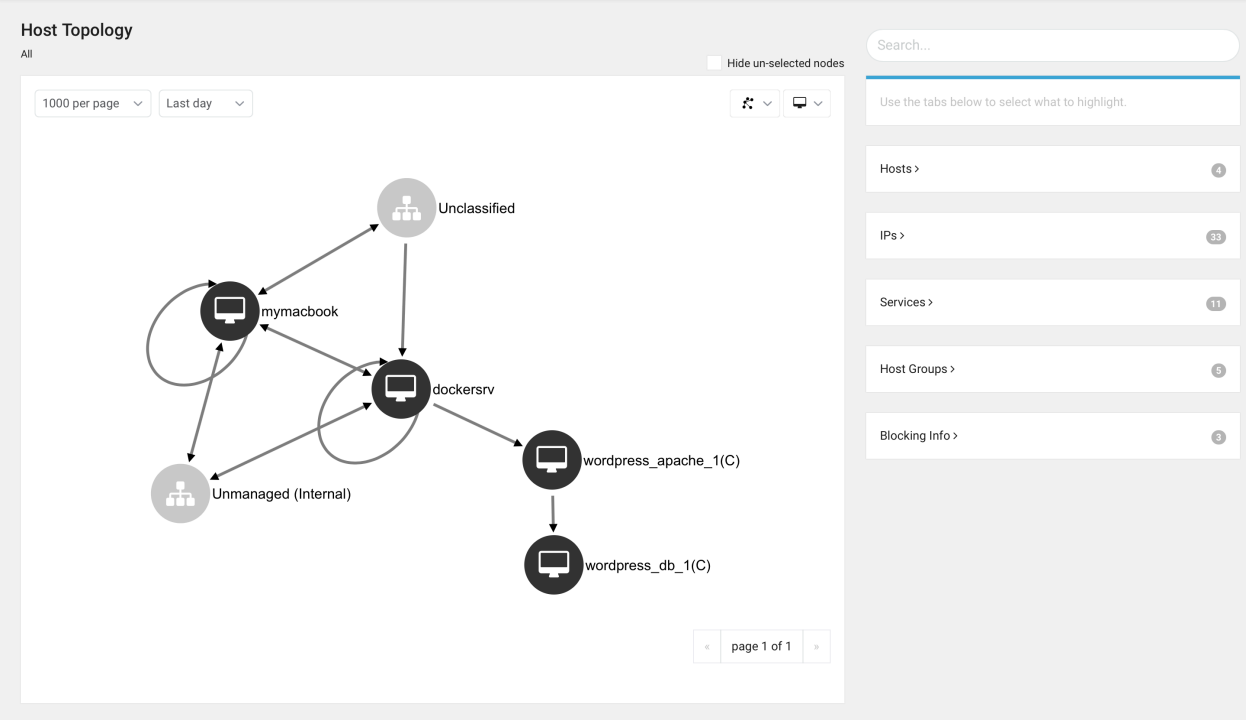
IP based network firewall policies can be difficult to manage in a Docker environment because individual containers can change IP addresses and in some cases move to different servers. In addition, Docker itself introduces a large number of rules to the iptables configuration, complicating management and analysis of the firewall policy.

OPAQ PathProtect™ is a commercially available, next-generation host-based firewall that can provide visibility and control of Docker containers. OPAQ PathProtect™ allows firewall policies to be applied based on container ID, regardless of that container's IP address or the host that it is running on. It also provides a crisp user interface for investigating container behavior and building policies.

OPAQ PathProtect™ achieves this result using an Endpoint Agent that is installed on the Linux-based Docker server that intercepts every network connection to, from, and between every container and reports them to a central Controller. The Controller tells the Agent whether to approve or deny each connection on a case by case basis, based on a combination of the device identity, the user identity, the source address, and the application being accessed. This architecture provides the Controller with total visibility into all of the traffic happening to and from the organization's assets at all times, and it enables dynamic policy enforcement that can adapt as users and workloads move between networks.

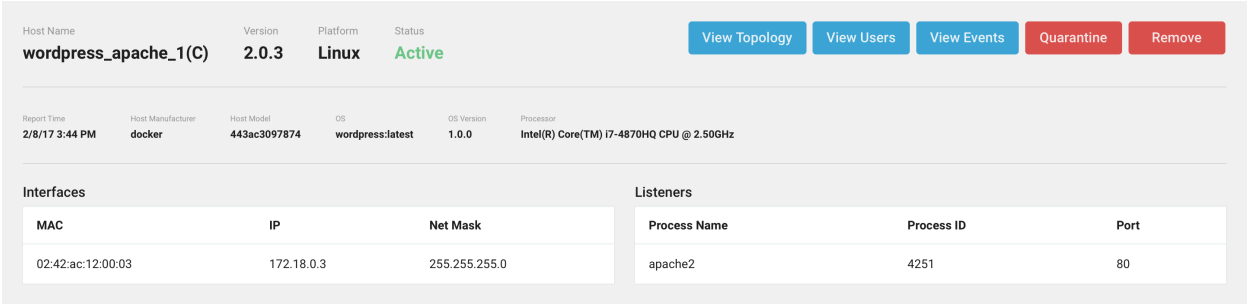
2 Monitoring and Securing Containers

The OPAQ PathProtect™ Agent for Linux has a small footprint, very few dependencies, and can be installed on virtually any Debian or Red Hat-based Linux system. Installing the Agent on a Linux-based Docker server provides full visibility and control of all network traffic in and out of the Linux server, as well as all traffic to, from, and between all Docker containers running on that server.



In the example topology shown above, the OPAQ PathProtect™ Agent for Mac OS X has been installed on a Macbook ("mymacbook") and the Linux Agent has been installed on a Linux-based Docker server ("dockersrv"). The Docker server is hosting a WordPress application on port 8000. The WordPress application consists of two containers launched together using Docker Compose. One container is running Apache listening on port 80, while the other is running MySQL listening on port 3306.

The hostname displayed for each container is the name assigned by the administrator, or in this case by Docker Compose. The administrator can select a node in the topology view, and view more details about the container, such as the container ID, image name, and listening processes.



When the Macbook user browses to the public WordPress instance on port 8000 of the Docker server, both agents detect and report the connection. The Mac Agent shows the user, "macuser", and process, "com.apple.WebKit" (aka. Safari), that initiated the connection, while the Linux agent shows the user, "root", and process, "docker-proxy", that terminated the connection. From here we can see that the docker-proxy forwarded the traffic to the Apache instance in the first container listening on port 80. And then Apache makes a connection to the MySQL server in the second container listening on port 3306.

Source Host	Target Host	IP	User	Service	Process	Report Time	Status	Action
wordpress_apac...	wordpress_db_1(C)	172.18.0.3/172.1...	999	TCP:3306	mysqld	43 minutes ago	ALLOWED	View
wordpress_apac...	wordpress_db_1(C)	172.18.0.3/172.1...	root	TCP:3306	apache2	43 minutes ago	ALLOWED	View
dockersrv	wordpress_apac...	172.18.0.1/172.1...	root	TCP:80	apache2	43 minutes ago	ALLOWED	View
dockersrv	wordpress_apac...	172.18.0.1/172.1...	root	TCP:80	docker-proxy	43 minutes ago	ALLOWED	View
mymacbook	dockersrv	192.168.1.36/19...	root	TCP:8000	docker-proxy	43 minutes ago	ALLOWED	View
mymacbook	dockersrv	192.168.1.36/19...	macuser	TCP:8000	com.apple.WebKi	43 minutes ago	ALLOWED	View

One complication with Docker containers is that they typically do not require static IP addresses. Although the container IDs will persist across reboots and restarts, the local IP addresses of those containers might not. Unlike other solutions, OPAQ PathProtect™ does not require that endpoints have static IP addresses. Each endpoint is identified by an agent UUID, which is unique to that workstation, server, or container. In the case of a Docker container, the agent UUID is associated with the container ID, and will not change unless the container ID changes.

OPAQ PathProtect™ allows the administrator to create host groups based on these agent UUIDs, and then write security policies using these host groups. The security policy will be enforced consistently regardless of whether the underlying IP addresses on the endpoints have changed.

Host Policy

User	Source	Destination	Service	Action	Status	Comments	Action
N/A	Any	wordpress_apache	TCP:80	ALLOWED	ENABLED	Allow Apache serve...	Edit
N/A	Any	wordpress_db	TCP:3306	ALLOWED	ENABLED	Allow MySQL server...	Edit

+ Add Host Policy

3 Conclusion

OPAQ PathProtect™ is a comprehensive solution that can provide visibility into and control over enterprise endpoint security policy, whether those endpoints are workstations, servers, or containers. It is designed to help users cut through the complexity of endpoint security policy management and enterprise network segmentation, by allowing segments to be defined in software and change dynamically as the network changes. The same technology that enables OPAQ PathProtect™ to apply a consistent security policy to containers as they change IP addresses also enables an access rule for a particular user to adapt as that user's workstation moves to different network segments. Therefore, organizations can define narrow "microsegments" that afford users only the access they require, and nothing more. This sort of policy can significantly reduce the risk an organization faces from attackers who seek to pivot laterally from an initial point of compromise to gain total control over the network. You can learn more at our website: www.opaqnetworks.com/solution.