SOLUTION BRIEF

# FortiCWP Traffic Analysis and Investigation

## Executive Summary

**Today's multi-cloud environment offers greater flexibility but less visibility: the more it is used, the bigger and more complex the digital attack surface becomes. A first step to improving a multi-cloud security posture is to obtain a centralized, real-time view of assets and resources across regions and clouds. A second step is to inspect traffic and evaluate actual traffic versus acceptable traffic using a global threat-intelligence feed to identify suspicious activity. With these in place, security teams can shorten the time to insight by drilling down to threat data presented in full contextual detail. These capabilities are provided by FortiCWP cloud workload protection (CWP).**

### FortiCWP Manages Cloud Security Posture:

- Centralized visibility via cloud API-based information
- Consistent security management across multiple clouds
- Ability to evaluate traffic against multiple global threat-intelligence services
- Drill down from regions to individual services and applications for full context
- Track, analyze, and audit easily

## A Multi-Cloud Environment Can Hide Threats

There are a number of reasons why public cloud services are expected to grow by 17.3% this year to $206 billion worldwide.[1] Cloud computing offers increased flexibility, faster time to value, and the ability to cost-efficiently scale up or down on the fly, among other benefits.

The downside for security teams is that resources from multiple clouds typically have been deployed across regions by different groups, all without centralized control. Assets change constantly, visibility is limited, and the built-in security tools from various public cloud vendors work differently and track different sets of security data.

The result is a larger digital attack surface, difficulty monitoring network traffic, and increased risk from cyberattacks. At the root of these challenges are:

- **Limited visibility.** Traditional security monitoring tools do not apply to cloud resources, services, and overall infrastructure deployments. Security teams do not have adequate tools to maintain complete visibility in the cloud.
- **Difficulty inspecting traffic.** Even with an accurate inventory management, the monitoring of traffic within and between clouds and detection of suspicious activity within that traffic is difficult due to lack of appropriate tools.
- **Complexity that slows investigations.** Fragmented security solutions inhibit the ability of security teams to drill down into data and specific incidents that are suspicious. This slows response times to attacks and breaches, increasing risk.

## FortiCWP Shortens Time to Insight

FortiCWP enables security architects to mitigate the above challenges by providing:

1. **Centralized visibility.** FortiCWP uses API-based access to cloud infrastructures and provides a single, central security posture management portal for public cloud services. Security teams can explore a current inventory of cloud assets, services, and resources as well as associated metrics to quickly and centrally administer security policies that are consistent across clouds.
2. **Traffic analysis and threat detection.** FortiCWP helps security administrators with the visibility needed in order to protect resources against inside or outside threats in major public cloud infrastructures. It integrates with indicators of compromise (IOCs) and anti-botnet databases from FortiGuard Labs to detect compromised instances and nefarious traffic. And it identifies traffic from suspicious IP addresses to sensitive workloads.

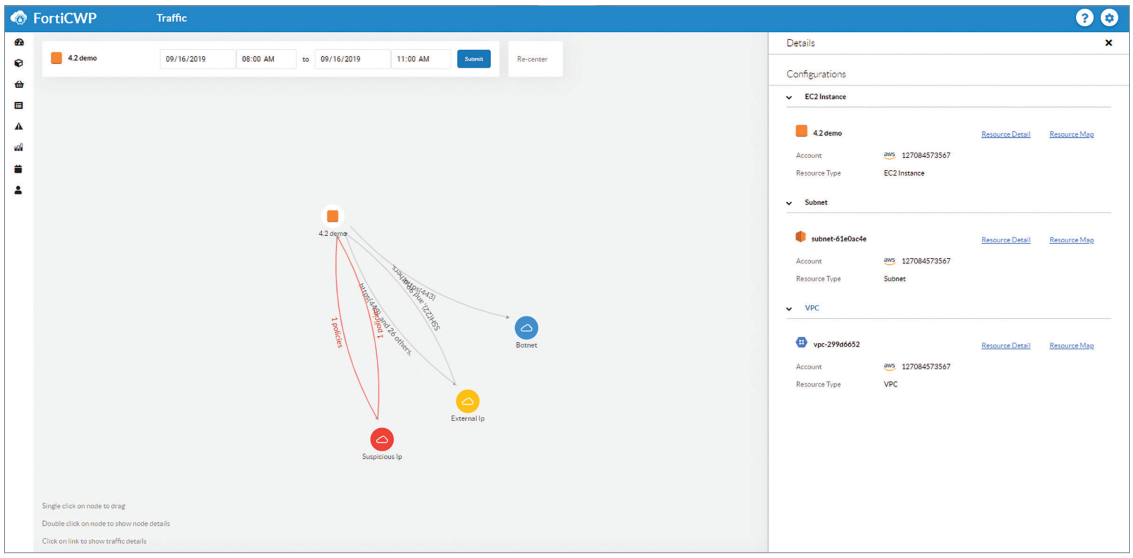


Figure 1: Making multi-cloud traffic and topologies visible.

The threat-intelligence feed from FortiGuard Labs is the product of 200-plus researchers who comb through a constant stream of data from 4.4 million sensors and hardware deployed around the world. The network also combines original research from strategic global security agencies, key technology partners, and cybersecurity alliances. All this information is fed back into FortiCWP, providing up-to-the-minute protection from zero-day threats, botnets, viruses, and other malicious exploits.

3. **Full context to streamline investigations.** When an attack or untolerable threat is detected, FortiCWP enables security teams to drill down as needed into the profile of each cloud service and view traffic patterns associated with that service. The solution provides a contextual understanding of the cloud environment that speeds time to insight. Security teams can quickly visualize traffic that flowed into and out of a cloud instance within a specified time range, using intuitive graphs that can help pinpoint anomalies. This makes it easier to track, analyze, and audit an incident to review its impact and improve security posture.

## A Foundation for Multi-Cloud Security

Centralized visibility, insight, and control are the cornerstones of a unified security posture management solution. FortiCWP provides comprehensive reporting tools and advanced controls to extend security policies across multi-cloud environments.

[1] Louis Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018," Forbes, September 23, 2018.





September21,201910:04AM

488526-0-0-EN

D:\Fortinet\Work\2019\September\092119\sb-fortiCWP-traffic-analysis