PICO

SERVICE ASSURANCE THROUGH THE DMZ

SOLUTION SHEET

CHALLENGE

Opposing Priorities of Performance and Security

Network and Security operations teams each face heightened pressures to deliver on their respective missions of performance and security, but increasingly find those missions in opposition. Good client response and experience remains paramount for digital business success.

To mitigate cyber risk, businesses must deploy technologies to detect and block intruders at the perimeter and anonymize and segment traffic. However, these technologies used to combat increasingly sophisticated cyber threats may impact network performance, resulting in a blame game due to:

- Limited ability to see and measure the specific performance impact of load balancers, firewalls, and other in-line devices
- Divergent data and insight from redundant tooling for capture and analysis network traffic across network and security groups
- Complexity from multi-vendor security devices

Without the ability to see and measure the specific performance impact of load balancers, firewalls, and other in-line devices, network teams often find themselves in an untenable position while security teams may lack a way to understand the effectiveness of these devices.

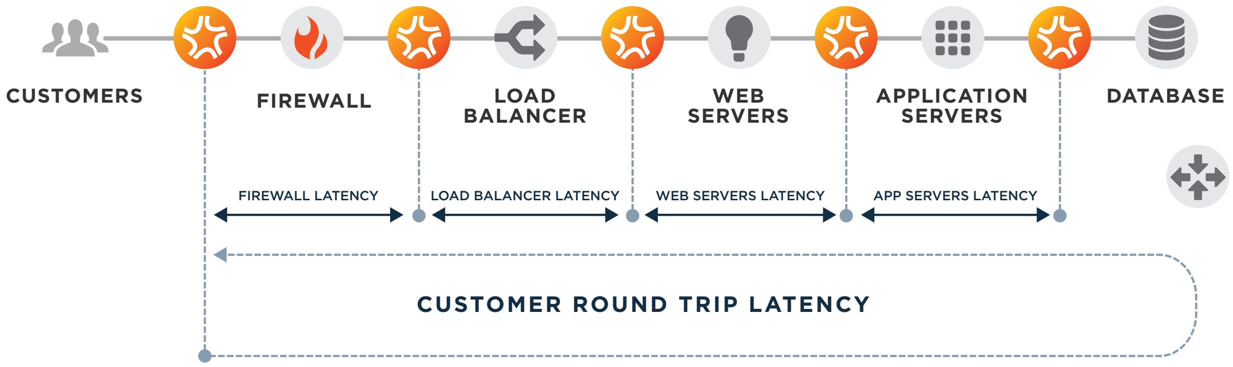
HIGHLIGHTS

- Pinpoint and measure the performance impact of the security apparatus
- Optimize the digital experience for employees and customers
- Empower NetOps and SecOps with a single source of data
- Identify 'leaky' firewalls for proactive prevention

SOLUTION

Visibility to Assure Fast, Secure Digital Experiences and to Align NetOps and SecOps

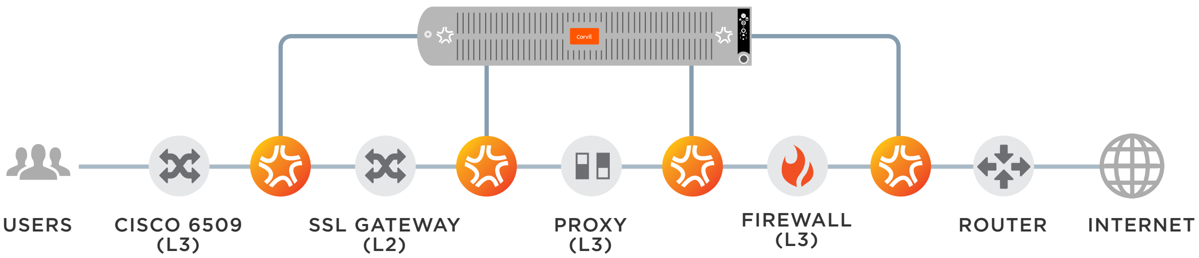
Corvil Analytics provides the intelligence to balance priorities and bridge the gap between optimal service experience and security. Corvil measures the precise directional latency through load balancers, firewalls, and other applications and devices. This "multi-hop visibility" provides an understanding of the actual performance impact of each device on user experience. As a result, network teams no longer are reduced to anecdotal defense when blamed for performance issues. Meanwhile, security teams have the means to understand and optimize the impact of their complex, often multi-vendor architectures as well as a means to understand the effectiveness of these devices.



Learn more www.pico.net

One Intelligence Source to Align Them All

Corvil provides a single data source consumable by NetOps and SecOps teams, and their respective ecosystem tooling, for identifying application, communication and infrastructure issues. NetOps teams can measure the performance impact, pinpoint the source of degradation, provide latency targets by device or stack, and quickly troubleshoot errant behaviors through such complex, often multi-vendor architectures. Meanwhile, leveraging the same data source, SecOps teams can identify "leaky" firewalls, isolate traffic that may evade rule sets, and obtain a record of the full communication path to extend troubleshooting to critical sections in the server processing.



KEY CAPABILITIES

Maximum Visibility and Measurement

Identify actual performance and latency contribution by application. Significantly shorten diagnosis and resolution times through microvisibility to identify even obscure performance issues through complexity of multi-tiered security and application environments.

Single, Shared Data

Continuous packet capture and real-time L2-L7 analysis which allows teams to capture data once and use it multiple times. Support DevSecOps initiatives from architecture through validated implementation and reduce capital cost and operating expense of managing multiple, similar network-based tools and the overhead of reconciling insights from different tools across teams.

Reinforced Defenses

Identify 'leaks' in firewalls and traffic anomalies that could indicate vulnerabilities or the first signs of a security breach that needs to be blocked.

Streamlined Workflows and Ecosystem Integration

Reduce or eliminate the overhead of fragmented toolsets integrating with other network monitoring and management toolsets as well as SIEMs and security tools.

User-Centric Traffic Analysis

With the addition of Corvil's Security Analytics module, see a prioritized list of suspicious user accounts, examine cloud usage, detect threats in real-time and rapidly investigate alerts.