FireMon + Cisco ACI
Support for Software Defined Networking

Software Defined Networking (SDN) is gaining rapid traction as CISOs look to improve their networks for better service delivery, centralize enterprise network management, and improve security. One of the first steps in the SDN adoption cycle is discovering application connectivity and mapping business application network flows and dependencies. SDN migrations are characterized by complexity and as such lack of a sound security strategy at the outset can expose new vulnerabilities triggered by uncontrolled network traffic. Cisco ACI supports centralized, application-level policy management with the Cisco Application Policy Infrastructure Controller (Cisco APIC). The FireMon-Cisco ACI integration, designed with open APIs, will enhance Cisco APIC’s capabilities for discovery and dynamic management of security policies across physical, virtual, and cloud deployments. However, this requires a detailed understanding of all the connectivity allowed by Cisco APIC. Leveraging FireMon Security Manager to access your ACI environment simplifies this complex process, allowing anyone in your organization to find and visualize Cisco ACI defined access controls in an easy to follow Policy View user interface. With FireMon, you don’t need to be an ACI expert to accurately understand your application connectivity and the policies needed to secure them.

Dynamic Policy-Driven Security for SDNs
While Cisco ACI itself is built to support application agility and data center automation, FireMon can further reinforce security controls in the environment through dynamic policy management and automation. FireMon’s integration with Cisco ACI addresses the following challenges:

- Support granular application traffic-filtering and the agility of Cisco ACI infrastructure with agile, policy-driven security
- Eliminate human errors that arise from complexity, and reduce the chances of misconfigurations
- Centralized visibility and threat management across a mixed environment – on-premises, virtual/SDN, and cloud
- Deploy applications and workloads securely. Secure application migrations
- Manage access & control privileges to SDN and on-premises workloads
- Accomplish all of the security deployments at the pace and scale demanded by SDN architectures
FireMon + Cisco ACI Delivers:

- Rapid rule creation to manage devices inside and outside the data center
- Create and modify firewall rules to support granular microsegmentation and application connectivity in the data center
- Configure consistent and global security and access control rules to support rapid migration between the data center and the cloud
- A single platform for your SDN and on-premises security for easy management. Work with the platform that you are already familiar with

<table>
<thead>
<tr>
<th>Features</th>
<th>Customer Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normalize and unify security policies into a single pane of glass across the Cisco ACI data center, on premises and cloud infrastructure</td>
<td>Implement global, uniform security policy across the environment to achieve a strong security posture</td>
</tr>
<tr>
<td>Monitoring, alerting, and observability for complex environments across the extended enterprise</td>
<td>100% visibility of the network results in comprehensive control and governance</td>
</tr>
<tr>
<td>Ability to update network policy changes on all devices and applications when migrating to the data center</td>
<td>Secure application migrations from on-premises to Cisco ACI data centers</td>
</tr>
<tr>
<td>Automate policy change processes in the SDN such as rule modification and deletion</td>
<td>Streamline policy management while reducing human errors</td>
</tr>
</tbody>
</table>

To learn more about FireMon's integration with Cisco ACI, please visit [www.firemon.com](http://www.firemon.com)