ALGOSEC APPVIZ

APPLICATION VISIBILITY FOR ALGOSEC FIREWALL ANALYZER

On any given day, new business applications are added, changed or removed, which requires the implementation of complex, time-consuming network security changes. Migrating business applications to the cloud adds additional complexities, such as understanding the network connectivity of each application prior to deployment, provisioning the relevant firewalls and routers in the cloud, and then migrating and adjusting existing network connectivity to support them.

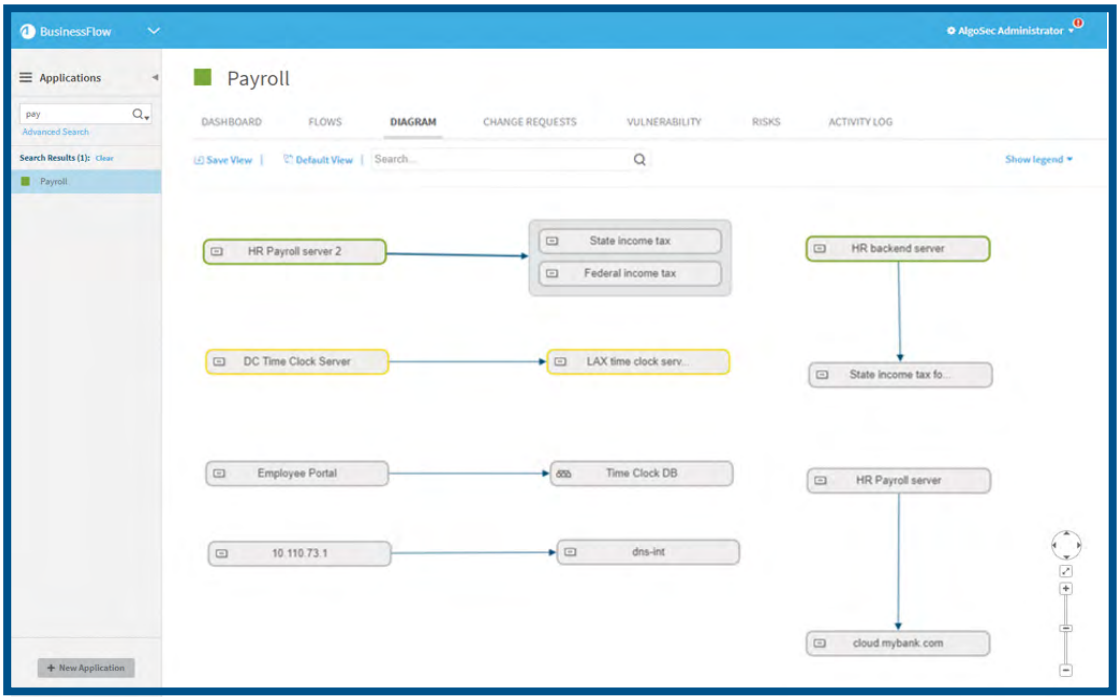
Moreover, for each business application to run smoothly, all teams within the IT organization need to collaborate, align, and communicate their needs in a common language. To achieve this, an application-centric approach to security policy management is needed.

Business-Driven Application Visibility add-on for AlgoSec Firewall Analyzer

AlgoSec manages security policies from the perspective of the business applications that they support, in addition to the networking attributes used to enforce them. With AlgoSec AppViz add-on, all business applications are discovered, identified, and mapped, providing visibility of the network connectivity flows associated with each business application, which in turn provides critical security information regarding the firewalls and firewall rules supporting each connectivity flow.

Automatic Mapping of Application to the Firewall Rule that Serves It

Firewall rules support applications or processes that require network connectivity to and from specific servers, users and networks. AlgoSec AppViz add-on automatically associates the relevant business applications that each firewall rule supports, enabling you to review the firewall rules quickly and easily.



Associate Vulnerabilities to Business Applications and Firewall Rules

Prioritizing your risk based on what your business values most — the applications that power it.

Using automatic integration and mapping of vulnerabilities from the leading vulnerability scanners to their business applications — including servers and complex connectivity flows, and provide a security rating for every business application.

Application-Centric Visibility

AlgoSec Auto-Discovery is an innovative technology that automatically identifies all your enterprise applications and services and their connectivity flows, and quickly generates an up-to-date connectivity map of your applications — without requiring any prior knowledge or manual configuration by your security, networking or applications experts. It provides full visibility of your network security environment, including firewalls and the firewall rules that determine network traffic. This facilitates a deep understanding of the implications of any planned changes to application connectivity and how to configure the firewalls appropriately with these changes.

Enhance Compliance

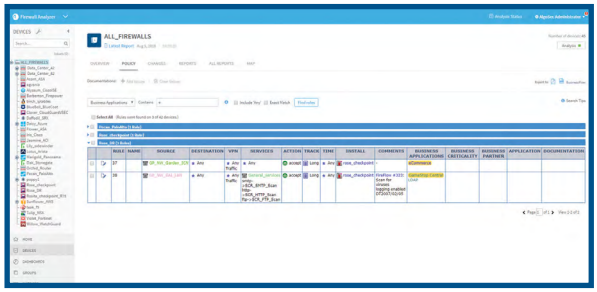
Having full knowledge of all business applications aids the company in their adherence to different compliance requirements. For example, PCI DSS requires customers to audit all the applications that fall within the scope of the regulation. This information is easy to determine through application network connectivity mapping.

Accelerate Troubleshooting

Application network connectivity mapping can reveal whether an application outage is due to issues with the network. For example, an employee opens a support ticket when he's not able to connect to the CRM application. Typically, the ticket will first go to the network team to determine if the problem is network related. Using the application-centric approach with its associated mapping, it is immediately clear whether the issue is network-related. If it is, it can be easily dealt with. If not, it can be sent to the appropriate department, thus saving time and resources.

Impact Analysis

Application network connectivity mapping provides a clear picture of the impact on business applications, of any planned changes to the network. This includes firewall changes, or other changes that may cause network downtime. Mapping will enable the implications of the changes to be fully understood and consequently downtime, for example, can be scheduled when it will have minimum impact on customers, partners, or employees.



Comprehensive Support for Heterogeneous Environments

AlgoSec seamlessly integrates with all leading brands of traditional and next-generation firewalls and cloud security controls, as well as routers, load balancers, web proxies and SIEM solutions, to deliver unified security policy management across any hybrid cloud, multi-cloud, SDN and on-premise enterprise network. Additional devices can be added via the AlgoSec Extension Framework.

amazon web services · AVAYA · JUNIPER · Azure · Check Point · cisco · splunk> · F5 · FORTINET
HUAWEI · IBM · BLUE COAT · BROCADE · paloalto · slack · DELL SONICWALL · vmware · WatchGuard

algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

AlgoSec.com