DoyleResearch

Orchestration and Automation of Network Security

Sponsored by Gluware

The popularity of virtualization, containers, DevOps style applications, and hybrid cloud deployments continue to increase the complexity of IT operations. The links between the network and sophisticated security appliances such as next generation firewalls is critical to detect anomalous traffic flows and identify malicious attacks. To secure its operations, IT needs the ability to track traffic flows, automate change requests, segment the network, and audit for compliance.

Network Security Challenges

IT operations are becoming increasingly complex to manage given the trends of virtualization, use of containers, pervasive mobility, and adoption of cloud-based applications. It is the network that connects these distributed applications and provides the means to track, audit, and segment traffic. The connection between the network and security appliances (e.g. NG-Firewalls, IDS/IPS, UTM, etc.) is critical to maintain appropriate security, especially in a highly distributed, mobile world where the security perimeter has largely been eliminated.

Enterprise networks typically comprise a range of ethernet switches, routers, and network security elements from a variety of suppliers. Each network element has a unique management and configuration system. The complexity of the rules for network behavior provides an environment that is difficult to administer and ripe for configuration error.

Human error through manual configuration still accounts for significant network downtime. The vast majority of network changes are still manual and these manual processes present significant risk in terms of network outages and security vulnerabilities. According to Gartner, the vast majority of firewall breaches are caused by misconfiguration – largely due to manual error.

Single vendor management platforms are not providing the unified solution required to push security policies to network devices. Network automation is an elusive goal given current management tools and legacy scripting.

Implementing Intent-Based Networking

Software defined network (SDN) technology has emerged over the last five years to break down the barriers of physical networks and network security. Organizations can deploy SDN to deliver intent-based networking which enables orchestration and automation of previously manual processes across physical and virtual domains. SDN provides centralized control and management to oversee activities on the network. For example, IT personnel can automatically push changes in access control lists from a centralized console to all distributed network/security elements.

Gluware Orchestration and Automation for Network Security

Gluware enables customers to automate and orchestrate changes across a multi-vendor network at scale. With Gluware's network feature modeling and intelligent intent-based orchestration engine IT operations can rapidly automate their existing network.

IT needs to be able to deploy security policies centrally across the multi-vendor routing/switching and firewall domains. Gluware is providing this capability enabling whitelisting to permit good traffic as well as capabilities to lock down the network on demand. Gluware can identify unauthorized configuration changes by enabling configuration detection across network devices. It provides audit and logging of changes to network and firewall devices to ensure proper configuration and assist with compliance requirements. Gluware enables the centralized push of new security policies to Cisco and Juniper routers and switches as well as

Fortinet and Palo Alto firewalls, thus automating the update of access control lists (ACLs). See Figure 1.

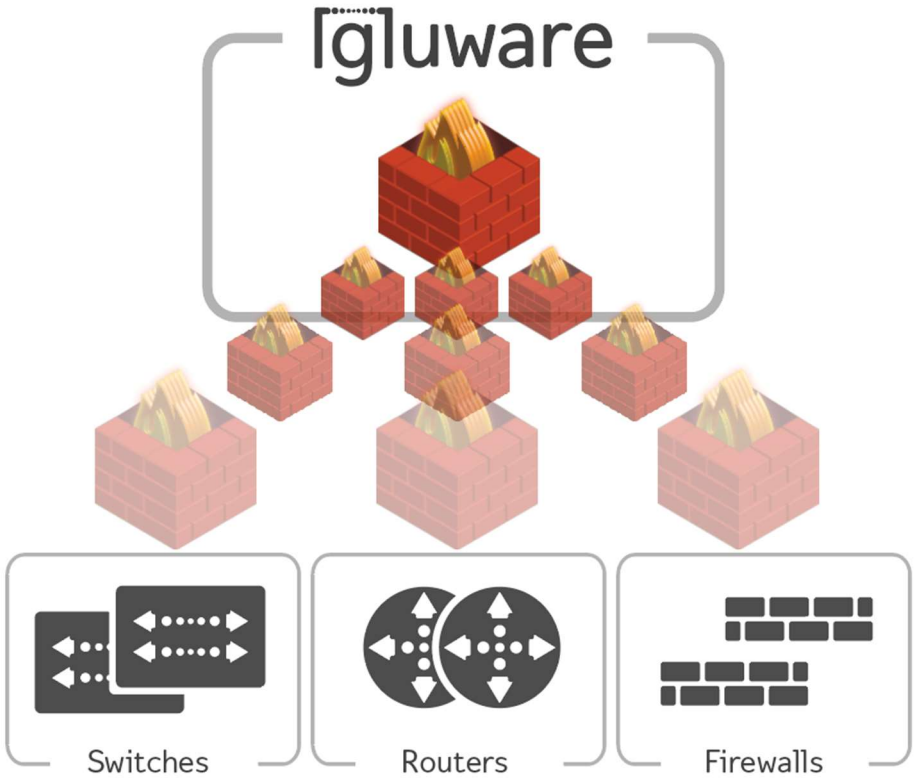

Figure 1

Recommendations for IT Leaders

To enable a DevOps style of application development in virtualized environments deployed across hybrid cloud platforms, IT organizations must embrace multi-vendor network orchestration and automation. SDN technologies with intent-based capabilities provide the tools to:

- Centrally manage/push required network changes (e.g. ACLs)
- Provide Change management – logging/track all network changes, ID the last changes
- Provision explicit black list and white list access rules
- Provide network segmentation to protect vital assets

IT organizations should select SDN tools that support multi-vendor network and security environments, that are easy to learn and use, and powerful enough to automate manual network tasks. These tools should enable a phased migration towards software-based networks with centralized management, orchestration, and automation benefits.

Meet the Author

Lee Doyle is Principal Analyst at Doyle Research, *providing client focused targeted analysis on the Evolution of Intelligent Networks. He has over 25 years' experience analyzing the IT, network, and telecom markets. Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies, and IT-Telecom convergence. Before founding Doyle Research, Lee was Group VP for Network, Telecom, and Security research at IDC. Lee contributes to such industry periodicals as Network World, Light Reading, and Tech Target. Lee holds a B.A. in Economics from Williams College.*