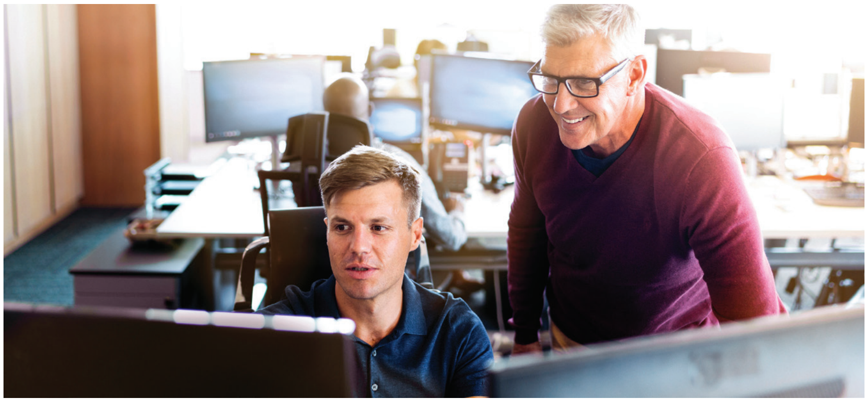
FIREMON GLOBAL POLICY CONTROLLER + VMWARE NSX

Enterprise IT organizations that aspire to deliver application services with cloud-like speed and agility are moving to VMware NSX. FireMon Global Policy Controller, coupled with VMware NSX, can help you manage change automation, enforce microsegmentation and improve your organization's security posture during this transition.



THE CHALLENGE

Network virtualization calls for speed and agility of IT operations

VMware NSX provides network virtualization, disaster recovery, and security to organizations that aspire to deploy applications with speed and provide an improved application experience to users. NSX streamlines network security operations across heterogeneous environments – the data center and the private, public and hybrid clouds. It provides IT organizations with critical speed and agility along with improved security posture. Organizations can create segmented zones and protection rules that can apply to virtual machines (VMs) or groups of VMs via the NSX distributed firewall. NSX also enhances agility by enabling application of security and optimization services at the VM level, and by enabling automation in fulfilling requests from application developers and DevOps.

However, network virtualization also calls for simplified and automated administration as even medium-sized organizations with fewer than eight firewalls can transform into a single NSX environment with 20, 50, 100, 200, or more secure zones with individual policies to manage. The increased security policy management requirements of NSX environments can introduce significant risk and impact agility.

WHY GLOBAL POLICY CONTROLLER?

Manage a single, global policy across a hybrid infrastructure and ensure it is all within compliance boundaries to move rapidly without introducing new security risk.

- Security configurations generated in seconds, not days
- Global policy visibility and management of network security posture
- Automatic cleanup of device rules that are no longer required
- Continuous security control across on-premises and virtual platforms
- Support for new architectures such as microsegmentation and Zero Trust
- Seamless integration with FireMon Security Manager monitoring and reporting tools

FIREMON

THE SOLUTION

FireMon Global Policy Controller + VMware NSX

Automation, specifically firewall rule management automation, is critical to the success of hybrid cloud environments at scale. As more firewall rules are created and changed within NSX, management complexity increases. Customers risk taking on significant overheads in firewall change tickets, which can result in misconfigurations caused by human error. To ensure that the benefits of microsegmentation are realized without an increased investment in staffing or risk of human error, firewall rule management should be integrated into the server automation and deployment process.

FireMon's Security Manager and Global Policy Controller (GPC) together enable and deliver automation both to existing physical firewalls tied to NSX and for all policies built in the NSX distributed firewall. The combined solution allows you to normalize all firewall configurations, make decisions on firewall rules based on the business intent of the deployment, and automate the creation, change or teardown of these rules as the environment evolves and scales – all through a single platform.

Using GPC's optimized NSX integration, you can automate firewall rules across your secure private cloud. Our proprietary compute engine allows you to leverage multiple sources of intent to compute firewall changes and automatically deploy new virtual resources, change existing resources, and remove obsolete or redundant firewall rules.

Once you have built intent into GPC, firewall rules are created (or removed) in NSX for each request that comes in, without having to enter rules into NSX's firewall manager. GPC is also a critical piece of the continuous integration and continuous delivery (CI/CD) model, allowing rules to be created by intent signaled in the resource request itself, without requiring operations personnel to log into either GPC or NSX to create rules.

Customers with Agile and CI/CD models can design automation in the development process itself to ensure agility, faster time-to-market, and reduced demand on operations personnel.

Your developers and DevSecOps teams can use a variety of tools to automate approved port access and distributed firewall rule creation without additional overhead for network operations by leveraging FireMon's integrations with Ansible, Puppet, Chef, and open APIs. Our security policy orchestration platform delivers:

- Efficient, compliant security configurations in seconds
- Global visibility and management of network posture
- Continuous security control for traditional and virtual platforms

Regardless of the type of request, GPC can interpret and compute the necessary changes, validate compliance, and push policy or create exception alerts across VMware NSX or multi-vendor environments.

SECURITY MANAGER

+

GLOBAL POLICY CONTROLLER

=

ENABLE AND DELIVER AUTOMATION TO PHYSICAL FIREWALLS TIED TO NSX AND FOR ALL POLICIES BUILT IN THE NSX DISTRIBUTED FIREWALL

WHO IS FIREMON?

FireMon delivers continuous security for hybrid enterprises through a powerful fusion of vulnerability management, compliance and orchestration. Since creating the first-ever network security policy management solution, FireMon has continued to deliver real-time visibility and control over complex network security infrastructures, policies, and risk postures for more than 1,700 customers around the world. For more information, visit **www.firemon.com.**