

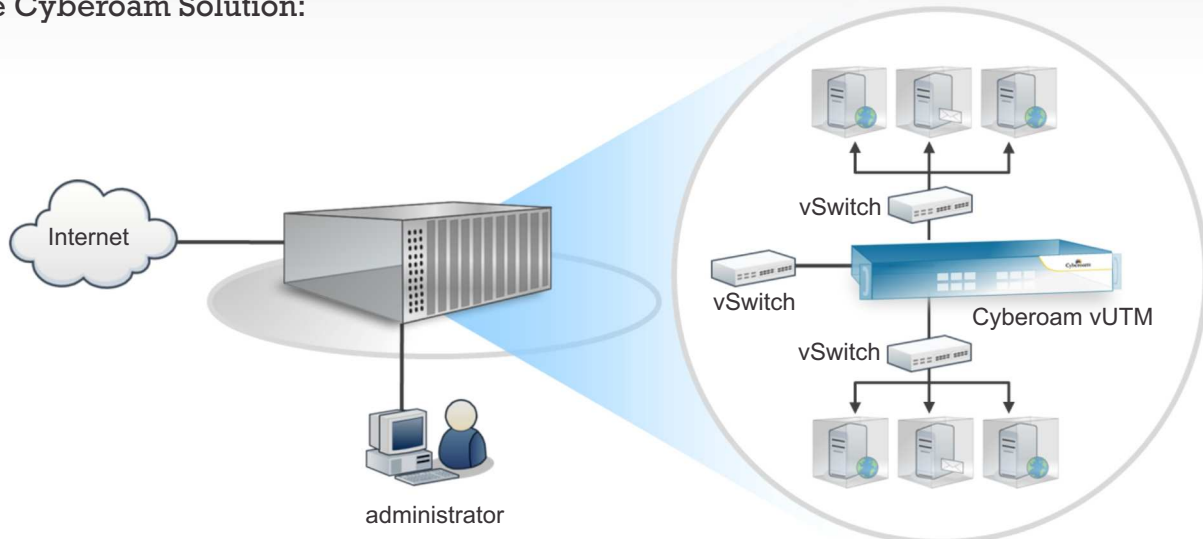
A growing business faces increasing demand for consumption of IT resources. The IT teams are constantly under pressure for generating more computing power out of existing server infrastructure. A common virtualization strategy adopted by such organizations is to virtualize data center. Data center virtualization helps organizations with greater efficiencies and performance, besides helping them reduce infrastructure complexities, management costs, power and cooling costs. One of the many benefits of virtualization is driving up the overall server utilization by intelligently utilizing un-used CPU cycles to address increased demand instead of adding new servers, like in the case of physical appliances.

Security Challenges of Virtualization:

Virtual networks are prone to attacks like hyperjacking; exploits attacking vulnerabilities in hypervisor, management console, hypervisor & Guest OS; security risks arising out of loss of separation of duties between security/network security and operations; and attacks on virtualized servers and web-facing applications.

An external hardware security appliance lacks the ability to scan inter-VM traffic, leaving organizations unaware of any security breaches in their virtualized infrastructure. As security policies cannot be applied between virtual entities using an external hardware security appliance, a single compromised virtual machine can infect the entire data center, bringing down the business. Also, the organization will have no logs and reports on network traffic to support forensic analysis in case of security breach and to display regulatory compliance.

The Cyberoam Solution:



Placed within the virtualized environment, Cyberoam virtual UTM appliances can scan inter-VM traffic and allow granular firewall and security policy enforcement on inter-VM traffic, besides allowing logs and reports, which enables the virtual data center to display and manage compliance requirements. The virtual security appliances ensure comprehensive security of the virtual data center by offering multiple security features, including IPS and

Web Application Firewall, integrated on a single virtual appliance.

Cyberoam virtual UTMs enable administrators to segment the management console in DMZ, route all traffic through Cyberoam virtual UTM appliances, and also enable separation of administrator duties with role-based administrator controls.