

Granular Security and Threat Mitigation in the Virtual Data Center

Within the physical data center, a multi-layer security architecture is critical to establishing corporate IT security posture, and for compliance to regulatory standards. Physical firewall devices are deployed to provide segmentation between departments, thereby controlling access to servers, databases, transaction systems, and other IT resources. VPN and remote access gateways enable access to applications and resources while maintaining data privacy and preventing data leakage. IPS systems round out a multi-layer security architecture by detecting intrusions and preventing propagation of attacks.

The virtual data center is no different from the physical data center in terms of security policy – virtual data centers must meet the same strict information security requirements adhered to in physical networks. This includes corporate security posture, regulatory compliance, departmental segmentation, data privacy, and threat awareness and mitigation. These requirements also extending into remote sites and user location that are now accessing virtual datacenters.

Vyatta Network OS in the Virtual Data Center

The Vyatta Network OS enables a multi-layer security approach in the virtual data center, by delivering comprehensive network security in a single virtual package, deployable in any hypervisor environment.

Vyatta’s enterprise-class SPI firewall enables IT to define and enforce access control policies and segment departments while isolating multi-tenant virtual infrastructure such as VDI, sensitive HR databases, or financial transaction systems. Zone-based deployment preserves existing PCI compliance, and also enables DMZ servers to be hosted securely in the virtual environment, without the need to restructure IT policy or firewall architecture.

For remote sites and the mobile workforce, access to VDI and virtual data center resources is transparent – 256-bit AES encryption for site-to-site VPN and SSL-based OpenVPN ensure authenticated data privacy across the WAN, ensuring HIPAA compliance.

With Vyatta, virtual data center migration is no longer a high-risk investment relying on unproven enforcement methods – the proven trust model of compliance is preserved throughout migration, enabling complex network topology and multi-tiered applications to transfer intact, directly from the server rack into the virtual host.

For defense-in-depth, Vyatta’s Snort VRT engine delivers best-in-class visibility for monitoring threats and suppressing attacks before they can propagate beyond a user-defined network segment.

Vyatta delivers the only multi-layer virtual network security solution that maintains compliance and enables instant migration of complex, layered firewall architectures from the physical network into any virtual data center, without compromises.

