Complete Security and Compliance for Virtual Environments

Vyatta takes the concept of virtualization beyond just applications and operating systems and allows enterprise IT to also virtualize network components that were traditionally hardware-bound. This application-centric approach to networking allows for complete migration of routing, firewall, VPN and more to virtual environments, ensuring that businesses can enforce the same security and compliance requirements of their physical network in next generation virtual environments.

Vyatta embraced the shift to virtualization as a network delivery platform with its first network virtual machine back in 2006. As the trend evolved, Vyatta has been at the leading edge of delivering networking to virtualization enabled devices and architectures such as:

<table>
<thead>
<tr>
<th>Network Virtualization Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter Virtualization</td>
</tr>
<tr>
<td>Cloud Computing</td>
</tr>
<tr>
<td>Edge Consolidation</td>
</tr>
</tbody>
</table>

Vyatta Network OS virtual machines tightly integrate enterprise-class routing, security and traffic management technologies into virtual machines that are optimized for the highest possible throughput and security in VMware, Microsoft Hyper-V, Citrix Xen/XenServer and Red Hat KVM hypervisor environments.

The Key Benefits of Vyatta Network OS Virtual Machines:

Complete Routing & Security: The Vyatta Network OS includes stateful firewall, IPSec and SSL-based VPN, web filtering, dynamic routing, Policy-Based Routing (PBR) and underlying services like NAT, DHCP and more as IPv6 ready pre-packaged virtual machines.

Platform Independence: Vyatta Network OS allows for a single virtualized routing and security package to be installed on VMware, Microsoft Hyper-V, Citrix Xen/XenServer and Red Hat KVM virtualization hypervisors.

Elasticity / Scalability: Vyatta Network OS removes the limitations of box-bound network devices by offering the ability to scale performance, add users or add instances as in seconds and minutes, not hours, days or weeks.

Physical-to-Virtual Migration: Using the Vyatta Network OS enables simple, straightforward migration from physical networks to the virtual environment without network redesign or compromising existing security policies and compliance.

Open API: Vyatta’s REST based Remote Access API easily integrates with any third party management, orchestration, or provisioning system to enable complete remote control of all configuration and logging within the Vyatta system.

Utility Licensing: Vyatta VSPL licensing offers pay-per-use billing options that map to common cloud computing consumption models.

“Vyatta’s software allows any solution provider or network administrator to go to the next level of virtualization in the data center – by virtualizing network infrastructure... Vyatta’s software solution allows solution providers and network administrators to manage their networks the same way they manage all other virtualized components.”

“Service providers that are able to leverage advances in virtualization and networking are in a unique position to bring to market the next-generation of premises-based equipment and services for Enterprise branch offices. This technology will simplify the management and deployment of edge devices and services and fundamentally alter the economics of managed service delivery.”

“Security is always a foremost concern, even for our training and development systems, and Vyatta’s router and firewall gave us the perfect blend of security and accessibility. Vyatta was the only solution we found that allowed us to mirror the architecture of our virtual training and development systems to that of our production environment.”

“If we had used physical network infrastructure for this, we would have sacrificed a lot of manageability and driven up our costs. I can recommend Vyatta whole-heartedly to any organization that is looking for a robust networking and security solution that plays well in a virtualized environment.”

“Vyatta was the only solution we found that allowed us to mirror the architecture of our virtual training and development systems to that of our production environment.”
VIRTUAL GATEWAY – Routing, Firewall, VPN

In traditional enterprise datacenters it’s common for routers, firewalls and VPNs to be deployed at various places to ensure data security for sensitive applications, databases and transaction systems. When consolidating business resources in virtual environments those sensitive resources are commonly condensed to a single server or pool of servers, removing the cable and rule-based physical isolation policies that kept them secure and isolated. To address issues related to both internal security (HR databases, financial systems) and external compliance (PCI, HIPAA) in a virtual environment, it is a requirement that a virtual networking solution be deployed that supports the same security policies and architectures.

The Vyatta Network OS is a single virtualization optimized solution that includes stateful firewall, IPSec and SSL-based OpenVPN and more. Vyatta Network OS virtual machines can be employed as a virtual gateway on per server basis to provide hypervisor and application protection by establishing zone or rule-based firewalling, detailed traffic inspection, and secure remote access.

COMPLEX N-TIER AND MULTI-TENANT SECURITY

Designing a network infrastructure for a virtual datacenter or cloud should allow for a complete migration of physical security, traffic management and compliance in the network design without compromise. Most networks are not single-tier flat architectures and virtual and cloud environments should not be subject to that limitation. Vyatta’s deep roots in delivering a complete Layer 3+ network OS offers customers a single solution that can route and secure traffic in a single flat network or create multi-tier environments complete with separate security policies.

An additional complexity that must be addressable in virtualization is the need to isolate applications and workloads in a shared resource environment. A common concern in cloud computing and in virtual datacenters is that an application or pool of applications sharing a single server environment may not have a common business unit owner or end-user customer owner, therefore these applications require complete isolation and protection from other users with access privileges to adjacent and common resources.

NETWORK EDGE CONSOLIDATION

The proliferation of single-purpose devices has created a complex, expensive network edge in the distributed enterprise, branch office and campus. The average branch has some combination of router, firewall, VPN, WAN optimization, web filtering and more, many of which are single purpose devices. Virtualization platforms create an opportunity to significantly reduce edge network device sprawl by employing network virtual machines instead of single-purpose devices.

The Vyatta Network OS provides the foundation for any best-of-breed consolidated edge networking solution by offering the industry’s most complete Layer 3+ virtualization optimized solution. A real world examples of this is:

Custom Edge Networking Solutions: Vyatta virtual machines have enabled customers around the world to simplify edge networking including Tier 1 global telecoms building generation business-class CPE devices and Fortune 500 enterprises who require flexible best-of-breed edge services for their business.
The Vyatta Network OS is a scalable, integrated, enterprise-class networking solution that delivers advanced routing and network security functionality for physical, virtual and cloud networking environments. The Vyatta Network OS includes dynamic routing, stateful firewall, VPN, threat protection, traffic management and more in a package that is optimized to take advantage of multicore x86 processing power, common hypervisor platforms and emerging cloud architectures. All features are configured through Vyatta’s familiar, networking-centric CLI, web-based GUI or third party management systems using the Vyatta REST-based Remote Access API.

**Vyatta Network OS Highlights**

» Advanced IPv4 and IPv6 routing (BGP Multipath, PBR, OSPF)
» Stateful firewall
» IPv6 compatible
» Linux-based extensible network OS
» IPSec & SSL-based OpenVPN
» Secure Web filtering
» VMware, Hyper-V, Xen/XenServer, Red Hat KVM Ready
» Restful API, CLI, Web GUI
» World-class 24x7 support

**Subscription Support Packages**

**BASIC:**
» Vyatta Software Updates
» Security Alerts & Patches
» Bug Fixes
» Proactive Notifications
» Online Documentation
» Knowledge Base Access

**ENTERPRISE:**
Local Features Plus
» 5 X 12 Phone Support
» Web-based Ticketing
» Customer Hot Fixes
» Case SLA - Severity Based
» Vyatta University Training
Getting Started Bundle

**PREMIUM:**
Enterprise Features Plus
» 7 X 24 Emergency Phone
» Case SLA - Priority Response

**Network Connectivity**
At the core of the Vyatta system is a complex routing engine with full support of IPv4 and IPv6 dynamic routing protocols (BGP Multipath, OSPF, RIP) and Policy-Based Routing. Vyatta systems include support for 802.11 wireless, Serial WAN Interfaces and a wide variety of 10/100 thru 10Gb Ethernet NICs.

**Traffic Management**
The Vyatta system provides a wide variety of QoS queuing mechanisms that can be applied to inbound traffic and outbound traffic for identifying and prioritizing applications and traffic flows.

**Firewall Protection**
The Vyatta firewall features IPv4/IPv6 stateful packet inspection to intercept and inspect network activity and protect your critical data. Vyatta advanced firewall capabilities include stateful failover, zone and time-based firewalling, P2P filtering and more.

**High Availability**
Mission critical networks can deploy Vyatta with the confidence that high availability and system redundancy can be achieved through a number of industry standard failover and configuration synchronization mechanisms.

**IPv6 Compatibility**
Vyatta Subscription Edition software is the only software-based routing and security solution with proven IPv6 functionality and interoperability, ensuring a future-proof investment in a solution that offers a simplified migration path from IPv4 to IPv6.

**Additional Protection**
Vyatta systems offer an additional level of proactive threat protection with integrated secure web filtering rules available as Vyatta PLUS subscription services.

**Secure Connectivity**
Establish secure site-to-site VPN tunnels with standards-based IPSec VPN between two or more Vyatta systems or any IPSec VPN device. Or provide secure network access to remote users via Vyatta’s SSL-based OpenVPN functionality.

**Administration & Authentication**
Vyatta systems can be managed through our familiar network-centric command line interface, web-based GUI or through external management systems using Vyatta’s Remote Access API. All network management sessions can be securely managed using SSHv2, RADIUS or TACACS+.

---

Vyatta Network OS for Network Virtualization

 Vyatta Data Model

FLEXIBLE SYSTEM MANAGEMENT

SUBSCRIPTION-BASED SECURITY

COMPLETE IP ROUTING & SECURITY

VIRTUALIZATION OPTIMIZED