

Secure Networks™ for Virtual Data Centers

Ensuring security, mobility, manageability, quality and reliability of virtualization technologies

The Data Center is the repository for all organizational intellectual property where mission critical applications are running and downtime can cost an enterprise millions of dollars per minute.

According to industry estimates more than 80 percent of IT budgets are dedicated to sustaining existing application environments within the Data Center, as a consequence there are wide-scale trends to reduce Total Cost of Ownership (TCO) by improving Data Center operational efficiencies through server, and storage consolidation. Data Center power and cooling costs are increasing exponentially, in many instances exceeding hardware costs as rising energy prices focus attention on environmental efficiency. For these reasons, and others, virtualization technologies are being deployed to drive efficiency and effectiveness of computing and storage resources.

Security threats to the Data Center are many and varied, they continue to morph and intensify and it is possible for a single vulnerability to imperil a corporation's viability. Traditional network infrastructures and security overlays are insufficient to meet the increasingly dynamic and converged deployments demanded by the virtualization of compute and storage resources. The Enterasys Secure Virtual Data Center Solution offers granular, flow-based visibility and control of individual users, applications and virtual machines. Network-based security, quality of service, and bandwidth control of each virtual server on a single or cluster of physical servers embraces the mobility, flexibility and computing efficiency advantages of Data Center virtualization while protecting the confidentiality, integrity and availability of information through assessment, authentication and authorization.

The key building blocks of the Enterasys Secure Virtual Data Center include:

- Security-enabled infrastructure using Matrix™ N-Series flow-based switches and Matrix™ X high performance routers, providing top-of-rack, end-of-row, and network core connectivity
- Advanced Dragon® security applications for intrusion detection/prevention, network access control and security information management
- Centralized visibility and control through NetSight® management applications that enforce role-based policies and automate corrective actions

Reliability is assured, based upon Enterasys Matrix™ N-Series switches whose architecture provides N:6 hardware availability and no single point of failure. While the Matrix™ X core routers include full hardware redundancy for all major subsystems, including control plane, management modules, switch fabrics, power and cooling. Furthermore, business continuity is enhanced by software resiliency features that enable firmware upgrades and restarts without impacting traffic flows. All Matrix™ switches and routers provide a plethora of industry standard Layer 2 and 3 resiliency features such as 802.1w Rapid Spanning Tree, Link Aggregation Groups, Virtual Router Redundancy Protocol (VRRP) and Equal Cost Multi-Patch OSPF. In the event of physical server or virtual machine failure, Enterasys Secure Networks support virtual machine mobility without requiring manual reconfiguration of the network or interrupting user access to information.

Security is assured as only authorized users and protocols can connect to authenticated virtual machines and associated virtualized storage resources. An Enterasys Matrix™ N-Series switch can discover, authenticate, and prioritize up to 1,000 virtual machines attached to a single gigabit or ten gigabit Ethernet network interface. Network behavioral analysis integrated with intrusion detection/prevention capabilities prevent the hosting or downloading of inappropriate or illegal content as well as the proliferation of worms or viruses. Enterasys Dragon software proactively prevents, intelligently senses and automatically responds to network security threats. Enterasys' Secure Virtual Data Center solution allows organizations to enforce security and application provisioning on mission critical resources proactively and effectively. The benefit of this is a

Solutions At-A-Glance

Features

- Granular, flow-based visibility and control of individual users, applications and virtual machines
- Authentication to ensure only authorized virtual machines speaking appropriate protocols are granted access
- Prioritization of specific voice/video/data and iSCSI applications and protocols through end-to-end QoS
- Authorization of access to specific virtual machine resources based on role and privileges
- Audit history of virtual machine mobility and current location
- Network link aggregation and load balancing for resiliency and scalable capacity
- Open-architecture, standards-based interoperability

Benefits

- Compelling Total Cost of Ownership
- Prevent rogue connectivity of virtual machines or storage arrays to the Data Center infrastructure
- Optimize performance for Service-Oriented Application Architectures
- Compliance with acceptable user, data privacy and/or other regulatory requirements
- Allows Compliance Reporting for all hosted services in the Data Center
- Disaster recovery and distributed fault tolerance to ensure business continuity
- Detects and responds to (distributed) Denial of Service attacks
- On-demand provisioning of additional capacity to meet business demands
- Integrated accounting and capacity planning
- Add policy-based network security and Quality of Service to the Data Center while protecting existing investments

**There is nothing more important
than our customers.**

security centric Data Center which provides network integrity, guarantees delivery of critical business applications, while eliminating services that are undesirable or prohibited.

Mobility is critical to virtualization environments to ensure continuity of operations in the event of hardware failure or controlled shut-down of a server to conserve energy during low demand time periods. Running server virtualization software on server farms connected to shared storage can also provide several advantages. By placing virtual machine virtual disks on storage area networks (SANs) accessible to all virtualized servers, virtual machines can easily migrate between servers as needed for load balancing or failover. Enterasys Matrix™ N-Series switches can enable virtual machine mobility automatically without requiring manual reconfiguration of network interfaces on either the physical server or network device as policies dynamically adapt on-demand. Real-time location of a virtual machine and associated application services, as well as an audit history of its mobility, is available through Enterasys NetSight software.

Data Center Management is more than monitoring whether a server is up or down, it also includes easily provisioning, monitoring and measuring against required Service Level Agreements (SLA'S), accounting for system usage and providing audit trails. Enterasys' NetSight suite of management applications delivers policy-based visibility and control over virtualized Data Center infrastructure to ensure mission critical applications are delivered reliably and enabling organizations to manage their Data Center network as a cohesive whole, rather than as a disparate set of individual components. Integrated Management of virtual servers, storage arrays and the network infrastructure will enable full realization of the ease-of-management promise of the Virtual Data Center.

Scalability, Performance and High Port Density of Matrix™ switch/routing solutions provide significant benefits in Data Center design. Bandwidth, latency, and buffering all become critical design constraints and support for high density Ten-Gigabit connectivity is fast becoming the standard deployment model for high-capacity servers and storage arrays. With in excess of 1000 ports of Gigabit Ethernet and 120 ports of Ten-Gigabit Ethernet per rack, Matrix™ switch/routing solutions enable less connections to fewer overall devices, minimizing sprawl and having a significant impact on cabling and power requirements. Additionally,

the architectural design of Matrix™ solutions guarantee support for next generation switching technology, offering even higher port density and performance, ensuring industry leading Return on Investment.

Quality of Data Center virtualization services is assured as granular end-to-end QoS capabilities prioritize application traffic throughout the network. Enterasys Matrix™ N-Series switches feature a unique ability to separately secure and prioritize each virtual machine connected to a single network port to provide the business with granular flow-based visibility and control over individual voice, video and data conversations for each user and application. Network usage is also monitored and can be used to optimize traffic flows and detect mis-configurations.

Conclusion

Enterasys is uniquely positioned to continue to provide industry leadership in the evolution of the Secure Virtual Data Center. Based upon a select combination of Enterasys' Secure Network™ components, the Secure Virtual Data Center implementation from Enterasys provides an holistic enterprise security framework delivering:

- Cost sensitive server and storage infrastructure
- 24x7x365 application availability
- Significant and measurable enhancements to the overall security of the network infrastructure
- State of the art common management and policy enforcement
- Increased ROI and reduced cost associated with securing the virtual Data Center environment
- Operational efficiencies gained by centralizing Data Center administration & support
- Investment protection for Data Center network infrastructure platforms, offering long term deployment lifecycles
- Adherence to regulatory compliance standards via an architectural approach to network security and business continuity.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

