White Paper

Five Steps For Securing The Data Center: Why Traditional Security May Not Work

What You Will Learn

Data center administrators face a significant challenge: They need to secure the data center without compromising the performance and functionality that new data center environments enable. Many are looking to secure the data center using solutions designed for the Internet edge, but these solutions are not enough. The data center has unique requirements around provisioning, performance, virtualization, applications, and traffic that Internet-edge security devices are simply not designed to address.

Securing the data center requires a solution that can:

- Provide visibility and control over custom data center applications
- Handle asymmetric traffic flows and application transactions between devices and data centers
- Adapt as data centers evolve: to virtualization, software-defined networking (SDN), network functions virtualization (NFV), Cisco Application-Centric Infrastructures (ACIs) and beyond
- Address the entire attack continuum: before, during, and after an attack
- Integrate with security deployed across the entire network
- Support geograpically dispersed inter-DC traffic and deployments, including private, public and cloud environments

Prime Target for Compromise: The Data Center

Many modern cybercrime campaigns are designed specifically to help adversaries reach the data center, where high-value data, including personal customer data, financial information, and corporate intellectual property resides.[1] However, securing the data center is a challenge. Asymmetric traffic, custom applications, high traffic volumes which need to be routed out of the compute layer and up to the data center perimeter for inspection, virtualization across multiple hypervisors, and geographically disparate data centers all make securing the data center difficult for security solutions that have not been designed for those purposes. The result is gaps in security coverage, severe impacts on data center performance, the need to compromise data center functionality to accommodate security limitations, and complex provisioning of security solutions that undermines the ability of the data center to dynamically provision resources on demand.

Meanwhile, the data center is evolving, migrating from physical to virtual to next-generation environments, such as SDN and ACI. Data center traffic is already growing exponentially, driven largely by increasing cloud utilization and the emerging Internet of Things (IoT) environment, where the Internet and networks expand to places such as manufacturing floors, energy grids, healthcare facilities, and transportation.

[1] Cisco 2014 Annual Security Report: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063.

Cisco forecasts that by 2017, 76 percent of data center traffic will stay within the data center and will be largely generated by storage, production, and development data in a virtualized environment.[2] Gartner projects a 3000 percent increase in data center connections per second by the end of 2015.[3]

Modern data centers are already providing a host of applications, services, and solutions to the business. Many organizations rely on services that have been deployed across geographically dispersed data centers to support their growing cloud computing and traffic needs. They also need to address strategic initiatives such as big data analytics and business continuity management that make the data center an even more critical part of the enterprise backbone. But this also solidifies the data center as a prime target for malicious actors designing increasingly sophisticated threats meant to evade detection in order to access data center resources. All of the above means the data center will become only more difficult for security teams to monitor and protect.

Another complication for data center administrators and their teams: Provisioning and performance limitations significantly impact how security solutions, such as next-generation firewalls, are deployed and what traffic they can inspect. Security cannot undermine data center performance. In today's data center, security provisioning must occur within hours or minutes, not days or weeks. Performance must dynamically scale to handle high-volume bursts of traffic.

Five Steps For Securing The Data Center

Comprehensive data center security requires a defense-in-depth approach that can deliver in five key areas. The solution must:

1. **Provide visibility and control over custom data center applications.** Data center administrators need visibility and control over custom data center applications, not just the traditional web-based applications (for example, Facebook and Twitter) and related microapplications that traditional Internet-edge security devices inspect. Most Next-generation firewalls are designed to inspect the type of traffic that is flowing through the Internet edge, and do not secure these custom data center applications.
2. **Manage asymmetric traffic flows and application transactions between devices or data centers.** Security must be integrated with the data center fabric, not simply sit at the edge. Solutions on the edge cannot inspect both north-south (inbound-outbound) traffic and east-west (inter-application) traffic flows, and the latter represents the bulk of today's data center traffic. If application traffic must be sent to the perimter of the data center to a next-generation firewall for inspection and then routed back to the computer layer (hairpinned), the solution undermines the dynamic traffic flow that modern data centers require.

   Many next-generation firewalls cannot secure asymmetric traffic. In asymmetric routing, typical to data centers, a packet will travel a different path when returning to its source. This becomes a problem for many next-generation firewalls as they are designed to track, inspect, and manage traffic flows along a single, predictable path.

   Security solutions for the data center also must be able to handle application transactions between data centers or devices, including virtual devices. Virtual devices are just as vulnerable as physical ones, but data center security must also be able to address the unique challenges of virtual environments, including the constant workload creation, tear-down, and migration.

[2] Cisco Global Cloud Index: Forecast and Methodology, 2012-2017: http://www.cisco.com/2012–2017/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.
[3] Security Week: http://www.securityweek.com/data-centered-focusing-security-combat-rise-data-center-attacks

3. **Adapt as data centers evolve.** As data center environments migrate from physical to virtual to next-generation SDN, ACI, and NFV models, security solutions must be able to scale dynamically and provide consistent protection that can work seamlessly across evolving and hybrid data center environments. In these new data center models where virtual and physical devices are being provisioned rapidly, security rules can quickly scale out of control. Access control list (ACL) management is already a challenge for many IT teams.

   Automatic enforcement is needed as new devices are provisioned so that deployments can be reduced from days to minutes without concern for the security consequences. Similarly, the ability to deploy a single security solution across hybrid data centers, many with multiple hypervisors (virtualization machine monitors), allows IT teams to focus on data center functionality without being burdened by administrative security overhead.

4. **Address the entire attack continuum, before, during, and after an attack.** Traditional security approaches offer limited threat awareness and visibility in a data center environment, and focus primarily on blocking at the perimeter. Covering the entire attack continuum requires monitoring across a broad range of attack vectors with solutions that operate everywhere the threat can manifest itself: on the network, on endpoints, on mobile devices, and in virtual environments. A holistic, threat-centric approach to securing the data center that includes protection before, during, and after an attack, is needed to protect the modern data center and its specialized traffic.

   Traditional next-generation firewalls offer virtually no solution for identifying and mitigating stealth attacks designed to slip past defenses, cannot provide remediation and analysis after an attack has been stopped, and are unable to track and secure the sort of asymmetric traffic data centers generate. They are almost exclusively defensive tools, yet they also cannot defend against emerging, unknown threats targeting vulnerable servers, unique applications, and valuable data.

5. **Protect the entire network.** Any data center security soution must acknowledge the remote user's need to connect directly to a critical data center resources.It needs to provide transparency between the remote user and data center resource, yet is part of a complex network environment extending through branch offices, across the core, into the data center, and out to the cloud. The security solution must be part of the data center architecture, as well as part of a broader solution that can see both internet-based threats and targeted data center attacks, while providing seamless protection along the entire data path.

Data center security is different. To truly protect the modern data center, and new data center models that are emerging now, organizations cannot rely on a next-generation firewall alone. They need a comprehensive and integrated security strategy and architecture that provides consistent and intelligent protection across the entire distributed network, from the edge to the data center to the cloud, without undermining performance.

Securing the Modern Data Center

Cisco offers powerful tools to defend today's evolving data center environments, and not just at the data center edge. The innovative Cisco® Adaptive Security Appliances (ASA) solutions for data center security are designed to secure both physical and virtual environments and to allow organizations to migrate seamlessly from traditional to next-generation data centers for future-proof deployments, investment protection, and comprehensive protection. New additions to the Cisco ASA platform include:

- **Cisco Adaptive Security Virtual Appliance (ASAv):** The Cisco ASAv is a virtual version of the complete Cisco ASA firewall feature set, combined with dynamic scalability and simplified provisioning for virtual environments. It is designed to run on a variety of hypervisors and is independent of VMware vSwitch

technology, making it a data center agnostic solution for Cisco, hybrid, and non-Cisco environments. The flexible architecture of the Cisco ASAv means it can be deployed both as a traditional security gateway, and as a security resource for intelligent SDN and ACI environments that can be dynamically stitched directly into application service chains.

- **Cisco ASA 5585-X with FirePOWER Services:** A purpose-built data center security appliance that fully supports traditional, SDN, and ACI data center environments, the Cisco ASA 5585-X Adaptive Security Appliance with FirePOWER Services features advanced firewall and next-gen IPS security functionality, including the abilty to detect and inspect custom data center applications, combined with enhanced performance and provisioning capabilities. It provides advanced clustering capabilities for up to 16 nodes, delivering 640 Gbps of data center-class performance that can be deployed across multiple data centers. Clustered solutions can be managed as a single device to significantly reduce administrative overhead. Like the ASAv, the 5585-X is also designed to work in traditional and next-generation data center environments such as SDN, NFV, and ACI, providing consistent security across hybrid environments and seamless protection as data centers are being migrated.
- **Cisco FirePOWER Next-generation IPS:** FirePOWER is the martket-leading NGIPS, available as a physical or virtual solutions, that identifies and evaluates connections to data center resources and monitors suspicious network activity. File activity is monitored and controlled in near real time, and certain files (especially unknown files that could be malware) receive further analysis via sandboxing (isolated file exercise and behavior analysis) or lookups to the cloud (checking at-large community intelligence for reputation). Such an approach allows for fine-grained analysis and response to critical data center traffic.

Other solutions available from Cisco that help to provide comprehensive data center security include:

- **Cisco Identity Services Engine and TrustSec:** IT teams can create, share, and implement security policies dynamically as new devices or users are added to the data center environment through the UCS director. ISE can then attach Security Group Tags that contain security policy and enforcement rules directly into individual packets. In addition, thise security tagging allows data centers can be segmented based on user and device role without the complications and overhead associated with VLANs and ACLs.
- **Cisco OpenAppID technology for Snort:** IT teams can create, share, and implement application detection, and develop custom rules for custom applications in the data center, with Cisco OpenAppID technology. It is an open, application-focused detection language and processing module for Snort™, the intrusion prevention system (IPS) and intrusion detection system (IDS) developed by Sourcefire, now part of Cisco. Cisco OpenAppID is fully integrated with the Snort framework, providing administrators with much deeper awareness of the applications on their networks.

  Snort users can utilize Cisco OpenAppID detectors to detect and identify applications and report on application use. Cisco OpenAppID provides application-layer context with security-related events and helps to enhance analysis and speed remediation. It enables Snort to block or alert on detection of certain applications, helping to reduce risks by managing the total threat surface.
- **Cisco FireAMP™ and FireSIGHT™ solutions:** Advanced malware analysis and protection are required to provide a holistic, threat-centric approach to securing the modern data center—before, during, and after an attack. Cisco FireAMP products, from Sourcefire, utilizes big data to detect, understand, and block advanced malware outbreaks. It is the only solution that provides the visibility and control needed to stop threats missed by other security layers. And by combining Cisco FireAMP products with the Cisco ASA, users can provide deep inspection and protection for asymmetric data center traffic.

Cisco FireSIGHT, also from Sourcefire, provides the network visibility, context, and automation required to respond to changing conditions and new attacks. Administrators can manage hundreds of appliances centrally using the Cisco FireSIGHT Management Center.

For More Information

For more information on Cisco security products, including the Cisco ASAv firewall, the Cisco ASA 5585-X appliance, the Cisco Secure Data Center Solution, and Sourcefire security solutions, visit www.cisco.com/c/en/us/products/security/index.html.

To learn more about Snort and Cisco OpenAppID, visit www.snort.org.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-732259-00 07/14