

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), 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

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 datacenter 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 that undermines the ability to dynamically spin up data center 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.

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

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

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.



Modern data centers are already providing a host of applications, services, and solutions to the business. Many organizations need to rely on several data centers, often geographically dispersed, to support their growing cloud computing and traffic needs, as well as strategic initiatives, such as big data analytics and business continuity management. As the data center becomes an even more critical part of the enterprise backbone, it will solidify its position as a prime target for malicious actors designing increasingly sophisticated threats meant to evade detection. 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, not 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 traffic flows, and the latter represents the bulk of today's data center traffic. If traffic must be sent out of the data center to a next-generation firewall for inspection and then routed back to the data center (hairpinned), the solution undermines the dynamic traffic flow the modern data center requires.

Securing asymmetric traffic is another challenge that many next-generation firewalls are not designed to address. In asymmetric routing, found in many data centers, a packet traverses from a source to a destination in one path and takes a different path when it returns to the source. This becomes a problem when next-generation firewalls are used in the routed path. They are simply not designed to track, inspect, or manage the sophisticated and unexpected traffic flows that asymmetric routing demands.

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 devices, so data center security must be able to address the unique challenges of virtual environments, including the constant creation and tear-down of devices.

3. **Adapt as data centers evolve.** As data center environments migrate from physical to virtual to next-generation SDN and ACI 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.

³ Security Week: <http://www.securityweek.com/data-centered-focusing-security-combat-rise-data-center-attacks>

Data center administrators need to be able to create automatic policy enforcement as new devices are provisioned, so they can greatly reduce manual effort and reduce deployments from days to minutes. 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 tasks across a complex set of unrelated security devices.

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. To cover the entire attack continuum, organizations need to address 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 security strategy must acknowledge that the goal of a remote user is not to connect to the edge of the network, but to access critical resources inside the data center. Data centers are part of a complex network environment extending from remote users and branch offices, across the core, into the data center, and out to the cloud. Security for the data center must be part of the data center architecture, as well as part of a broader solution that can see the whole network and provide 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 those that are not 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 Adaptive Security Appliance:** 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 features newly 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. And like the Cisco ASAv, it is designed to work in traditional and next-generation data center environments such as SDN and ACI, providing consistent security across hybrid environments and seamless protection as data centers are being migrated.

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

- **Cisco OpenAppID technology:** 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C11-732259-00 07/14