Next-Generation Data Centers: Protect Your Networks with Cisco ASA Firewalls

The proliferation and complexity of today's cyberattacks require data centers to implement protection that provides a high level of confidence. Today's attacks target personal customer data as well as corporate intellectual property. The potential for financial losses based on theft, loss of customer trust, and damage to brands is high.

In this rapidly changing attack landscape, basic stateful firewalls are no longer sufficient to block complex attacks. Performing a deep inspection of every single network flow directly lowers application performance. Additionally, security appliance architectures must embrace virtual applications and deliver the same feature set with consistently high performance in traditional as well as next-generation software-defined networking (SDN) environments.

A next-generation data center security solution must:

- Be easily extendable
- Deliver a defense-in-depth approach to reduce application latency and improve performance
- Offer flexible insertion options
- Be highly available and elastically scalable

Flexible Performance for All Environments

The evolution of modern data centers has been shaped by multiple factors. The rapid move toward server and application virtualization in particular has required a decoupling from traditional static network topologies. Applications are no longer tied to specific computing hardware with a predetermined physical location in the data center network. The emphasis on VLAN-based segmentation with basic dynamic routing does not scale as well in the new programmable, application-centric model introduced by SDN and other approaches. And the ongoing move toward greater programmability will continue to transform data centers in the years to come.

Because many interdependent applications are now hosted on the same physical server hardware, moving these connections to external network devices becomes extremely inefficient and expensive. The application response time linearly follows network latency, and even individual consumers are starting to expect the same service levels that were once exclusive to real-time financial applications. If your customers cannot wait, your data center simply has no choice but to become even faster.

As requirements for low or zero latency become more and more pronounced in any application environment, functional modularity and minimal interdependency are mandatory for any data center security device. Even when such a device implements multiple functions, it should be architected so it can make policy decisions with the least necessary number of checks. If an inbound connection can be denied based on the reputation of a specific endpoint, there is little reason to spend firewall cycles on fully inspecting the application payload. Cisco® ASA 5500-X Series Next-Generation Firewalls rely on this defense-in-depth approach to block the most basic

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

TCP/IP attacks before deploying dedicated advanced protection modules for more detailed inspection of the remaining traffic. A Cisco ASA with FirePOWER™ Services module can use its application visibility and control (AVC) and next-generation IPS (NGIPS) capabilities to exempt certain flows from permanent deep inspection and offload them to the host Cisco ASA appliance. For instance, a high-bandwidth trusted Microsoft Active Directory backup flow can only be subjected to basic Layer 2-4 stateful checks by the Cisco ASA once the installed FirePOWER module identifies the application and confirms its safe status. This approach allows accelerating the trusted application performance and spending valuable Layer 7 inspection resources on less trusted flows instead.

Many firewalls implement most of their security features in application-specific integrated circuit (ASIC) and field-programmable gate array (FPGA) hardware modules. This approach leads to lower latency and higher performance, which is increasingly important for data center applications. However, there are many downsides to this approach. Most important, the inspection capabilities are limited to the original hardware design. When application protocols change or new security features are introduced, even the most flexible FPGAs struggle to maintain the intended performance or even support more complex operations. Such a firewall is usually forced to send such connections to the main CPU (typically called the control plane), which is not designed to handle high volumes of transit connections. As a result, the firewall performance becomes inconsistent across features and traffic profiles.

Because data center applications and the associated attack vectors change very rapidly, such hardware-centric firewalls age very quickly. The Cisco ASA 5585-X Adaptive Security Appliance implements the entire feature set in a very powerful general-purpose CPU complex, using multiple hardware processors and parallel processing threads. It offloads some basic forwarding tasks to intelligent network interface controller (NIC) modules and uses hardware accelerators for routine encryption and decryption operations. Since these basic operations are well-established, these hardware components do not require major functional redesigns when the protected applications evolve. The general-purpose CPU complex can easily implement any existing and new application protocols as well as security features with a simple software update. Furthermore, it delivers consistent and predictable performance across the entire feature set.

Another advantage of the general-purpose CPU architecture is its ease of portability. Security appliances that heavily rely on ASICs and FPGAs do not implement the security functions in software very efficiently because they do not expect to handle the majority of protected connections outside the hardware. Relying on physical network devices to secure traffic between virtualized applications is extremely inefficient, so it makes sense to port the security appliances for inter-application protection into the compute layer. If the appliance was never designed for efficient operation in the general-purpose CPU complex, packaging this solution in a virtual form factor becomes challenging in terms of feature support and consistent performance. Supported by the modular and highly portable Cisco ASA architecture, the new Cisco virtual ASA (ASAv) appliance delivers the complete Cisco ASA security feature set. It has all the capabilities to protect physical and virtual endpoints alike and it can effectively protect virtual endpoints without ever leaving the compute layer. Since rapid service provisioning is another emerging requirement in cloud-based data centers, new Cisco ASAv instances can be deployed on-demand using such intelligent application-centric solutions as Embrane.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Stateful Reliability and Scalability

Data centers must provide an unparalleled level of availability to its hosted applications. Instead of simply duplicating every network and computing hardware component and eliminating a single point of failure, modern data centers seek to derive the greatest value out of all the provisioned hardware. Although some older data center designs rely on Spanning Tree Protocol (STP) to block redundant Layer 2 paths, next-generation deployments require intelligent load-sharing mechanisms to avoid idling network links and devices.

EtherChannel interfaces enable the bundling of multiple physical Ethernet links in a single logical interface, where all of the member ports actively forward traffic. These member interfaces can be added or removed from the bundle on the fly and without any impact to transit application traffic. In order to quickly react to member port failures, some advanced EtherChannel-capable devices implement standardized Link Aggregation Control Protocol (LACP) for the dynamic bundling and debundling of interfaces. Those network devices that support only static EtherChannel bundling without LACP do not offer the same level of service assurance. If such a device exhibits a software failure without actually bringing the interface link down, transit application traffic through the statically bundled EtherChannel could be blackholed.

In addition to link level redundancy with EtherChannels, the Cisco Catalyst® 6500 Virtual Switching System (VSS) and Cisco Nexus® virtual port channel (vPC) technologies allow deploying redundant switch pairs in the dual-active mode. This way, both chassis actively process the traffic load as opposed to one of them remaining in standby. Since both switches in a VSS or vPC pair act as a single logical entity, EtherChannel bundles can span member ports on both physical chassis for complete redundancy and load sharing. Cisco ASA 5585-X appliances fully support LACP-based EtherChannels with up to 16 member interfaces per bundle in standalone and failover mode. These next-generation firewalls are also fully interoperable with Cisco Catalyst VSS and Cisco Nexus vPC deployments.

High availability is extremely important at the security-device level as well. Since most data center firewalls have to implement stateful inspection of all transit connections, it is not sufficient to simply deploy several such devices along the redundant paths. Although new application flows will switch to the new firewall instance in case of the original device's failure, existing connections will have to be reestablished because of the missing stateful information. Most stateful security devices can be configured in a redundant group where the connection state information is fully synchronized. If one device in the group fails, another unit can pick up the flow-forwarding function exactly where it was left off in terms of the application security context.

The unfortunate downside of this approach to high availability is that the maximum stateful connection counts and connection setup rates do not scale with the number of security appliances in the group. Since the same connection table is synchronized to all members of the redundant group, even multiple firewall appliances will not scale beyond the connection capacity of a single member. This is not acceptable in any modern data center where application connection volumes scale very rapidly, especially when servicing mobile users.

Another important limitation of many of these stateful security solutions is that load sharing is implemented through a single redundant group member, which then redirects the traffic to another firewall for processing. This effectively limits the throughput to that of a single member as well. Cisco ASA 5585-X and ASAv firewalls support both device-level active/standby and virtual context group-level active/active failover deployments for classic proven-and-true high availability. By using a single virtual active MAC and IP address pair on each data interface with stateful connection data replication, switchovers occur completely transparently to the adjacent network devices and - most important - the protected applications.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

In addition to failover, the Cisco ASA 5585-X offers firewall clustering, which is the true next-generation high-scalability solution. Instead of blindly replicating the entire connection table across all cluster members, Cisco ASA employs innovative techniques to maintain full stateful session redundancy with less data overlap between units. A firewall cluster can sustain the loss of a single member at a time with no impact to the application connections. At the same time, it can still scale the maximum stateful connections and connection rates in a pay-as-you-grow model.

Clustering supports stateless traffic load balancing with LACP-based cluster-spanned EtherChannels, dynamic routing protocols, or policy-based routing (PBR). Each cluster member independently creates and processes transit connections as well as compensates for any external traffic asymmetry. With up to 16 clustered firewalls, Cisco ASA can currently scale up to 640 Gbps of combined throughput with 100 million concurrent stateful connections and 2.8 million connection attempts per second. When paired with a Cisco Nexus vPC switch pair, Cisco ASA clustering supports up to 32 member ports per cluster-spanned EtherChannel.

A High Degree of Security in Any Topology

Traditional firewalls base all security policies on IP addresses and TCP or UDP transport ports. Although this approach has proven to be effective in relatively static data center application deployments over the years, more abstract and flexible endpoint and application identity schemes are desired. Some security devices solve this problem by being integrated into specific user-identity models, such as Microsoft Active Directory. This approach may work well for limiting access from internal users on dedicated endpoints, but it does not scale with externally accessible data center applications or the rapidly increasing mobile user base.

Cisco FirePOWER hardware modules for Cisco ASA5585-X appliances add the ability to use application identification in security policies and reports. Even though rules based on IP and transport ports still offer better security in a controlled data center environment, they can be combined with application-based rules for additional security and flexibility. For instance, one can create a policy rule that allows only Oracle SQL*Net database connections on TCP port 1521. This protects your data center from malicious parties that tunnel unauthorized services over well-known and typically allowed business application ports. Similarly, the Cisco ASA FirePOWER solution can automatically detect application mismatches on other well-known ports, such as TCP/22 for Secure Shell (SSH). These built-in application identification capabilities also allow a comprehensive visualization of the secure data center landscape through custom reports.

The Cisco TrustSec® solution offers a generic framework for application and endpoint identity establishment at the network perimeter and for a centralized enforcement of access policies on all participating devices. It abstracts the policies with security group tag (SGT) and SGT name constructs, so the firewall rules can be written in terms of human-readable elements. Access layer and other edge devices can also attach the appropriate tag to the transit frames for in-line policy enforcement and metadata propagation throughout the Cisco TrustSec enabled network. Cisco ASA 5585-X and ASAv appliances fully support security group access control list (SG-ACL) policies for a smooth Cisco TrustSec integration. Cisco ASA firewalls dynamically retrieve tag-to-name mappings from the Cisco Identity Services Engine (ISE) and learn assigned endpoint SGT values using SGT Exchange Protocol (SXP) adjacencies with edge devices. The Cisco ASA platform will also support security policy enforcement based on in-line frame tagging in the near future.

Many modern data centers are starting to rely on Layer 3 routed topologies in order to connect the infrastructure devices in a spine-and-leaf design. In addition to diverse routing protocol support, this approach requires high availability and quick convergence properties from all interconnected network devices.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Many security devices have very limited support for dynamic protocols, but even advanced devices run into difficulties with uninterrupted forwarding during switchovers within a redundant group. Even if the redundant firewalls establish independent routing adjacencies, the adjacent routers may blackhole traffic due to the dynamic protocol hold-down timers when a particular firewall is taken out of service. This outage may last only about a minute, but even a few seconds of downtime is unacceptable for the modern critical data center applications.

The Cisco ASA 5585-X supports a variety of dynamic routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) v2 and v3, and Border Gateway Protocol (BGP) v4 in order to integrate into such a data center. When using failover and clustering, Routing Information Base (RIB) data structures are replicated from the unit that maintains the dynamic routing protocol adjacencies to all the other Cisco ASA devices, thus enabling uninterrupted stateful traffic forwarding in case of a single member failure. Standardized Nonstop Forwarding (NSF) support for dynamic routing protocols will be available on the Cisco ASA platform in the near future. A highly available Cisco ASA failover pair or a cluster can then interact with the directly adjacent routers during switchover events and maintain uninterrupted traffic forwarding on both sides. Another upcoming Cisco ASA enhancement will enable equal-cost multi-path (ECMP) load balancing across multiple logical firewall interfaces while maintaining stateful session tracking of such asymmetric flows. This capability will solidify the Cisco ASA 5585-X's position as the security device of choice in fully meshed Layer 3 data center topologies.

In some new data center implementations, the underlying network infrastructure relies on stateful device service farms to deliver desired security services exactly where application segmentation needs to happen. Although it has been effective over the years, the current approach of implementing application segmentation with VLANs and routed hops will be replaced with security service insertion in SDN environments. A perfect example of such a next-generation technology is the Cisco Application Centric Infrastructure (ACI). Instead of designing the applications around the data center network and its limitations, Cisco ACI helps the administrator instantiate the desired network topology on demand along with the applications.

Traditional security devices suffer from access-rule-proliferation issues when old policies are not removed even after the associated applications are decommissioned. As a result, the firewall rule table continues to grow, thus complicating policy management and negatively affecting the application performance.

Cisco ASA 5585-X and ASAv both natively integrate into Cisco ACI with the traditional insertion mode, where firewalls are instantiated along with the applications directly from the Cisco Application Policy Infrastructure Controller (APIC). Cisco APIC automatically programs all of the necessary Cisco ASA policies to support the protected application and stitches the firewall services directly into the path of the inter-application traffic flows. When the applications are decommissioned, Cisco APIC unconfigures all the associated firewall policies on the Cisco ASA as well. This approach eliminates the dangers of access rule proliferation and keeps the Cisco ASA rule set current with the protected applications. Because Cisco ACI is a stateless network fabric, it requires the associated security devices to provide stateful scaling capabilities for the applications. This is yet another deployment scenario where stateful connection and connection-rate scalability are extremely important. ACI is fully compatible with Cisco ASA clustering, so you can use this firewall feature to build highly scalable and powerful SDN security service farms within your fabric-based next-generation data center.

Conclusion

Modern data centers are undergoing many transformations, but security continues to be as important as ever. As applications become more demanding, their associated security devices must keep up with them. To meet low-latency and high-performance requirements, next-generation data center firewalls have become more intelligent in applying their security policies and allocating resources.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Hardware-based security appliances alone are no longer adequate for protecting rapidly changing applications against more and more elaborate network attacks. The ongoing move toward data center virtualization requires that security devices deliver the same high performance and robust features in both physical and virtual form factors. High scalability has become as important as high availability both at network device and link levels. Modern data center applications require firewalls to scale the throughput as well as the stateful connection entries and connection setup rates. Fully distributed connection handling and transparent switchovers allow properly designed firewall clusters to elastically scale with data center application demands. Future data center designs will also require the security devices to be versatile in terms of access policy abstractions, dynamic routing capabilities, and SDN fabric-insertion capabilities.

Why Cisco

Protecting both physical and virtual environments, Cisco ASA 5585-X and ASAv meet all of the next-generation data center requirements by implementing an effective defense-in-depth approach within the highly extendable general-purpose CPU architecture. Cisco ASAv failover and Cisco ASA 5585-X clustering features help enable both high availability and scalability in the pay-as-you grow model and achieve up to 640 Gbps of throughput with 16 appliances in a single cluster. LACP-based EtherChannel insertion into VSS and vPC switch environments helps the Cisco ASA protect critical data center applications with low reaction times on failure. FirePOWER AVC and NGIPS services on the optional Cisco ASA5585-X module enable application-based policies and advanced threat mitigation capabilities for ultimate data center protection. Cisco ASA SG-ACL support with Cisco TrustSec technology also delivers the new level of abstraction for more flexible security policies. Robust dynamic routing functionality with RIB synchronization and future NSF and ECMP support make Cisco ASA 5585-X and ASAv perfect firewalls for Layer 3 data center topologies. Last but not least, effective interoperability with Cisco ACI helps enable all Cisco ASA platforms to integrate into next-generation SDN fabric topologies.

Next Steps

Please visit these webpages for more information about the Cisco ASA Firewalls:

- http://www.cisco.com/c/en/us/products/security/asa-5585-x-adaptive-security-appliance/index.html.
- http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/design_guide_c22-624431.html.
- http://www.cisco.com/c/en/us/products/security/asa-firepower-services/literature.html.

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 C22-731801-01 10/14

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.