Cisco ASA 5585-X in the Data Center

Cisco® ASA 5500 Series Adaptive Security Appliances combine advanced stateful firewall and VPN concentrator capabilities in one device. The appliances include many advanced features, such as multiple security contexts (similar to virtualized firewalls), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, intrusion prevention, IPsec and WebVPN support, and more.

Data Center

In this section we will discuss the business needs associated with deploying firewalls in the Data Center, what the requirements for the proposed solution. An overview of the various ASA technologies that are incorporated in the solution is also discussed.

Business Need: Deploying Firewalls in the Data Center

The data center is more important to the enterprise than ever before. An increase in the concentration of data services in data centers has led to a corresponding increase in the need for high performance and scalable network security. To address this need, Cisco introduced the ASA 5580, an appliance meeting the 5 Gbps and 10 Gbps needs of campuses and data centers. Cisco has now broadened the ASA portfolio further: The next-generation ASA 5585-X appliance is expanding the performance envelope of the ASA 5500 Series to offer 2 Gbps to 20 Gbps of real-world HTTP traffic and 35 Gbps of large packet traffic. The Cisco ASA 5585-X supports up to 350,000 connections per second and a total of up to two million simultaneous connections initially, and is slated to support up to eight million simultaneous connections in a later release.

The advent of Web 2.0 applications has brought about a dramatic increase in new device types and the extensive use of complex content, which is straining existing security infrastructures. Today's security systems are often unable to meet the high transaction rates or depth of security policies necessary in these environments. As a result, information technology staffs often struggle to provide basic security services and to keep up with the magnitude of security events generated by these systems for necessary monitoring, auditing, and compliance purposes.

Cisco ASA 5585-X appliances are designed to protect the media-rich, highly transactional, and latency-sensitive applications at the enterprise data center. Providing market-leading throughput, the highest connection rates in the industry, large policy configurations, and very low latency, the ASA 5585-X is highly suitable for the security needs of organizations with the most demanding applications, such as voice, video, data backup, scientific or grid computing, and financial trading systems.

Solution Requirements

The Cisco ASA 5585-X appliance provides a flexible, cost-effective, and performance-based solution that allows users and administrators to establish security domains with different policies within the organization. Users need to be able to set appropriate policies for different VLANs. Data centers require stateful firewall security solutions to filter malicious traffic and protect data in the demilitarized zones (DMZ) and extranet server farms while delivering multi gigabit performance at the lowest possible cost.

The Cisco ASA 5585-X appliance can be deployed in an Active/Active or Active/Standby topology and can make use of additional features such as interface redundancy for added resilience. Separate links are used also for the fault tolerance and state links.

The Cisco ASA 5585-X appliance delivers multi gigabit security services for large enterprise, data center, and service provider networks. The appliance accommodates high-density copper and optical interfaces with scalability from Fast Ethernet to 10 Gigabit Ethernet, enabling unparalleled security and deployment flexibility. This high-density design enables security virtualization while retaining the physical segmentation desired in managed security and infrastructure consolidation applications.

Scope

This document provides information about design considerations and implementation guidelines when deploying firewall services in the data center using the Cisco ASA 5585-X appliance.

Cisco ASA Technical Concepts

Security Policy

Firewalls protect internal networks from unauthorized access by users on an external network. The firewall can also protect internal networks from each other - for example, by keeping a human resources network separate from a user network. Cisco ASA appliances include many advanced features, such as multiple security contexts, transparent (Layer 2) firewall or routed (Layer 3) firewall operation, hundreds of interfaces, and more. When discussing networks connected to a firewall, the external network is in front of the firewall, and the internal network is protected and behind the firewall. A security policy determines the kind of traffic that is allowed to pass through the firewall to access another network, and will generally not allow any traffic to pass the firewall unless the security explicitly allows it to happen.

Cisco Intrusion Prevention Services

The Cisco Advanced Inspection and Prevention Security Services Processor (AIP SSP) combines inline intrusion prevention services with innovative technologies to improve accuracy. When deployed within Cisco ASA 5585-X appliances, the SSPs offer comprehensive protection of your IPv6 and IPv4 networks by collaborating with other network security resources, providing a proactive approach to protecting your network.

The Cisco AIP SSP helps you stop threats with greater confidence through the use of:

- **Wide-ranging IPS capabilities:** The Cisco AIP SSP delivers all the IPS capabilities available on Cisco IPS 4200 Series Sensors, and can be deployed inline in the traffic path or in promiscuous mode.
- **Global correlation:** The Cisco AIP SSP provides real-time updates on the global threat environment beyond your perimeter by adding reputation analysis, reducing the window of threat exposure, and providing continuous feedback.
- **Comprehensive and timely attack protection:** The Cisco AIP SSP delivers protection against tens of thousands of known exploits and millions more potential unknown exploit variants using specialized IPS detection engines and thousands of signatures.
- **Zero-day attack protection:** Cisco anomaly detection learns the normal behavior on your network and alerts you when it sees anomalous activities in your network, helping to protect against new threats even before signatures are available.

When IPS is deployed to traffic flows within the ASA appliance, those flows will automatically inherit all redundancy capabilities of the appliance.

High Availability

Cisco ASA security appliances provide one of the most resilient and comprehensive high-availability solutions in the industry. With features such as sub-second failover and interface redundancy, customers can implement very advanced high-availability deployments, including full-mesh Active/Standby and Active/Active failover configurations.

This provides customers with continued protection from network-based attacks and secures connectivity to meet today's business requirements.

With Active/Active failover, both units can pass network traffic. This also lets you configure traffic sharing on your network. Active/Active failover is available only on units running in "multiple" context mode. With Active/Standby failover, a single unit passes traffic while the other unit waits in a standby state. Active/Standby failover is available on units running in either "single" or "multiple" context mode. Both failover configurations support stateful or stateless failover.

The unit can fail if one of these events occurs:

- The unit has a hardware failure or a power failure.
- The unit has a software failure.
- Too many monitored interfaces fail.
- The administrator has triggered a manual failure by using the CLI command "no failure active"

Even with stateful failover enabled, device-to-device failover may cause some service interruptions. Some examples are:

- Incomplete TCP 3-way handshakes must be reinitiated.
- In Cisco ASA Software Release 8.3 and earlier, Open Shortest Path First (OSPF) routes are not replicated from the active to standby unit. Upon failover, OSPF adjacencies have to be reestablished and routes re-learnt.
- Most inspection engines' states are not synchronized to the failover peer unit. Failover to the peer device loses the inspection engines' states.

Active/Standby Failover

Active/Standby failover lets you use a standby security appliance to take over the functions of a failed unit. When the active unit fails, it changes to the standby state while the standby unit changes to the active state. The unit that becomes active assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no Address Resolution Protocol (ARP) entries change or time out anywhere on the network.

In Active/Standby failover, failover occurs on a physical unit basis and not on a context basis in multiple context mode. Active/Standby failover is the most commonly deployed method of high availability on the ASA platform.

Active/Active Failover

Active/Active failover is available to security appliances in "multiple" context mode. Both security appliances can pass network traffic at the same time, and can be deployed in a way that they can handle asymmetric data flows. You divide the security contexts on the security appliance into failover groups. A failover group is simply a logical group of one or more security contexts. A maximum of two failover groups on the security appliance can be created.

The failover group forms the base unit for failover in Active/Active failover. Interface failure monitoring, failover, and active/standby status are all attributes of a failover group rather than the physical unit. When an active failover group fails, it changes to the standby state while the standby failover group becomes active. The interfaces in the failover group that becomes active assume the MAC and IP addresses of the interfaces in the failover group that failed. The interfaces in the failover group that is now in the standby state take over the standby MAC and IP addresses. This is similar to the behavior that is seen in physical Active/Standby failover.

Redundant Interface

Interface-level redundancy revolves around the concept that a logical interface (called a redundant interface) can be configured on top of two physical interfaces on an ASA appliance. This feature was introduced in Cisco ASA Software Release 8.0.

One member interface will be acting as the active interface responsible for passing traffic. The other interface remains in standby state. When the active interface fails, all traffic is failed over to the standby interface. The key benefit of this feature is that failover would then occur within the same physical device, which prevents device-level failover from occurring unnecessarily. These redundant interfaces are treated like physical interfaces once configured.

Link failure on the active device would cause a device-level failover, while a redundant interface will not. In a data center environment, the following are benefits of using redundant interfaces to create a full-meshed topology:

- Incomplete TCP 3-way handshakes do not have to be reinitiated when interface-level failover occurs.
- If and when dynamic routing protocol is used on an ASA appliance, routing adjacencies do not have to be re-established/re-learnt.
- Most inspection engine states will not be lost at the interface-level failover, but at device- level failover.

There is less impact to end users because ASA stateful failover does not replicate all of a session's data. For example, some voice protocols' (e.g., Media Gateway Control Protocol [MGCP]) control sessions are not replicated and a failover could disrupt those sessions.

With interface redundancy feature, a (redundant) interface would be considered in failure state only when both underlying physical interfaces are failed.

The key benefits of interface-level redundancy are:

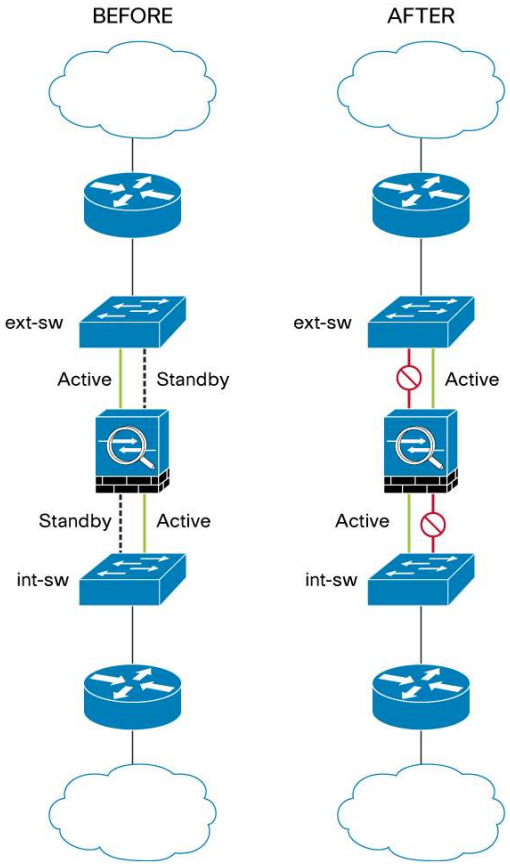
- Reducing the probability for device-level failover in a failover environment, thus increasing network/firewall availability and eliminating unnecessary service/network disruptions.
- Achieving a full-meshed firewall architecture to increase throughput and availability.

Figure 1 depicts a simple deployment scenario for an ASA appliance with interface redundancy enabled and no device-level (A/S or A/A) failover.

In this scenario, when the ASA interface failure occurs, the security appliance will continue to pass traffic since the standby physical interface of the redundant interface will take over as an active interface.

This design is supported on single context mode, multiple context mode, routed firewall mode, and transparent firewall mode.

Figure 1. This depicts a before after picture of the use of redundant interfaces, where physical interface failures have been introduced, without introducing any redundant interface failures.



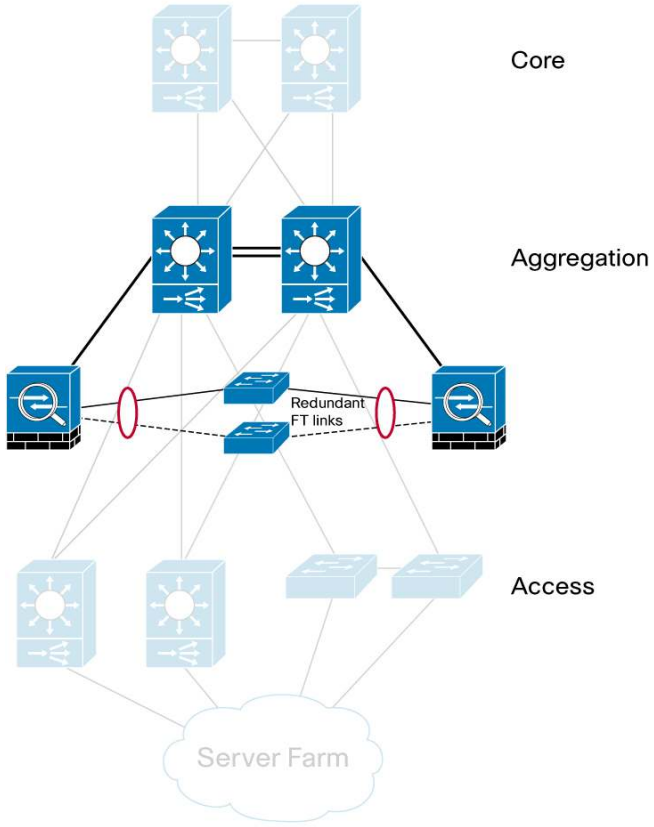
Cisco ASA 5585-X appliances fit into a standard data center design, as shown in Figure 2. VLANs are extended from the physical switches to the external ASA appliances and use dedicated redundant failover and state links connected to separate switches. The technologies described in earlier sections will be combined to create a highly redundant network design. We will be using these three key features on the ASA appliance:

- Redundant interfaces
- Active/Active failover
- Transparent mode

You can partition a single ASA appliance into multiple virtual devices, known as security contexts. In “multiple” context mode, the ASA appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system configuration identifies basic settings for the ASA, but does not include any network interfaces or network settings for itself. The “admin” context is like any other context in all ways but one: When a user logs in to the “admin” context, that user has system administrator rights and can access the “system” and all other contexts.

Architecture Overview

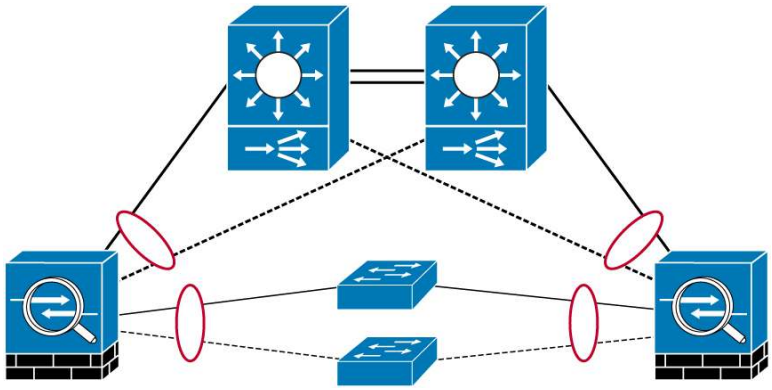
Figure 2. Standard Data Center Architecture



IPS services can be integrated into each of the ASA appliances within the design, or a separate standalone IPS/IDS can be applied. The advantage of implementing the IPS services within the ASA appliance is that you can use fine-grained control to classify traffic to be inspected by the IPS services.

The ASA 5585-X is integrated into the architecture at the aggregation layer by connecting trunk ports carrying the VLANs that are to be firewalled. Redundant links can also be configured to the aggregation layer to provide an extra level of availability, if required (Figure 3). Link failure on the active device would cause a device-level failover, while a redundant interface will not.

Figure 3. Redundant Link Connectivity



Transparent or Routed Firewall Mode

The Cisco ASA 5585-X supports two different firewall modes: routed and transparent. In routed firewall mode, the ASA appliance is considered a router hop in the network. In transparent firewall mode, the appliance acts like a "stealth firewall" and is not considered a router hop. The ASA appliance connects to the same network on its internal and external interfaces. Transparent mode is useful if you want the firewall to be invisible to attackers. The data center design uses the transparent mode to support the Active/Active architecture on the ASA appliance.

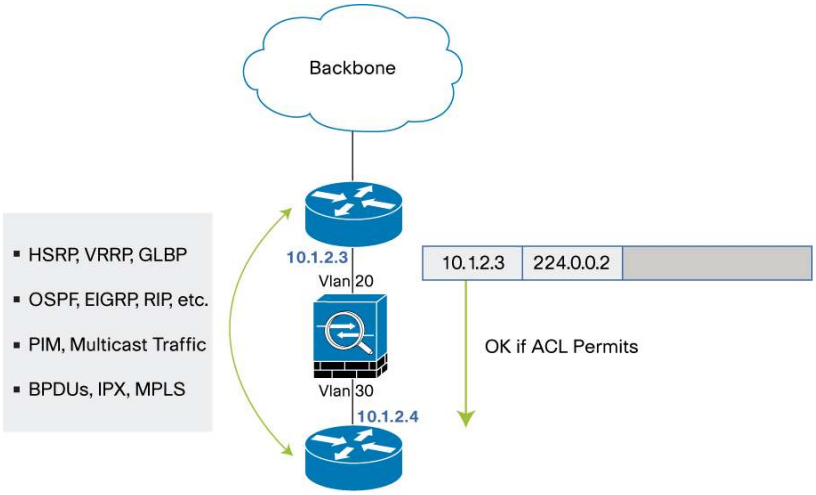
Table 1 shows the features of both types of deployment.

Table 1. Comparing Routed and Transparent Firewall Modes

Routed	Transparent
All "flavors" of NAT available	Two interfaces per context
Data traffic is routed	NAT support for transparent mode
Does not pass Multicast traffic	Data traffic is bridged
Interfaces can be shared between contexts	Passes Multicast traffic
	No shared interfaces

In transparent mode, the Cisco ASA 5585-X appliance is not a router hop. The ASA appliance connects the same network on its internal and external ports, but each port must be on a different VLAN. No dynamic routing protocols or NAT are required on the ASA appliance. Other advantages of transparent mode in the data center are shown in Figure 4.

Figure 4. Transparent Firewall Mode in the Data Center



- Routers can establish routing protocols adjacencies through the firewall.
- Protocols such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP) can cross the firewall. Multicast streams can also traverse the firewall.
- Non-IP traffic can be allowed (pre-configured types are IPX, MPLS, BPDUs), but it must be using Ethernet V2/DIX encapsulation - no inspection, just bridging.

Performance and Scalability

Up until now, the main deciding factor for performance of a firewall has been throughput in terms of Mbps. However, applications have become much more demanding; they are now either keeping connections open for longer durations (persistent connections as used in file sharing or multimedia) or they open many short-lived connections (as typically used in common websites such as Facebook).

While throughout is still important, it is becoming equally important to handle newer applications that are stretching the capabilities on concurrent connections and to provide the ability to open new connections quickly. The Cisco ASA 5585-X expands these capabilities, but special attention has been paid to deliver superior performance in connection rate per second and in total simultaneous connections. The Cisco ASA 5585-X has addressed the performance requirements by utilizing a high-speed switched backplane with very low latency and a parallel CPU architecture.

Summary

In this document we have discussed how the Cisco ASA 5585-X appliance can be used in a data center design, taking into account the needs for the common data center. The ASA 5585-X has been deployed in the data center in a fashion that has the least disrupting impact on the design, by using a highly redundant network design and high-availability features within the ASA 5585-X.

For More Information

For more information about Cisco ASA 5500 Series appliances, visit http://www.cisco.com/go/asa or contact your local account representative.

For more information about the Cisco End-of-Life Policy, go to: http://www.cisco.com/en/US/products/prod_end_of_life.html.

To subscribe to receive end-of-life/end-of-sale information, go to: http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.

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 C22-624431-00 10/10