Fast Lane

Consulting and Education Services Inc.

Design & Implementation of a Secure Cisco Nexus Powered Data Center Network

Summary

Today, a network infrastructure must adhere to robust and demanding requirements. Applications and “big data” are driving network requirements more so now than ever before, and additional requirements such as security or compliance must be a design consideration. Ubiquitous network access has set a precedent that networks must be robust, scalable, and secure. Furthermore, networks, in particular mission critical networks, must be transparent to the end-user and maintainable for the enterprise network engineer.

June 2015

Background

Historically, networks were purpose built for one or more specific applications. Organizations housed their network infrastructure in a “computer room” or fashioned a “server room” from a spare room or closet. From a physical/environmental perspective, these spaces did not lend themselves to be highly available due to limitations on power, cooling, and access.

More specifically, network infrastructure consisted of more or less autonomous networks separated by low-speed (by today’s standards) telecommunications circuits. Homogenous networks were virtually non-existent. Hardware was disparate by location, and demands on the network were, for the most part, minimal.

Several drivers caused network design practices to evolve. New protocols and standards comprise the bulk of network design evolution. Telecommunications carriers have moved Ethernet from local to metro, and even to the Wide Area Network (WAN) space. Organizations have consolidated physical locations, and in doing so, centralized their information technology applications. Financial incentives drive organizations to outsource their “computer rooms” to purpose-built data centers. Compliance requirements drive some to those same data centers.

Today, networks must be homogenous. An organization must be able to deploy applications over one infrastructure, and in essence “re-use” that infrastructure. Enterprise data center networks must be built to provide quick turnaround times during application deployment, and comply with rigorous business requirements. In addition, the network must be transparent to the end-user. The network must always be “on.”

Building the Data Center

Planning

1

When building a data center network, careful planning and consideration to application requirements is imperative. Several solutions are available from vendors like Cisco and Juniper. However, the solution must fit within the existing (if there is one) environment, and any and all application requirements. Application owners must understand the capabilities and limits of the network, while network design engineers must understand application requirements like traffic patterns, connectivity flows, and availability. Is the application “chatty?” Does it involve bulk file transfers? Is the application sensitive to network degradation? Is it transaction based? Does it require responses within a specified amount of time?

The oft asked question from a network design standpoint is: what is the application’s bandwidth requirements? How much capacity must be built to support the application? Traffic types and patterns may dictate network segmentation, firewall placement, link speeds, and availability.

In a virtualized environment, the question that needs to be asked is what type of compute platform is being considered? What uplink speeds are being considered for blade servers? The 802.3ba standard for 40 gigabits-per-second (Gbps) data center is approaching--even before 10 Gbps has become ubiquitous.

From an availability perspective, inquiries must be made regarding uptime requirements. Will physical servers be dual-homed to the network? Do the uptime requirements necessitate redundant core switches? If perimeter security is a requirement, do perimeter firewalls need to be highly available? Database servers, for example, are highly redundant and the underlying network must support such functionality.

Not every environment has security compliance requirements; however, every network design must be secure. Does the environment require specific security zones? How are these zones delineated? Can isolation be attained via firewall, or via logical segmentation using virtual LANs (VLANs)? What design elements must be built in your network to comply with security controls like NIST 800-531 or PCI-DSS2?

2 Design

Once the planning session has been finalized and all the necessary questions have been answered, the network design phase begins. For the purposes of this paper, the design will focus on the Cisco Nexus data center solution. The Cisco Nexus platform is included in the Cisco Validated Design Program. The Cisco Validated Design Program "provide[s] the foundation for systems design based on common use cases or current engineering system priorities."[3] The program provides guidance for data center network deployment based on Cisco tested and validated designs. Details about the program are beyond the scope of this paper.

The requirements and/or constraints for the design are as follows:

- Internet accessible portal provides access to application
- One application contains sensitive data including personally identifiable information (PII).
- A different application contains sensitive data including social security numbers (SSN).
- Customer service representatives (CSR) access the application environment between the hours of 8a.m. and 4p.m., excluding weekends.
- CSRs access the application through a WAN rather than through the Internet portal.
- There are several database clusters included in every application.
- There are several web servers providing the Internet portal portion of the applications.

Two applications, both of which, contain sensitive information suggest that segmentation or isolation is required, data in transit must also be protected. The model network design in this paper will comprise the following network hardware:

- Nexus 5548P (2)
- Cisco 2248 Fabric Extenders (FEX) (4)
- HP C7000 Blade System (2)
- Cisco ASA 5585 (2)
- Cisco 3945 ISR (2)

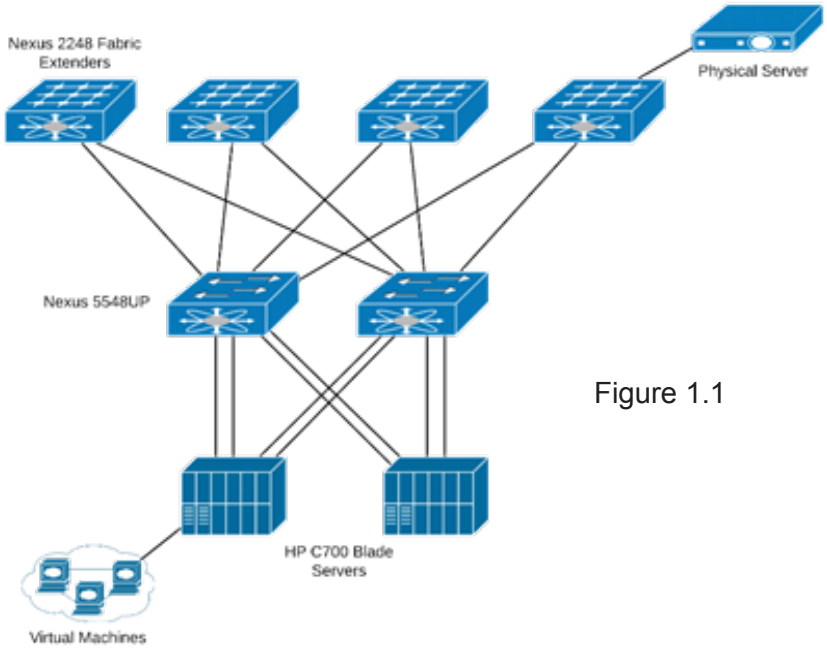


Figure 1.1

The Nexus 5548P pair will serve as the core switching platform for the environment, and Layer-3 (IP) core routing platform. Layer-3 capabilities require the Layer-3 daughter card (part number: N55-D160L3 or N55-D160L3-V2). The physical layout of the core network is illustrated above in Figure 1.1. This depicts the Nexus core, fabric extenders, blade server system, virtual machines (VMs), and a physical server.

This core network design accomplishes two things: building the network to scale with existing physical servers, network appliances, or other hosts while the blade servers accommodate virtual machines. The Nexus 5548UP supports 10 gigabit speeds and 1 gigabit speeds via SFP and SFP+ transceivers. This provides scalability and flexibility for growth and integrating existing networks.

This network model allows for scalability and backwards compatibility; however, there are Nexus platform specific details that must be considered. Fabric extender counts on the Nexus 5500 platform may be capped depending on the version of NX-OS running on the device. This is especially crucial when creating virtual port channels (VPCs) between the FEX units and the 5548; and between the FEX units and a server. Virtual Port Channels bond physical gigabit or ten gigabit Ethernet links in a virtual fashion. Bundled links appear as a single logical link to physical servers, FEX units, and blade servers. Figure 1.2 illustrates the physical and logical layout of VPCs.

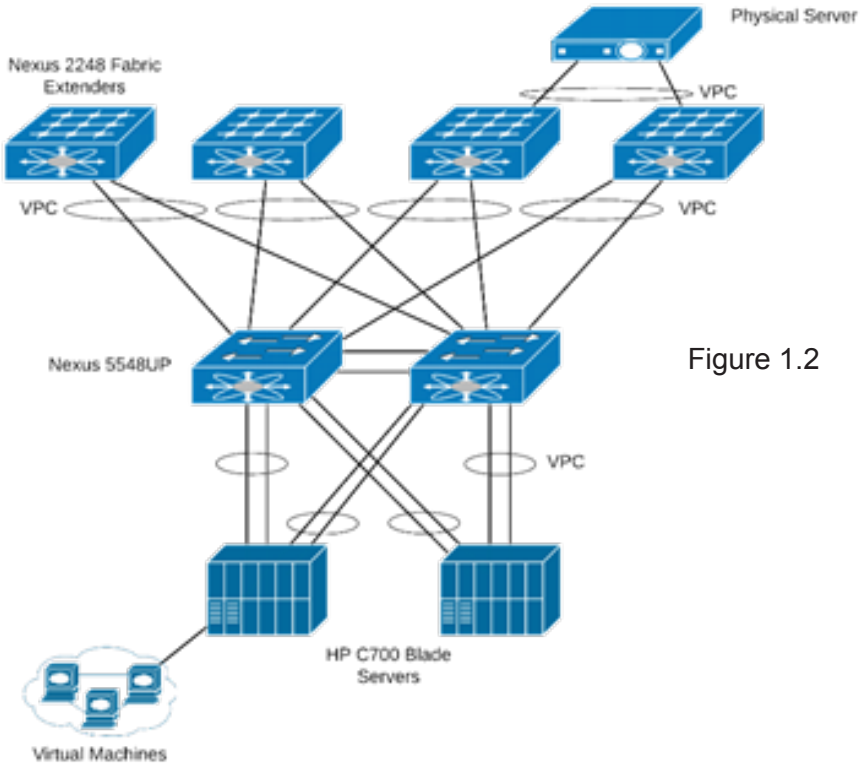


Figure 1.2

Virtual Port Channels provide redundancy during link failure, increased aggregate bandwidth, and a simplified Layer 2 topology. Virtual Port Channels provide redundancy and active/active links for physical servers that support Link Aggregation Control Protocol (LACP). The network model provides high availability, bandwidth efficiency, and scalability using VPC. It is important to determine whether the FEX units shall be single-homed or dual-homed to a Nexus 5548. Hosts should be dual homed to two different FEX units to take advantage of high availability and redundancy using VPCs.

Security requirements dictate that the network must be designed to protect information in transit, and at rest. These requirements may be satisfied by Layer 2 segmentation using VLANs, or Layer 3 using firewalls, access lists and routing. Figure 1.3 depicts Layer 2 segmentation.

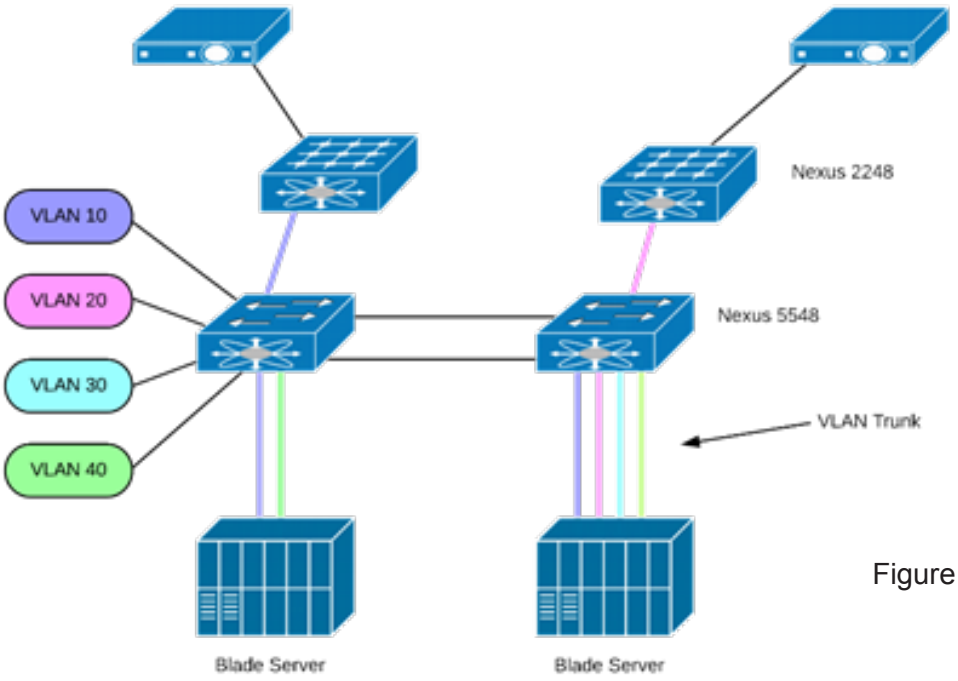


Figure 1.3

Access can be restricted by permitting specific VLANs on trunk links to the blade servers. In Figure 1.3, VLANs 10 and 40 are permitted on the trunk links connected to the leftmost blade server; while all VLANS (10, 20, 30 and 40) are permitted on the trunk links connected to the rightmost blade server. An identical access control method can be implemented on the FEX units. Virtual LANs may be restricted (pruned) or permitted on VPC trunks connected to the FEX units.

Layer 3 access control can be accomplished using Virtual Routing and Forwarding (VRF) instances. Virtual Routing and Forwarding is mainly used for MPLS VPNs and multi-tenant routing environments. VRFs allow multiple routing tables in a physical router. While VRFs are not a security tool per se, they can be used to isolate and segment a network. Figure 1.4 shows a simple VRF network model.

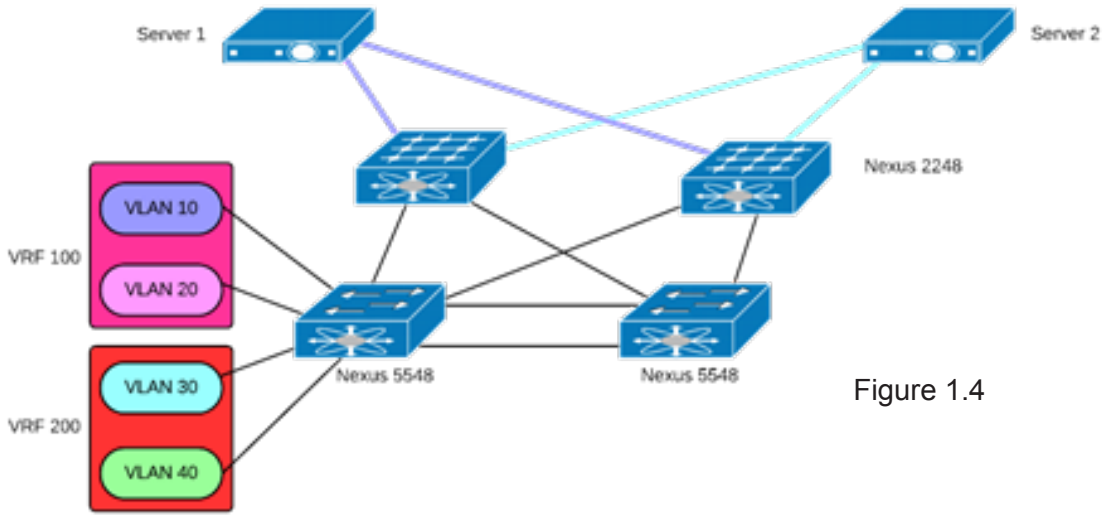


Figure 1.4

Server 1 is assigned to VLAN 10, and thus isolated from Server 2; however, if both VLANs were not assigned to a VRF instance, each server can communicate with each other; because a VLAN is considered a connected route within the Nexus. Server 1 would send a packet towards their default gateway (VLAN Interface on Nexus 5548) and the Nexus 5548 would route the packet to Server 2. In Figure 1.4, Server 1 would send a packet to its default gateway (in VRF 100); however, the packet would not arrive at Server 2 because Server 2 is in VRF 200. All routing is confined to a specific VRF. When initially provisioned, layer 3 interfaces are assigned to a specific VRF. This would be considered an extreme form of segmentation or isolation. If we apply the above VRF model to our security requirements, servers containing social security number (SSN) information would be in VRF 100, and servers containing personally identifiable information (PII) would be in VRF 200. The two servers would not be able to communicate with each other.

The three tier architecture would be considered another “extreme” form of network segmentation and isolation. This type of segmentation is done at layer 3 using VLANs and firewalls. VRFs may also be used to further isolate, but this can further complicate the deployment. Figure 1.5 illustrates the three tier model.

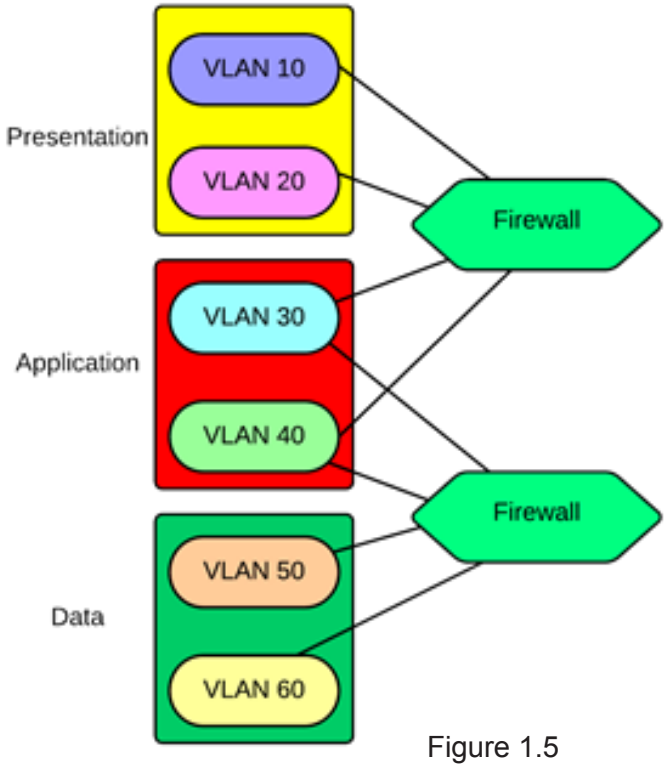


Figure 1.5

The three tier architecture is a generic conceptual model, and not necessarily a vendor specific implementation. The model fits well within the aforementioned security requirements. The presentation tier comprises the “front end” of the environment. Typically, web servers, application delivery controllers, or proxies reside in this tier. Application programming interface (API) servers, middleware, and application servers reside in the application tier. The data tier houses LDAP, SQL, or other database servers. Security features of the three tier architecture include total isolation and segmentation of an application’s critical components. Firewalls must not be bypassed when communicating between tiers. Additionally, the outside world (Internet) should only communicate with the presentation tier. The application and data tiers should not be able to communicate with the outside world, and vice versa.

This architecture fits the network model presented in this paper. In fact, Cisco has developed their Application Centric Infrastructure (ACI) to support data center networks similar to the three tier architecture. ACI suggests the use of a virtual security gateway (VSG) for segmentation and isolation. The VSG corresponds to the fire-wall within the generic three tier architecture. The Cisco ACI is, however, beyond the scope of this paper.

The network model thus far discussed in this paper focused on the core switching and core layer 3 design. The aforementioned requirements dictate that the web portal of the application is accessible through the public internet. The edge network design must be considered as well.

Figure 1.6

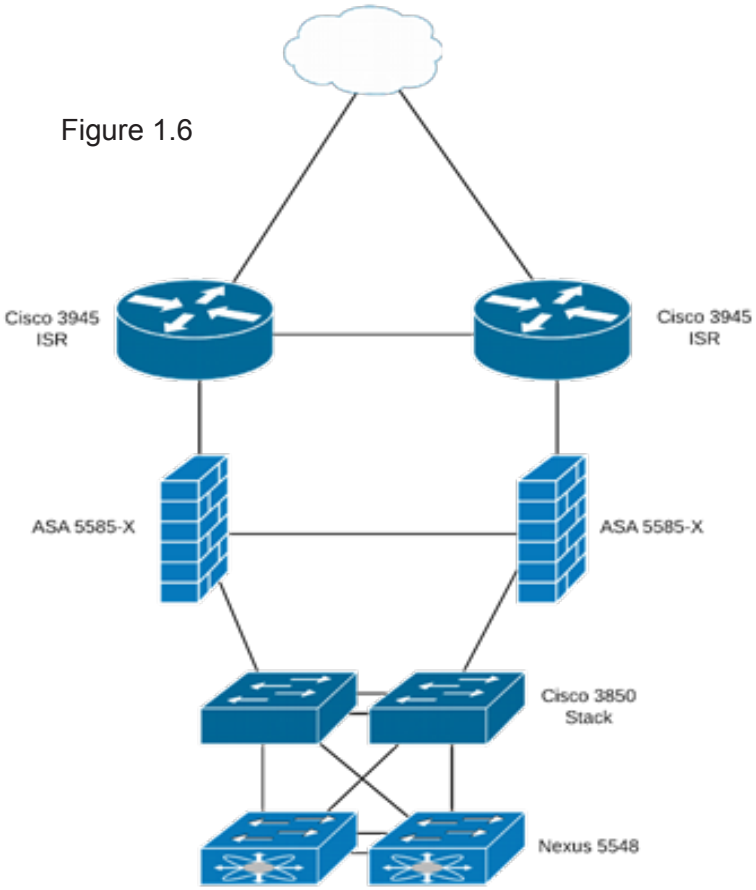
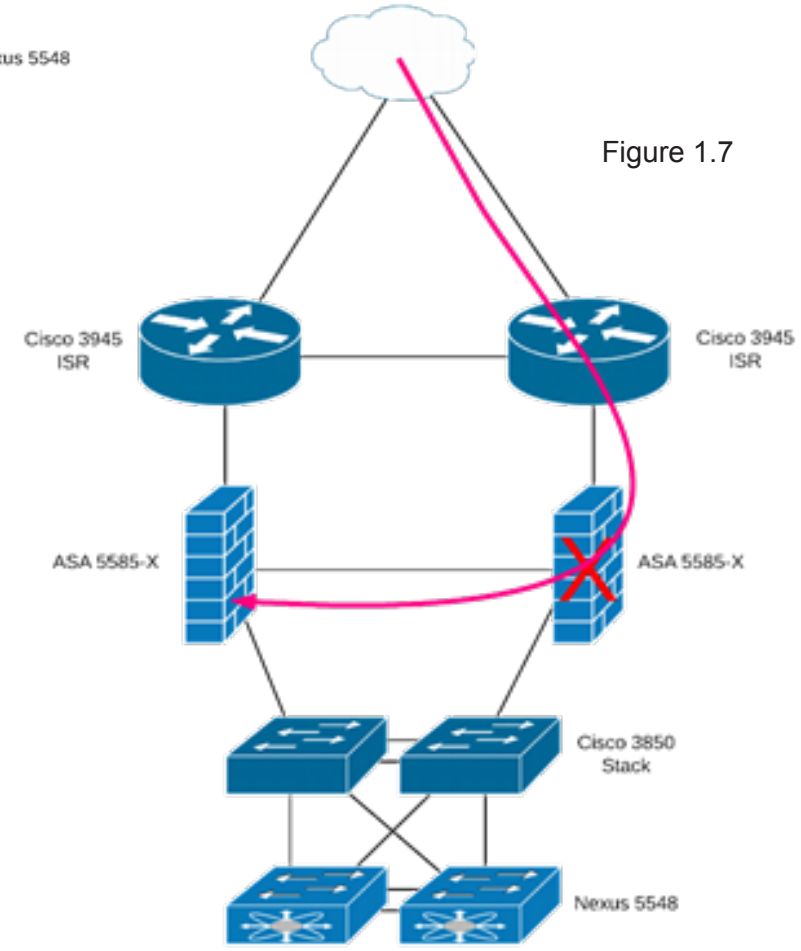


Figure 1.6 depicts the edge network and ingress to the core switch infrastructure. This edge network design model accommodates additional edge appliances such as an IDS/IPS, WAN optimization, or other edge device. The Cisco 3850 stack acts as the insertion point for additional edge devices/appliances. Each edge network element is deployed in a highly available fashion. This fulfills the application requirement that the web portal be available 24x7x365. The Adaptive Security Appliance (ASA) can be integrated into the core switching infrastructure by connecting directly to the Nexus 5548; however, this negates the ability to create an insertion point for additional appliances. By connecting the ASA cluster to the Cisco 3850 stack, this allows for an additional layer of protection between the core and the edge.

Figure 1.7



To fulfill availability requirements, the Cisco 3945 pair must be configured for Hot Standby Router Protocol (HSRP). It is recommended that HSRP timers be tuned for optimal failover. Any failover events must be transparent to the end user and the application. Proceeding down from the routers, the ASA must be configured for failover and a connection state link. Any connections going through the ASA are mirrored to the failover ASA via the connection state link. Any connections "in-flight" will not be disrupted by a failover event. Figure 1.7 illustrates a failover event.

The Cisco 3850 in stack configuration is fully redundant. Shared power between the switches provides redundant power, and layer 2 redundancy is achieved using stack cables between switches. The Nexus connects to the Cisco 3850 stack by way of a “criss-cross applesauce” configuration. The links are configured as 802.1q trunks, port channels and VPCs on the Nexus. In the event of a link failure, connectivity will not be disrupted.

Referring back to Figure 1.6, it is crucial that the pertinent VLANs are assigned to the 802.1q trunks between the Cisco 3850 stack and the Nexus 5548 pair. Only configuring the necessary VLANs establishes a “least access” security control. Least access security controls must also be considered when developing firewall rules. Two security models may be considered when creating firewall rules: the negative security model, and the positive security model. The negative security model defines access to reject or filter; while allowing all other traffic. The positive security model defines access that is allowed, while denying all other traffic. Regardless of the approach taken, access should always be limited to only that which is necessary. Again, least access security must be considered.

Conclusion

The model network presented here fulfills the application requirements; however, like most real-world implementation, requirements change, and configurations must be altered to fit those changes. The models, concepts, and recommendations presented should be considered as such--guidelines. It is an overview of a specific network design model to which a hypothetical set of requirements have been applied. The Nexus 5548 network model represents a real-world implementation. It should by no means be interpreted as the standard network model, only one of many design considerations. Again, the design must fit the requirements.

Before choosing a vendor or looking at solutions, one should obtain as much information as possible. The design engineer must familiarize his or herself with application behavior, and ask as many questions of the application owners as possible. Good design starts with good and useful information.

An adequate timeline must be established in order to design, deploy, test and validate a network design. Tight timelines and unreasonable milestones can overrun a budget. Additional third party resources usually compensate for tight timelines. For some organizations, this is business-as-usual; however, tight budgets don’t always allow for consultants and professional services. Good design relies upon excellent planning, reasonable timelines and milestones.

The network model presented is based on the Cisco Nexus platform; however, good design relies upon the best solution to fit the requirements. A design using the Cisco 4500-X can accomplish the same objectives and fit application requirements. A conceptual design, followed by a careful hardware selection will bring about the best results.

Project plans should include a test and validation plan. Several issues are worked out and resolved during a test and validation phase. Vendor cooperation during this phase will greatly reduce the potential for software bugs. Similarly, vendor implementation advice can greatly improve a design. Test and validation can demonstrate shortcomings in failover events, or application performance. During this phase, a design engineer should make adjustments in order to achieve optimum network performance. Failure to include a test and validation plan, again, can overrun a budget due to loss of time and unexpected costs.

Related Courses

If you are looking to expand your knowledge on this topic, Fast Lane offers the following courses:

Configuring Cisco Nexus 5000 Switches (DCNX5K)
Implementing Cisco Data Center Unified Computing (DCUCI)
Implementing Cisco Data Center Unified Fabric (DCUFI)
Troubleshooting Cisco Data Center Unified Computing (DCUCT)
Troubleshooting Cisco Data Center Unified Fabric (DCUFT)
Designing Cisco Data Center Unified Computing (DCUCD)
Introducing Cisco Data Center Networking (DCICN)
Designing Cisco Data Center Unified Fabric (DCUFD)
Configuring Data Center Unified Computing (DCUCS)
Configuring Cisco Nexus 7000 Switches (DCNX7K)
Implementing Cisco Threat Control Solutions (SITCS)
Implementing Cisco IP Routing v2.0 (ROUTE)

References

1. NIST 800-53 Special Publication, “Security and Privacy Controls for Federal Information Systems and Organizations” April 2013.

2. PCI-DSS; Payment Card Industry Data Security Standard

3. Cisco Validated Design Program, http://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.html

4. Nexus 5000 Design Best Practices, http://docwiki.cisco.com/wiki/Nexus_5000_vPC_Design_Best_Practices

5. Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.1(3)N1(1), http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration_limits/limits_513/nexus_5000_config_limits_513.html

6. Cisco Nexus 5548P, 5548UP, 5596UP, and 5596T Switches Data Sheet, http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/data_sheet_c78-618603.html