# Good example of essay on big switch network design

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Big Switch is a medium-size sales organization operated by 100 employees with annual turnover of 10$ million. It has a number of departments including sales with 30 employees while other 70 employees are spread across Finance, Operations, Human Resources, Marketing, Technology and corporate office in 10 offices in United States. Big Switch network consist of a backbone, campus, data center, branch/WAN and Ethernet edge. Due to recent security breaches in the campus network Big Switch desires an infrastructure that will provide sufficient security for its operations.

Acting on mandate as a network analyst, I will design a network infrastructure that implements VLAN segments, protect against MAC layer attacks, protect against VLAN attacks, protect against spoofing attacks, and finally secure the network switches.

Traditional networks usually use perimeter defenses to protect the data center from external threats while omitting internal threat agents. If an attacker has free access to the inner network, it has freedom of launching surface attacks. Since no system attack surface defense is fool proof, eliminating unwanted access is the first step in reducing risks of system breach. In a traditional system trust boundaries are located either on or external to the data center perimeter. Usually, a DMZ and SSL VPN provide protection from unauthorized access, but virtually do nothing once a threat gets to the data center network. Local devices also have full access to the network once a user is authenticated. Perimeter control features have been used with the believe that they control unauthorized access to the system attack surfaces. This assumption is however misguided.

Another problem is that the data center is one large broadcast domain that allows a device looking for an IP address for instance, to send and receive responses if the address is assigned to an active server on the network. An attacker can therefore see all the servers and resources in the data center, providing potential access to all the system attack surfaces. With dedication and the right skills, an attacker can crack the surface in no time.

VLAN segmentation is a technology that creates a collection of isolated networks within the data centre. Each network is isolated by a different broadcast domain to prevent access to system attack surfaces. Segmentation potentially reduces packet-sniffing capabilities and increases threat agent effort. Thus, authorized users only see the servers and resources necessary for their operation. With VLAN segmentation, users in Big Switch can only sees the resources they need. For instance, sales personnel only access the resources they requite for their sales activities unlike in the present scenario where they can access even finance and corporate servers. Big Switch network consist of a backbone, campus, data center, branch/WAN and Ethernet edge. Due to recent security breaches in the campus network Big Switch desires an infrastructure that will provide sufficient security for its operations.

A VLAN separates devices by media access control addresses on OSI level 2 model. This is essentially similar to physically separating traffic with completely independent infrastructure, except that network traffic separation is possible through switches. VLANs minimize the visibility of the network more than previously possible within the limits of the flat infrastructure.

In order to achieve the desired levels of network segmentation, switch-based VLAN technology is used. An Ethernet IP sec VPN technology is also proposed to provide privacy for traffic traversing the perimeter of the sub-networks.

A combination of VLAN and VPN results in a network that has multiple levels to traverse before a security breach is successful.

## As shown in the figure below

A switch manages communication inside the sub-networks and passes traffic traversing the boundary of a sun-network to the adjoining router or firewall.

This significantly minimizes the security obligations of a particular device.

The current network in Bridge Switch is a typical comprises of a campus, core backbone, data center, internet edge and branch/WAN. Thus, no equipment would be needed to achieve the same network functionality.

Te fig. above illustrates the use of four individual VLANs separating internal protection, general assets and critical assets. Subscribing to these assets are four IP sec tunnels with a subset of SA’s that creates connection to outside sub-networks. VLAN will communicate on a separate subnet as SA’s are identified with an IP subnet and not VLAN itself.

In this case one SA will be defined for critical resources VLAN1 while another will be defined for general resources VLAN2. Protection communication is on VLAN 3. VLAN 3 has the highest prioritization and as a matter of fact, traffic from external location will not be allowed in VLAN3. VLAN 3 will only be used for traffic inside the perimeter. Thus, a device outside the perimeter attempting to communicate with a device on BS IP sec will fail because the incoming VPN port does not recognize VLAN and traffic will subsequently be dropped. VLAN traffic will remain protected and within the confines of a particular BS department. With this segmentation using VLANs, secure communication is facilitated. Likewise, creating IP sec tunnels using SA's allow separation of communication according to specific BS departments. Using an IP sec security protocol supports strong authentication protocols such as cryptographic authentication and encryption. Many routers and layer 2/3 switches support IP sec through Access Control List entry mode. SA selectors will allow ACL entries that force a router to apply IP sec protocol certain TCP/IP traffic profiles. IP is usually implemented at lower layers exposing TCP/UDP header information. Thus, it is efficient to filter TCP/UDP traffic into a set of SA allowing the filtering mechanism to handle all the traffic that enters or leaves IP sec device with no room for hosts at the terminal of IP sec to inject malicious packets or analyze the network.

## Security

VLAN benefit from switch security capabilities apart from segmentation. Basic switches IEEE Std 802. 1D operates at layer two of the OSI model.

However, using 802. 1Q switches allows for the segmentation of the network. In this case, it is favorable to use this kind of switches as they have the capability to manage a collection of devices.

In the VLAN/VPN solution MAC security attacks such as flooding can be prevented by limiting the number of MAC addresses that can be utilized by a single port. Tagging attacks can be mitigated through configuration settings. By setting the DTP to off on all non-trusted ports, switch ports will be unable to receive fake DTP packets. For the case of VLAN hopping and attacks between devices on a common VLAN, a solution can be grafted that tighten up trunk configurations and negotiation state of unused ports. All unused ports are placed in a common VLAN while implementing private VLANs respectively.

In order to prevent MAC address flooding, configure port security to define the number of MAC. Using Cisco Catalyst switches, for instance, can restrict flooding of unknown multicast MAC-addressed traffic on every port in addition to restriction of unknown unicast destination MAC addresses. VLAN spoofing is always associated with DCHP spoofing devices that creates man-in-the-middle attack and can go entirely undetected as the intruder intercepts data. In mitigating this kind of attack, the Cisco Catalyst feature, for instance, determines which switch port can respond to DHCP requests according to their trust levels. If a port is designated as untrusted, DHCP requests are dropped.

## Deployment

Upon obtaining all the resources, a choice will be made of the favorable deployment option. A remote backup service is chosen as the best deployment option for Bridge Switch. A remote backup infrastructure is located within Bridge Switch data center and is accessible via agents installed onto the production servers physically located on the BS premises. Deployment will be executed in a predesigned manner that is expected to minimize business interruptions in all the BS departments. VPN deployment requires definition of authentication requirements upfront. DNS authentication will, thus, be defined together with username and password combinations to provide the required level of security. In addition, a user policy is documented to give VPN users in all the branches access to resources they require. Using a top down deployment architecture, meaning that deployment will proceed from the headquarters all through to the branch offices and all the departments.

In the illustrated deployment solution, virtual systems connect to internal protected network using VLAN interfaces. VSX Gateway utilized in this scenario connects to a VLAN switch using 802. 1q VLAN trunk which is an aggregate of all VLANs traversing through it.

The deployment option is favorable because a lot of virtual users in all the departments require internal resources and VLAN will provide scalability, granularity as well as security without impacting the existing IP address structure.

Since the network comprise of different network segments and subnets where internal users are located, users connecting to the network can potentially spread malware and viruses that can entire affect the whole network including servers and computers on the network. In order to ensure that only authenticated users pass and connect to the network, Security Gateway is implemented close to access networks before the core network. Deploying Security Gateway between the segments, LAN and data center as well as between LAN and Internet is essential during deployment and afterwards. Security Gateway of a particular segment authenticates users using a predefined method. This will significantly boost security.

## Conclusion

This paper has proposed a solution based on a combination of VPN and VLAN segmentation. The solution is viable for Bridge Switch in serving its purpose in its various departments. Specifically, the solution is expected to gather for VLAN segmentation, VLAN attacks spoofing attacks and provide a network wide security. VPN handles external traffic between sub-networks while VLANs minimizes the visibility of the networks and essentially accord each user exclusive resources it requires. Employees in finance department cannot have a view of the entire network, neither can those in any other department not authorized to do so.

## References

Donahue, G. A. (2011). Network Warrior. " O'Reilly Media, Inc.

Hooper, H. (2012). CCNP Security VPN 642-648 Official Cert Guide. Cisco Press.

Lammle, T. (2007). CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802. John Wiley & Sons.

Mauricio Arregoces, M. P. (2003). Data Center Fundamentals. Cisco Press.

Syngress, D. L. (2006). Firewall Policies and VPN Configurations. Syngress.