Perimeter protection case study examples

Business, Management

Introduction

In today's world business connectivity is crucial. In an organization, where computers and, hence, users connect through networking, there is better productivity and is able to make decisions much more quickly and reliable. These benefits are achieved through connectivity and sharing of information and resource. Users are able to communicate and use instant mails by connecting to the network. They can also share files. Also, through networking, it is possible to share hardware resources such as Hard Drives and Printer which makes use of resource much more efficient. In many organizations, computers connected through network also share a single connection, which otherwise would only be available on one computer. Furthermore, networking in a business environment allows for the organization of data and restricting it to certain resource (such as Server PC), which would allow for implementation of much better data security as well as ease of maintenance. In this report, we have attempted to connect offices of an organization which are in different cities of Australia. The aim is to build a network that is structured and secure while providing connectivity to all three offices.

Omega Research Main Office – Reston

There is a laxity of access criteria and policies. A very important step in designing our secure network is defining the topology of the network. Talking of the topology of the network, this refers to the logical layout of the network. On the physical side, we will need to provide a network distribution if the offices which are located in the different departments in the company.

The network will also need to provide connectivity to the servers, to the Internet, to remote sites, to business partners or even to other companies through telephone lines. As much as we are considering the physical topology, the logical topology must also be considered. The logical topology is affected to some degree by the physical topology, but with the advent of technologies like Virtual Local Area Networks (VLANs) and Virtual Private Networks (VPN), there has been considerable flexibility in the coming up of the logical design of the network.

When we are laying out the logical topology for Omega Research, we need to put into much consideration the policy that we set up for the organization, and we have to decide what our trust model is. We also have to decide which parts of the networks are less trusted and which ones are more trusted. We should also come up with a list of the groups of users on the network which needs to be grouped because of the fact that they are related in the nature of their work. We should also come up with a list of users and network devices which should be separated.

Securing attacks from the Internet

Most attacks are from the Internet. The communication between the three branches should be well guarded. Someone from San Diego branch should not access the database directly but should go through a proxy. All connections to the database should be filtered to ensure that all forms of attacks are known and avoided. There is a need to have a firewall that should be introduced with connections to the internet. This is shown in the new diagram below:

Figure 1: Firewall introduced

The firewall has been introduced in figure 1. All connections to the Internet are done via a firewall and, therefore, the attacks from the Internet are kept at bay.

Securing the user groups

There will be also the introduction of switches and routers to be used in the network. When we are laying out the logical topology of the organization, we need to put into much consideration the policy that we set up for the organization, and we have to decide what our trust model is. We also have to decide which parts of the networks are less trusted and which ones are more trusted. We should also come up with a list of the groups of users on the network which needs to be grouped because of the fact that they are related in the nature of their work. We should also come up with a list of users and network devices which should be separated. Figure 2 shows a graphical representation of my network proposal:

Figure 2: Group security

The design which is illustrated above shows a connection to the Internet with a border router and firewall, and the organization’s extranet servers which are connected to a third interface on the firewall. The firewall is a 4s switch and will be upgraded to a 3s switch if higher performance is required. The other connections to our core router constitute of the floor or building switches whose main task is to provide connectivity to the various departments in the organization and also to the intranet servers which are available in the organization.

This topology illustrates how devices, which have similar functionalities, can be grouped together to provide the required security measures for the organization. The various devices include extranet servers, workstations for the various users, and the intranet servers. Our creation of separate zones of security, we will be in a position to enforce the organization's security policy with the firewall rules which are appropriate and layer 3 access lists.

One of the key elements that my network design still lacks is the framework/infrastructure that we will use to manage the network. For this to be achieved, we will need to have in place at least one management workstation, one tftp servers, and at least one SYSLOG server. It is evident that we also need to have password management servers that will be used to manage the passwords that will be used for authentication purposes. The branches of three offices of the organization have their users using Microsoft password management systems which is something wanting. For this purpose, we will need RSA SecurID or Axent Defender, or RADIUS server. This will be implemented in all the three branches of the offices. The pilot implementation will be started at the headquarters of Omega Research. These servers will be used to manage the security of the organization; this will, therefore, mean that we create a separate VLAN for these servers which will be different from the rest of the devices on the network. For this isolation to be achieved, we will need to have a firewall that will isolate the management servers from the rest of the network. The traffic, which will be allowed into the management network, come from the managed devices or which are protected by encryption.

One of the goals in our design is to make sure that the management traffic

will be kept away from the production network so that the chances of being intercepted when on transit are eliminated by all means. The ideal way that this could be achieved is that we could make sure that each device should have a physical port on the management VLAN. This is not always easy to achieve due to physical limitations. If this is the case, management network should have an encryption through the use of ssh or IPSEC. The diagram below gives a representation of the management network.

Figure 3: Infrastructure management network

Securing routers and routers

The hosts in each subnet will be connected to the network through an Ethernet switch. A switch has the advantage that it provides a high network performance in that each host is put on its own collision domain, and also this setup enhances security because of the fact that arp based attacks is made impossible. Sniffing is also made impossible with this setup. Another option instead of deploying a switch is the use of a hub, but this is not desired by many designers because it has less security features and also low performance compared to switches.

Layer 3 design and access lists

Our design that we will use in layer 3 is simplified; w will have a central router which we will use it to connect to the different departments from the organization. Due to the fact that we have mapped out our trust model and security policies, we can then use access lists at layer 3 to implement the organization security policy. For the traffic that will be entering into a particular subnet, the packets, which will be allowed into the network, will be

based on the security policy for that particular subnet. In the same case, we will make sure that outbound traffic is filtered so that chances of spoofing is eliminated and the chances of having malicious or illegitimate activities. At this point, I will consider some good examples of access lists based on the Cisco IOS command set.

Let us take a scenario where the organization has a Windows 2000 file server (which is highly unlikely because of technology) and a web server on our management or server subnet. We have to find a way in which we will configure our access list so that the necessary traffic is permitted and all the other traffic is denied access. The commands which are shown below shows the concepts that our layer 3 uses to get the design. The commands would need to be expanded further so that a production environment will be accommodated.

Our next consideration will be that of workgroup subnet, which has been populated with desktops but with no servers in place. Due to this fact that servers will not be expected to appear here, our inbound tcp traffic will be limited. This is shown in the commands that follow:

The final thing we will want to do is make sure that all the traffic, which is leaving each subnet, is filtered so that spoofing does not occur. This could mean that there is a machine in the network which is not configured correctly. It could also mean that a machine in the network could have been compromised, thus attempting to launch an attack which is similar to DDOS. For the outbound filters to be defined for use in the workgroup subnets, the commands shown below suffice.

Securing layer 3

We have shown in the design above how we are going to implement our layer 3 so that we implement the security of the organization. For enough protection against any form of attack, we are going to make sure that routers are secured against attacks. There are many ways, which are excellent, of making the Cisco routers against attacks. I will point out some key strategies that are very relevant to this paper.

There are various ways of managing the safety of the routers. One of these ways is the management of the virtual LANs which ensures that traffic from the management subnet does not traverse the network that is used by production. The ports in the management should be configured to have access lists to make sure illegitimate connections are kept at bay. Another way of ensuring management traffic is always secured is by use of Out Of Bound (OOB) communication through the terminal server. We will use strong authentication, which is provided by the password servers (these servers are one-time) such as RSA Security's ACE server. If there is in band communication is necessary, encryption communication protocols such as ssh should be used.

For us to meet our auditing requirements, we will be required to log into the SYSLOG servers which are located on the management network.

Layer 2 design

In the previous sections, we have explored ways in which layer 3 design can be secured through the use of access lists and hardening of routers themselves. At this stage, we will look at ways of addressing the threats that come in layer 2 designs and look further at the way that will allow us to

enforce the security policies in this layer.

One thing, which will guide us, is to ask ourselves one question, which is how to maximize port security. We should be able to look at cases such as where an attacker can attack a host in one VLAN and being able to jump to another VLAN and attack a host in that VLAN. Is this scenario possible? This is possible, and; therefore, it needs us to look at ways of ensuring that this does not happen. The only way of ensuring that this does not happen is by securing the ports where the attackers will use to jump to the other VLANs. There is also another loophole where a misconfiguration can provide a way in which an intruder can gain access to the network. For all these to be kept at bay, we will configure only one VLAN per switch. By this, we will be able to have maximum security of the VLANs. This is the most secure form of security in VLANs, and it is recommended for organizations like ours which has many departments and handles sensitive data in these departments. What is more, it is the most secure way of protecting likely attack points like the organizational Internet when facing server segmentation.

Studies have shown that it is much possible to jump from one VLAN to another by injecting frames which specially created in the default configuration. A research, which was commissioned by Cisco, has shown that there is minimal risk when VLANs are configured using the best practices. The structure and the configuration of VLAN will normally depend on the budget allocations of the designer combined with configuration confidence. Designers will have to make careful considerations basing on the risks and costs before making their final decisions on the final configuration.

Given the fact that the gateways to the network are the switch ports, we will

have to look for a way of disabling these ports and making sure the access to these ports is controlled. Since monitoring the ports will be tedious for system administrators, there are ways of monitoring the network of the organization. One of these ways will require users to authenticate themselves by use of RADIUS or LDAP before they gain access to the network resources. This feature is common in Cisco's User Registration Tool (URT) or from other vendors competing with Cisco. Cisco's URT will enable users of the network to be assigned a VLAN according to the credentials they have been assigned.

Another way of ensuring this is through the limiting of MAC addresses so that every flood that will be experienced in MAC will be an indication of a possible intrusion to the MAC address. For this is to be avoided, switches should be configured with static MAC assignments because this will redirect frames which are directed to the ports to the specified ports.

The organization would also make sure that time that MAC addresses exist in the network is limited. This will ensure that a timeout is always there so that the creations of a MAC address will always timeout after sometime.

Securing network 2

As much as we have seen some of the good strategies which are used in securing the organizational network, we will also take additional steps and make sure that the switches are secure from attacks. These attacks include attacks against layer 2 protocols like Spinning-Tree Protocols (STP), which sometimes lead to problems and issues like Denial of Service.

Locking down the security on the layer 2 devices will follow the principles that are used when locking down the routers like disabling insecure default

configurations, making sure that the management channel is safe and that passwords which are strong and through one-time infrastructure. After we are able to secure the switch, we will then make sure that the infrastructure is secure against attacks on the layer 2 protocols which are lying underneath.

STP is used by switches to create forwarding takes and to create tree-like topology, which is used to forward frames through the path which is fast and without loops in the network. The switches use Bridge Board Data Units to share data that concern the topology of the network.

The work of the STP is to manage the changes that usually take place in the topology but most of the time it is susceptible to failure if we have many hosts, which are transmitting BPDUs, and affecting the spanning tree. This usually happens if a switch would be attached to the organizational ported. This could also happen if one of hosts is running Linux.

In order to have an optimal performance, we will need to have the root bridge being located in the area where there is a lot of bandwidths. If don’t want the roots to appear, we make sure that Root guard is enabled on those ports.

References

Huang, S., MacCallum, D., & Du, D.-Z. (2010). Network security. New York: Springer.

Poole, O. (2012). Network security: A practical guide. New York: Routledge.

Wang, J. (2009). Computer network security: Theory and practice. New York: Springer.