Example of research paper on cisco network architecture

Business, Company

Chapter 8 Security Services Design

Network security is a vital component of any enterprise that seeks to protect its information. Lack of a security system may result to loss of property, money, or damages. Network security includes the use of firewalls, network access controls, and intrusion detection and intrusion prevention systems. Firewalls are designed to ensure that network intrusion is prevented. Certain issues need to be considered when designing firewalls. For instance, the user policies and connection information should agree to ensure access to network resources. The Cisco SAFE architecture is a major security component of its enterprise networks.

One needs to recognize the benefits that a firewall offers to an organization. According to Doherty and Anderson (2006), the use of firewall restricts unauthorized access by unwanted persons to your network. Firewalls will protect the network by continuously monitoring the broadband connection and will only allow genuine traffic to access your network. Furthermore, firewalls control access to network resources, mitigate denial-of service attacks, and apply deep pack inspections as a means of detecting unwanted traffic in the network (Hutton and Tiso, 2011). A common example of a firewall type used is the stateful packet inspection (SPI) firewalls. If the request comes from the outside or a hacker, the SPI firewall will block its access since there was no initial request from the computer. The use of SPI firewall increases the level of security in a home network. Another example of a firewall to use is the personal software firewall (Doherty and Anderson, 2006). This firewall software acts as a barrier to any information from company computers that may go to the internet.

The firewall is placed between the enterprise network and the internet. This is achieved by installing the firewall device between the broadband cable and the enterprise network router. This could also be achieved by turning on the SPI firewall located in the router.

Firewall Modes

A number of firewall design considerations need to be considered when designing a firewall. Firewall modes can be either in transparent mode or router mode. The router mode is when the firewall has a three-layer device in the network. The router mode can support many interfaces. The router mode allows network address translation and offers IP routing support. Since each interface is on a different subnet, the IP routing support manages the IP addresses of each interface. Network address translation allows the router to function as the connection between the public network and the organization’s network. Benefits associated with network address translation include resolving of IP routing problems by supporting overlapping IP addresses, the use of private addresses inside the enterprise network and attackers cannot be able to discover the real addresses of the enterprise network.

A transparent firewall mode is a more modern mode that has a two-layer firewall. The transparent firewall utilizes a single IP address to manage packets originating from the firewall. This mode also allows certain traffic types that are blocked by the router mode. Examples of unsupported protocols that a transparent firewall can allow include the Routing

Information Protocol (RIP) and the Open Shortest Path First (OSPF) (Hutton and Tiso, 2011).

Zone-based Policy Firewall

This is a new design supported by the Cisco IOS Firewall Feature Set. This model can be implemented on integrated service routers and asymmetric routers. A zone is used to identify a boundary where traffic will pass through a number of policy restrictions as it moves to another part of the network. This creates security borders in the network. An advantage of zone-based policy firewall is the ability to apply policy across groups of interfaces and allow deep packet inspection.

A number of things need to done before doing any configuration. One needs to be sure what the security policy is and how the network is designed. Further, the traffic that moves across the network should be known. Policies will be applied to the traffic moving between different zones as stated earlier. It is vital to know the amount of traffic since extra duties in a router may slow it down.

Network Security with Access control

Access control is vital to ensure there is limited access to the network resources in Cisco architecture. Access control has several functions that are crucial in a network security design. One of the functions is to identify the identity of the user and verify the user’s access. Secondly, through access control, enforcement of security policies is assured. Security software will be used before allowing network access. Access control allows isolation of

devices that do not meet requirements of a company’s security policy to be separated and attended separately.

Network access control provides access of network resources to known and trusted client devices. Cisco has a network access control appliance agent that is installed on a client device. This ensures that a client device is assessed critically before allowing it to access the network. In case, a virus has compromised the client device, the network access control moves it into a quarantine segment. Once the virus is removed, the client is allowed to access the network. The Cisco 802. 1 X/IBNS and network access control provide additional functions such as posture validation and user authentication.

Cisco has two types of network access control, the NAC framework, and the Cisco NAC appliance. According to Paquet (2009), the NAC framework utilizes third party software present in the Cisco network infrastructure to improve security compliance. The NAC framework best suits high performance network environments. The Cisco NAC appliance, on the other hand, combines the functions of the network access control to provide a turnkey solution to control network access. This will be best suited if the organization requires a simplified and integrated tracking operating system and vulnerability updates and antivirus patches (Paquet, 2009).

Intrusion Detection and Intrusion Prevention Systems

Cisco architecture provides an intrusion detection and prevention solution that identifies and stops network viruses, worms, and unwanted traffic. Threat detection and mitigation is essential to ensure that the network is

safe from outside attacks. Increasing advances in technology have resulted to an increase in the rise of complicated attacks on networks. This necessitates the need to have high-tech security systems to cope with the attacks. Cisco’s SAFE architecture utilizes network telemetry to observe the network activities. In addition, any information collected by the routers and firewalls is used in determining possible threats to the network. The intrusion prevention systems, network access control, firewalls, monitoring and analysis software are used to identify and respond to potential attacks to the network. The architecture has the capacity to identify the origin of the attack, envisage the attack path, and provide possible response actions to the attack, which include packet filtering, connection resets, source filtering, rate limiting, and isolation of compromised systems.

Intrusion Detection Systems

These systems are used to observe all traffic on the network. Intrusion detection is not located on the traffic path, but rather it has promiscuous interfaces that are used to monitor multiple networks. Once an attack is detected by the intrusion detection system, an alert is generated and sent to the management station. The intrusion detection system has also the ability to send a TCP reset to the end host, which terminates any unwanted TCP connections. The advantage of using promiscuous interfaces is that the sensor does not affect packet flow with the forwarded traffic. The downside is that the use of promiscuous interfaces cannot prevent unwanted traffic from reaching its target.

Intrusion Prevention Systems

These devices are located found in the traffic path (Hutton and Tiso, 2011). The intrusion prevention system listens to the inline network traffic and either permits or denies packets and flows into the network. Once malicious traffic is detected, the intrusion prevention system will block the unwanted traffic and send an alert to the management station.

Intrusion Detection and Intrusion Prevention Design Considerations

According to Tiso (2011) the intrusion detection system needs to be connected in promiscuous mode, where the packets do not flow into the sensor, whereas, for the intrusion prevention systems, the system is set in the traffic path. Location of the systems is also important. Location considerations include the perimeter of the network where the network is most exposed, internal to the network at the zones of trust and at servers where an event can be most crucial (Tiso 2011).

References

Doherty, J. & Anderson, N. (2007). Home Network Security Simplified. Indianapolis: Cisco

Systems.

Paquet, C. (2009). Implementing Cisco IOS Network Security (IINS): [authorized self-study

Guide. Indianapolis: Cisco Press.

Tiso, J. (2011). Designing Cisco Network Service Architectures (ARCH) Foundation Learning

Guide. Indianapolis: Cisco Press.

Tiso, J., & Hutton, K. (2011). Designing Cisco network service architectures

(ARCH):

Foundation learning guide (3rd Ed.). Indianapolis, IN: Cisco Press.