U.P.B. Sci. Bull., Series C, Vol. 71, Iss. 3, 2009 ISSN 1454-234x

GENERAL GUIDELINES FOR THE SECURITY OF A LARGE SCALE DATA CENTER DESIGN

Jalal FRIHAT[1], Florica MOLDOVEANU[2], Alin MOLDOVEANU[3]

Securitatea unui centru de date de scară largă se bazează pe o politică efectivă de securitate, care defineşte cerinţele de protecţie a resurselor reţelei contra pericolelor de securitate interne şi externe, şi asigură integritatea şi securitatea datelor. În acest articol sintetizăm principiile securizării stratificate şi modul în care au fost aplicate în proiectarea reţelei unui centru de date de scară largă.

The security of a large scale data center is based on an effective security policy that defines the requirements to protect network resources from internal and external security threats and ensures data privacy and integrity. This paper summarizes the layered security principles and how they have been applied in the design of a large scale data center network.

Keywords : Layered security, Firewall IDS,VPN, VLAN

1. Introduction

A data center is a facility used to house computer network components, such as switches, routers, data storage systems and servers. It generally includes backup power supplies, redundant communication lines connections, and environmental conditions control (like air conditioning, humidity control and fire systems). A data center represents the heart of any organization’s network. Companies relay on the data stored in the data center to interact with its employees and customers.

The proliferation of the Web-based technologies makes the data center more vulnerable to security attacks. Any security attack on the data center can destroy the whole organization’s network and data.

Several researches were dedicated to the security issues and the design constraints of large scale data centers from different points of view. The authors

[1] PhD student, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania, e-mail: Frihat_Jalal@yahoo.com

[2] Professor, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania

[3] Lecturer, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania

of [14] discuss the security strategies such as consolidation, relocation, migration, expansion and review of asset management policies. The authors of [15] overview the communication network design problems that arise with large numbers of nodes, links and switch costs.

The layered security architecture is a modern solution to the complexity of security problems that have to be solved for a data center. A layered security solution consists of a set of tools that achieve best security level for the data center. It is designed to protect critical network resources that reside on the network. If one layer fails, the next layer will stop the attack and limit the damages that may occur. Some layered security models are discussed in [16] and [17].

This paper, first describes shortly the most important solutions, technologies and tools that can be used to secure a data center. Then, a layered security model that can be used for a data center is presented. We discuss the security problems at a data center and their solutions based on the layered security architecture. Finally, it is presented a design proposal of a data center layered security architecture.

2. Data center security technologies

Information stored at the data center must be protected from any security threats that may destroy or modify it in any unwanted way. These security threats can originate from hackers outside or from users inside the data center network. Different solutions to the security threats can be used together to achieve the highest possible data protection. Some of these technologies are:

- Firewalls
- Network intrusion detection and prevention systems
- Virtual Local Area Networks (VLAN)
- Virtual Private Network (VPN) and IPSec

Firewalls

A firewall is a device or a software configured to permit, deny or proxy all traffic between different networks that have different security levels, typically between an internal network and the Internet, based upon a set of rules and other criteria. A firewall may consist of several equipments, including a router, a gateway server, and an authentication server.

Firewalls protect sensitive data in the internal networks from outside threats and also within the network itself from the inside users. No internal host is directly accessible from the external network and no external host is directly accessible by an internal host.

The major aspect of the design of any network that is connected to Internet in a secure manner is to create what is called a ***Demilitarized Zone*** "DMZ", which is a network that exists between the protected and the unprotected network. Also the firewall is used to protect the DMZ form any external attacks coming from the Internet. Internet users can freely enter the DMZ to access public Web servers, but screening firewalls exist at the access point to filter out unwanted traffic, such as floods of packets from hackers who are trying to disrupt operations.

A firewall can be integrated into a router or a switch, it can be software-based, hardware-based or can be implemented as additional components to existing hardware or software.

Firewalls provide a combination of functions to protect networks from malicious traffic. The more common components of a firewall are the following:

- Static packet filtering. Static packet filtering controls traffic by using information stored within the packet headers (destination IP address or subnet, source IP address or subnet, destination service port or source service port). Packet filter services deployed at the data center consists of Access Controls Lists (ACLs) that are defined in the firewalls or/and routers. ACL deployment in the data center is important for limiting access to and from networks. ACLs can be set to filter by ports (source and destination ports of the packet). In addition, ACLs are very difficult to write and more difficult to manage at large scale.
- Dynamic packet filtering. A dynamic packet filter is a firewall that can monitor the state tables of active connections and use this information to determine whether to allow or deny the packet, by recording session information such as IP addresses and port numbers.
- Stateful filtering. Stateful rules are protocol-specific, keeping track of the context of a session. This allows filtering rules to differentiate between the various connectionless protocols (such as UDP, NFS, and RPC).
- Proxy. A proxy firewall (also known as an application gateway or forwarder) is an application that mediates traffic between two network segments. Proxies are often used instead of filtering to prevent traffic from passing directly between network segments.

The firewall normally has three interfaces: Internal interface, DMZ interface and the External interface. Each of these interfaces is connected to one network either internal, DMZ or external. Also the firewall may act as a proxy that makes any connection request to the Internet on behalf of a host.

A firewall stands between the protected and the unprotected network. The firewall architecture is shown in Fig. 1.

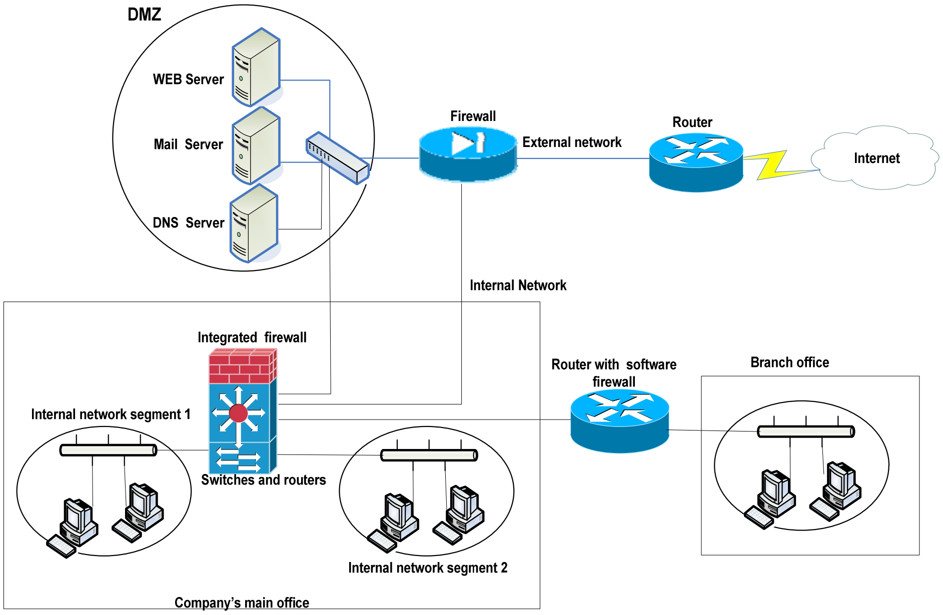

Fig.1. Firewall architecture

Network Intrusion Detection and Prevention Systems (IDS/IPS)

Network IDS/IPS devices are deployed at the data center to provide a good level of protection for the data center. They are the second level of protection for server farm components. An IDS detect the so called “bad traffic” based on signatures and protocol anomaly detection. An IPS not only detects the “bad traffic” but also drop and block the connection transporting real “bad traffic”.

The network IDS sensors can be logically configured to reside behind the firewall. This allows the sensor to avoid network attacks that were not filtered while passing through the firewall. In the server farm, many servers often exist in the same subnet. If one server is compromised, the possibility of other servers as being compromised increases. Alternatively, if the server is secure and uncompromised and the attacker is able to gain control of the switch, data traffic to and from the server(s) can be captured regardless of the security of the server operating system and applications.

Virtual Local Area Networks (VLANs)

Virtual networking refers to the ability of switches and routers to allow any random collection of virtual LAN segments within a network to be combined into an independent user group, appearing as a single LAN. A VLAN has the same attributes as a physical LAN, but it allows hosts to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices. VLANs offer benefits like efficient use of bandwidth, flexibility, performance, and security. If one VLAN is compromised by a hacker it can be isolated from the other network segments to minimize damage. In addition, the traffic between different VLANs can be controlled according to the predefined ACL at the firewall (no user can access other VLAN unless its VLAN is granted permission to access that VLAN). In some particular situations it is important to control traffic between different hosts belonging to different VLANs. For example, in Fig. 2 user A at the human resources department (that belongs to VLAN1) can not access the application server of the financial department (that belongs to VLAN2) unless the ACL is configured to allow that traffic.

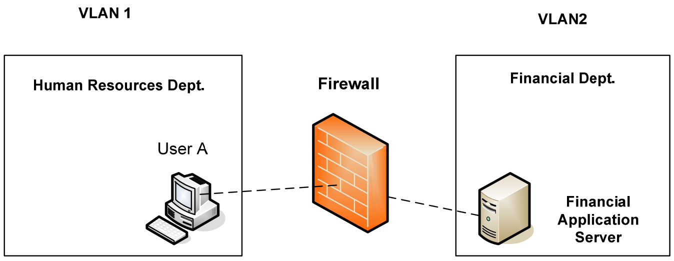

Fig.2 Traffic control between VLANS

Virtual Private Network (VPN) and IPSec

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining confidentiality through the use of a tunneling protocol and security measures. Virtual private networks can be more cost effective than dedicated private lines and represent a secure way for different corporations to provide users access to the company network and for remote networks to communicate with each other across the Internet.

VPN involves two parts:

- the protected (inside) network, which provides physical and administrative security for secure data exchange

- the unsecured network, (usually through the Internet).

Generally, a firewall sits between the remote site and the internal network. A VPN makes it possible to have the same protected sharing of public resources for data. Companies today are using VPNs for both extranets and wide-area intranets [1].

A client may pass authentication data to an authentication server inside the boundary network. Many VPN client programs can be configured to require that all IP traffic to pass through the tunnel (while the VPN connection is active) for increased security. This means that while the VPN connection is active, all access outside the secure network must pass through the same firewall as if the users were physically connected to the inside of the secured network. This reduces the risk that an attacker might gain access to the secured network by attacking the VPN client's host machine.

Tunneling is the transmission of data through a public network in such a way that routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network protocol data so that the tunneled data is not available to anyone examining the transmitted data frames. Tunneling allows the use of public networks (example: the Internet), to carry data on behalf of users as though they have access to a private network.

Secure VPNs use cryptographic tunneling protocols to provide:

- Confidentiality (blocking snooping and thus packet sniffing)
- Origin authentication (blocking identity spoofing)
- Message integrity (blocking message modification)

Secure VPN technologies may also be used to enhance security within the organization’s network infrastructure. In addition, they include the Secure Socket Layer/Transport Layer Security (SSL/TLS), which are cryptographic protocols to provide a secure connection for the Internet, and IPSec (IP security).

3. Secure network management

The management of every network device in the data center needs to be secured to avoid unauthorized access. Usernames and passwords on the local database of each switch or on a centralized access control server, use Authentication Authorization and Accounting (AAA) server technology in conjunction with a Terminal Access Controller Access Control System (TACACS) or RADIUS (Remote Authentication Dial-in User Service) server. Usernames and passwords in the local database can be used if the access control server becomes unavailable. Also, it is important to have system log (syslog) at an *informational level*. When the syslogs file is available, it should be sent to a server rather than stored on the switch or router buffer. When a switch reload occurs, syslogs stored on the switch buffer are lost, which makes their use in network problems troubleshooting difficult. Proper management of configuration changes can considerably improve data center accessibility, by periodically retrieving and saving configurations and by auditing the history of configuration changes.

Software compatibility is critical for achieving maximum data center availability. Before upgrading to a new release, it is important to check the compatibility of the new software with existing hardware [5, 7].

4. Security problems and their solution at the data center

As mentioned in the previous section, there are several security threats that affect the data center. This section provides a brief description of these security threats and the available solutions to mitigate them [5, 6, and 7].

Unauthorized Access

To prevent unauthorized access, the AAA (Authentication, Authorization, Accounting) server is used to provide login authentication, command based authorization, and accounting of user information. Remote Authentication Dial-in User Service (RADIUS) is one of the AAA server implementations, which is used to maintain a central location of usernames and passwords information. One of the disadvantages of the RADIUS is that it encrypts only the password in the access-request packet from the client to the server. This leaves other information such as username, authorized services, and accounting open to be captured by a third part.

Local AAA implementations use the local usernames and passwords database on the switch to authenticate user's login attempts. Command authorization per user can be performed by setting the individual user privilege level in the local usernames and passwords data base.

MAC Flooding

MAC flooding is the effort to make use of the fixed hardware limitations of the switch's Content Addressable Memory (CAM) table. The switch CAM table stores the source MAC address and the associated port of each device connected to the switch. The CAM table contains a limited number of entries. Once CAM is full, the traffic is flooded out to all ports on the same VLAN on which the source traffic is being received.

Multiple well known tools can be used to perform ethical hacking in testing security settings. Each tool can fill up the entire CAM table causing all traffic on that particular VLAN to be flooded, resulting in the ability to sniff all traffic. Once all traffic is flooded from the switch, all traffic in the VLAN can be seen. Features that can be deployed to guard against MAC flooding are:

- Port security. Port security allows IT staff to specify the MAC addresses for each port or to permit a limited number of MAC addresses. When a port receives a packet, the source MAC address of the packet is compared to the list of the source addresses that were configured manually on that port. If the MAC address of a device differs from the list of source addresses, the port either shuts down permanently or shuts down for the time that has been previously specified, or drops incoming packets. The port's behavior depends on the configuration to respond to a security threat.
- IEEE802.1x: IEEE 802.1x uses Extensible Authentication Protocol (EAP) to authenticate a device before allowing it to forward any traffic to the switch. The supplicant (client) must be approved by the authenticator (switch). The authenticator utilizes a RADIUS server to authenticate client requests. If the client does not authenticate, the client is not connected.

Address Resolution Protocol (ARP) Spoofing

ARP request messages are placed in a frame broadcast to all devices on a segment; each device on the segment receives the broadcast message and examines the required IP address. Either the host that owns the IP address being requested or a router that knows the location of that host responds to the request by sending back the target MAC address via unicast frame. When the attacker sends an ARP, the server updates its ARP table and forwards traffic to the attacker because server thinks that the attacker's computer is its default gateway [3].

There are several features available that can be used as tools against ARP spoofing attacks:

- Port Security : as discussed in the previous section
- IEEE 802.1 x : as discussed in the previous section
- Static ARP entries: a static ARP configuration can be used in an extremely secure data center environment, where security is more important than the operational overhead associated with maintaining static ARP mappings (The MAC addresses for each port are mapped to the IP addresses manually)
- VLANs: can be used to provide protection at layer 2 of the OSI model (the data link layer), and to provide logical network segmentations into smaller logical networks. VLANs isolate data center servers residing in the same VLAN or broadcast domain. This feature provides an effective means for guarding against ARP-based attacks.

IP Spoofing

IP spoofing occurs when an attacker gains unauthorized access to a computer by making it appears as that the traffic has originated from a trusted host. IP spoofing is used to make other attacks like a sequence number predication that is used for session hijacking. Access Control Lists (ACLs) are deployed to prevent IP spoofing [4].

Denial of Service (DoS)

The purpose of these attacks is making the victim machine or victim network resources or services unavailable. In DoS, the attacker floods the victim host with a huge number of packets in a short amount of time. DoS is concerned only with consuming bandwidth and resources of the victim machine. The attacker uses a spoofed IP address as the source IP address to make tracking and stopping of DoS very difficult. It is possible to the attacker to use multiple compromised machines which he has already hijacked them to attack the victim machine at the same time (this attack is known as Distributed DoS) and it’s very difficult to track and stop. Packet filtering (using Access Control List) by firewalls, encryption and authentication techniques can be employed to reduce the risk and impact of DoS attacks.

Network inspection

Network inspection techniques are used to discover security vulnerabilities within a network. Firewalls use packet filtering to prevent unauthorized access to devices residing within the data center and provide filtering services up to Layer 4 of the OSI model (transport layer). Intrusion detection sensors use signatures to watch for specific attack trends to prevent application and upper-layer attacks. A signature is a specific pattern being looked for within traffic.

Viruses, worms and Trojans

Viruses, worms and Trojans can be mitigated through the use of Antivirus solutions that can be software based or hardware based. Antivirus software defends against the threats posed by a virus. There are a number of techniques that antivirus software use to detect a virus: signature scanning and heuristic.

Signature scanning involves searching for a pattern that could indicate a virus; these patterns are referred to as signatures. Heuristic scanning looks for the characteristics of malicious software. The advantage of heuristic scanning is that is does not rely on bit level signatures.

Internal security

It is known that more than 50% of the attacks and security breaches affecting any corporate network came from users and devices inside the network. Internal threats can originate from many sources:

- Devices compromised by outside attackers
- An employee within the network
- Accidental employee actions

There are several solutions for the internal security threats like firewall, IDS, antivirus, as will discussed in next section.

5. A layered security architecture for a data center

The data center security is based on an effective security policy that defines the connection requirements, access and requirements to protect resources from internal and external threats and to ensure data privacy and integrity. A layered security architecture provides a scalable and modular approach for deploying security between the multiple data center tiers.

The first layer of the layered security architecture is the perimeter layer; it is the first line of defense for any security threats coming from an untrusted external network. The perimeter is the area where the internal network ends and the external network (Internet) begins. The perimeter consists of one or more firewalls and protected servers located in the Demilitarized Zone (DMZ). The DMZ contains Web servers, email gateways, network antivirus, and DNS servers.

The second layer of the layered-security model is the network level, which refers to the internal LAN and WAN. The internal network may include desktops and application servers.

The third layer is the host level concerning the individual devices, such as servers, desktops, switches and routers.

The forth layer is the application-level security. Poorly protected applications can provide easy access to confidential data and records. Applications are being placed on the Web for access by customers or even remote employees with increasing productivity.

The last layer is the data-level security which entails the use of encryption. Data encryption is required when it travels across the network. If all other security measures fail, a strong encryption scheme protects these proprietary data.

The security services that must often be deployed in the data center to defend against different threats applied to different levels [16] are:

1. <u>Perimeter defense</u>. Several security means can be used: firewalls, network-based anti-virus solutions and VPN technologies.

2. The network level includes Intrusion Detection Systems, networks access control, network management systems and user authentication.
3. Host level includes: host based IDS, Anti-virus and access control/user authentication.
4. Application-level security has great importance. Poorly protected applications can provide illegal access to confidential data stored at data center. Application security includes access control and authentication of users and devices.
5. Data-level security includes encryption and user authentication.

6. Design of a data center security architecture

Improperly secured data centers are targeted of security attacks by hackers and worms, which can cause considerable damage of data. Secure network architecture implies what is called "defense in depth", which uses multiple security layers and related means against security threats.

Any security strategy begins with a security policy, which defines how to implement security processes and technologies. One component of the security policy should deal with the particular requirements of the data center, its application requirements and authentication and authorization of users. The policy determines the security technologies, management that enables policy implementation and enforcement. The network components are an essential part of the security because they connect applications and users. The network should provide a hard first layer of security that protects operating system and applications. It is important to create a secure environment not only at the network outside boundary, but also in security zones inside the data center. Separating the network into VLANs allows IT staff to control user access to each application. A successful security policy satisfies the following requirements:

- Security threat defense: monitor any improper behavior in the network; network monitoring technologies include firewalls and intrusion detection (IDS)
- Identity management: users and devices access to the network resources is controlled based on access policies, such as Remote Authentication Dial-in User Service (RADIUS) access control servers.
- Defense in depth: mitigates known and unknown security threats.
- Network segmentation: segmenting network infrastructure into security zones that provide strong access controls. For example, the network can be divided into internal, DMZ and external zones. The internal zone has the highest security level and includes the internal network devices and servers. The DMZ has a moderate security level

and contains the DNS, WEB and mail servers. The external network is any network outside the enterprise network and has the lowest security level.

- <u>Service integrity</u>: protects data on application and storage servers.
- <u>Flexibility</u>: security architecture being capable to quickly adapt to new threats.

The following steps are important to secure the data center:

- ***<u>Security VLANs</u>.***
  Data center has to be divided into areas or VLANs that are logically separated from one another to maintain an attack at minimal damage. Each VLAN has a different security level than other VLANs. For example, there are: database servers' VLAN, network devices VLAN, internal users' VLAN and data storage VLAN. Firewalls can be used to provide secure connectivity between application and server environments. User access to different VLANs can be controlled by the access rules that are configured in the firewall.
- ***<u>Protection for critical servers and hosts</u>***
  Behavior-based Intrusion Detection Systems can be used to detect any attacks to the critical servers and hosts.
- ***<u>Utilization of network ID</u>S***
  Network IDSs can be used to analyze traffic streams to identify and prevent attacks such as DoS. IDSs can be also configured to control firewalls or routers to block packets from known malicious traffic.
- ***<u>Implement VLANs on switches</u>***.
  When each host belongs to a VLAN, security attacks can be prevented from spreading to other hosts; hosts on each VLAN can communicate only with the default gateway, not with other hosts.
- ***<u>Data center access control</u>***.
  Access to data center resources is granted only for authorized users and administrators.
- ***<u>Efficient management and monitoring tools</u>.***
  Communication between data center network devices must be secured using a dedicated administration VLAN. It is recommended to encrypt management traffic with Secure Socket Layer (SSL), Simple Network Management Protocol (SNMP) version 3 or Secure Shell (SSH) technology.

In this section there are presented the design guidelines used in the design of the network architecture for a large data center, to provide a secure, scalable, and resilient data center. Fig. 3 shows the proposed layered secure network architecture for the data center.

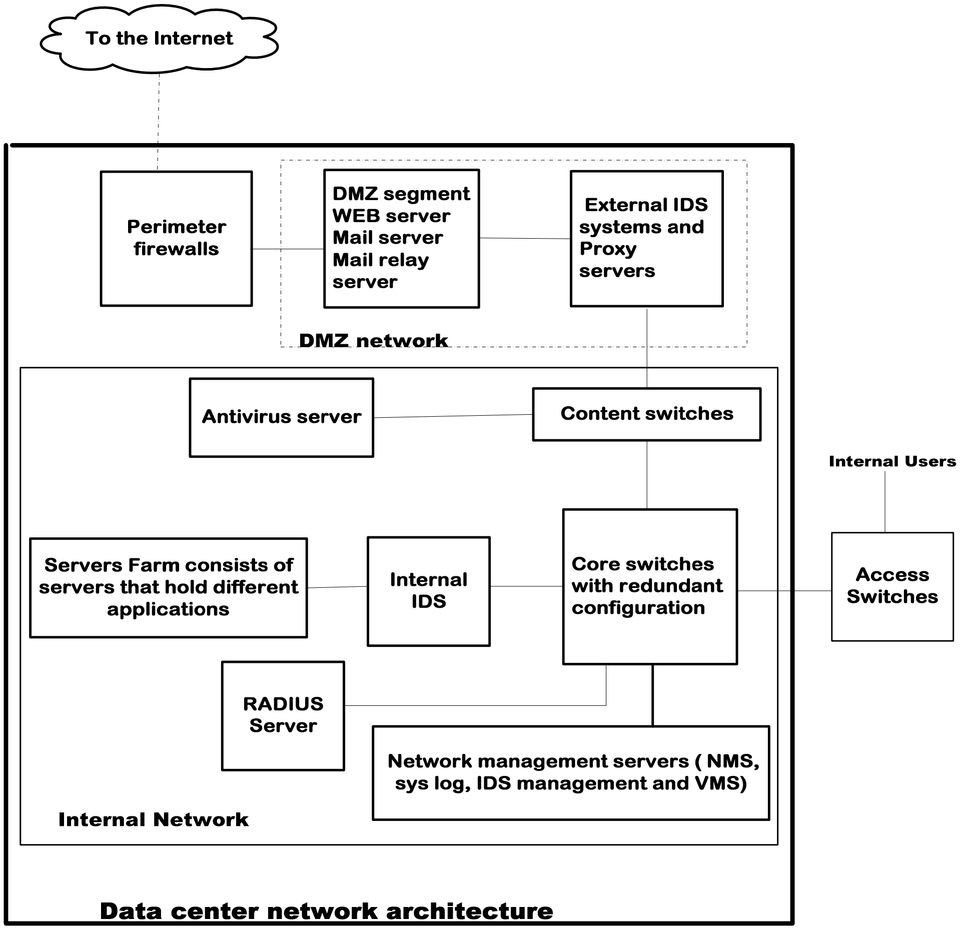
To the Internet
Perimeter firewalls
DMZ segment
WEB server
Mail server
Mail relay server
External IDS systems and Proxy servers
DMZ network
Antivirus server
Content switches
Internal Users
Servers Farm consists of servers that hold different applications
Internal IDS
Core switches with redundant configuration
Access Switches
RADIUS Server
Network management servers (NMS, sys log, IDS management and VMS)
Internal Network
Data center network architecture

Fig. 3. Layered security network architecture of a large scale data center

In the network design we have considered all the requirements of network security management. The design is based on layered security architecture; there are several lines of defense against any security threat (external or internal). In the following, we present shortly the components of the layered security architecture of the data center.

The data network architecture consists of hardware components and software components. The hardware components are: firewalls, Intrusion

Detection Systems, contents switches, access switches and core switches. The software components are: IPSec and VPN, antivirus software, network management systems and access control server.

The first line of defense is the **perimeter firewalls** that protect the internal network from any security risk coming from the outside network. There is a standby firewall that works in case of primary firewall failure.

The second line of defense is the **network IDS** (external and internal IDSs are network based IDSs not host based) that can detect any intruder activity not prevented by the firewalls or any unusual network activity. The perimeter firewalls and the external IDS together ensure that no direct connection can be made to the internal (protected) network.

The **proxy servers** are used by the internal users to access the Internet. Also they are used to filter out any unwanted Internet sites according to the enterprise security policy. Content switches can use up to the OSI layer 7 packets information. They are used for load balancing among groups of servers, firewalls and any other devices to improve utilization and availability. Proxy servers belong to the first and forth layers of defense.

The **core switches** play a very important role in this design; they are the heart of the network. We normally have two core switches; each core switch contains a routing part, a switching part and an internal firewall part. The switching part is used for connecting different servers and network devices together. The routing part main functionality is the routing between different VLANs; finally, the internal firewall is to protect the network from the internal security risks. The two core switches are connected to each other by fiber link to provide redundancy and failover; the Virtual Router Redundancy Protocol (VRRP) is used in case of a one core switch failure. The VRRP protocol establishes a redundant path between two routers in order to achieve default router failover if the primary router becomes inaccessible; then the traffic is routed to the other core switch without losing network connectivity.

For redundancy, there is more than one connection between any two network devices, with Spanning Tree Protocol enabled to prevent looping.

Each **access switch** is connected to the two core switches by different cables for redundancy, such that if one core switch is down then the access switch is connected to the other core switch.

Internal network users are connected to the access switches' ports that are assigned to their dedicated VLANs, to control their access to the internal network resources according to the Access Control Lists (ACLs) at the internal firewall.

VLANs are used to isolate network traffic between different networks (unless the traffic is allowed by the IT department security policy), prevent broadcasting and enhance security. There are several VLANs in this network:

- VLAN for computers in the internal network; all internal network computers can communicate within this VLAN;
- VLAN for each application server in the server's farm in the data center;
- VLAN for access switches; all access switches can communicate using this VLAN;
- VLAN for network devices (core switches, IDS and content switches); this VLAN is used for communication between the core switches;
- VLAN for the DMZ segment. WEB server, Email server, DNS server and email relay server belong to this VLAN.

IPSec and VPN can be configured at the firewalls to connect the internal network to any external network. Encryption (e.g. 3DES) that is used for VPN can be configured in the perimeter firewall. IPSec and VPN belong to the fifth layer of defense.

The antivirus server holds the antivirus software that is used to mitigate viruses, worms and Trojans. Antivirus sever belongs to the first and third layers of defense.

The RADIUS server is a very important component. It is used to control access to the network resources and devices using user credentials (Username and Password). These credentials are stored at the RADIUS server to provide authentication, authorization and accounting. RADIUS belongs to the second, third and fifth layers of defense.

The Network Management Server (NMS) is used to manage network components such as those based on SNMP. NMS is also used to monitor network-attached devices for conditions that need an administrative attention.

The system logging (syslog) server is used to store log messages coming from all network devices and servers into a centralized location.

The Virtual Memory System (VMS) is a multi-user, multiprocessing virtual memory-based operating system designed for transaction processing. It offers high system availability through clustering, or the ability to distribute the system over multiple physical machines. For example, for servers that hold the same application, VMS can be used to balance the load between these servers

The IDS management server is used to store all the alert messages and alarms coming from IDS (either internal or external), to alert the IT staff for any malicious activities coming from the internal or external networks.

7. Conclusions

The data center security guidelines discussed in this paper and applied in the design of our data center network architecture are conceived to achieve the best possible security. Although each security recommendation should be implemented if possible, each network has its own requirements such as cost of implementing security technologies and the application requirements that may limit the full implementation of these recommendations.

We followed the hierarchical network security model which is essential for achieving high data centre availability. In a hierarchical design, the capacity, features, and functionality of a specific device are optimized for its position in the network and the role that it plays. This promotes scalability and stability. The large scale network can take advantage of the design principles and implementation described in this paper to implement a network that will provide the optimal performance and flexibility.

In this paper we investigated some of the security threats that impact any data center network. Security considerations for the large scale data center are dependent on the network security policies. It is important to identify and understand these security considerations before designing any large scale data center.

Network security management has played a very important role in our design of network architecture. The proposed data center network architecture ensures the maximum security for the sensitive data of a large network. The design integrates different security technologies such as using high redundant core switches with internal firewall and IDS, external firewall for packet filtering and network access control from the outside networks, network IDS to detect any malicious network activities, segmenting the network into different segments (VLANs) for different applications and network devices, content switches for load balancing between proxy servers and the WEB server and protecting the servers' farm by the internal IDS and internal firewall.

A tradeoff between the security and cost should be made for this design of a large scale data center. For smaller networks, some of the components such as the content switches and one of the core switches can be eliminated to reduce the cost.

Table of abbreviations

AAA	Authentication, Authorization accounting
ACL	Access Control List
ARP	Address Resolution Protocol
CAM	Content Addressable Memory
DMZ	Demilitarized Zone

DoS	Denial of Service
EAP	Extensible Authentication Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	Internet Protocol Security
MAC	Medium Access Control
MITM	Man In The Middle
NMS	Network Management system
OS	Operating System
OSI	Open system Interconnect
QoS	Quality of Service
RADIUS	Remote Authentication Dial-in User Service
SNMP	Simple Network Management Protocol
SSH	Secure Socket Shell
SSL	Secure Socket Layer
TACACS	Terminal Access Controller Access Control System
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VMS	Virtual Memory System
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

REFERENCES

[1] SANS Institute, "IP Security Protocol-based VPNs " ,2001, URL: http://www.sans.org/rr/white papers /protocols/372.php

[2] *Mohammad Haidari*,"IPV6 Security considerations",June 2004, URL:http://www.Securitydocs.com/ library/2757

[3] *Mitchell Rowton*," Introduction to Network Security - Intrusion Detection", February 2005, URL: http:// www.securitydocs.com/library/3009

[4] *Mathew Tanase*, " IP Spoofing: An Introduction", March 2003, URL: http://www .secuirtyfocus .com focus/1674

[5] Data Center: Infrastructure Architecture SRND, URL: http://www.cisco.com/application/ pdf /en /us /guest/netsol/ns304/c649/cdccont_0900aecd800e4d2e.pdf

[6] Data Center: Securing Server Farms , URL: ww.cisco.com/application/pdf/en/us/ guest/ netsol/ ns304/c649/ccmigration_09186a008014edf3.pdf

[7] Data Center Security Topologies: www.cisco.com/application/pdf/en/ us/ guest/netsol/ns376 /c649/cdccont_0900aecd800ebd1d.pdf

[8] SANS Institute, "The Twenty Most Critical Internet Security Vulnerabilities", October 2004, URL: http: // www.sans.org/top20/top20.pdf

[9] The Information Workers' Security Handbook, January 2005, URL: http://www_.secinf.net/network _Security/Information-Workers-Security-Handbook.html

[10] *John V. Harrison*," A protocol Layer Survey for Network security", November 2004, URL: http://www.acm.org/hlb/publications/aic/aic1028.html#3#3

[11] *Matthew Strebe* " Network Security JumpStart: Computer and Network Security Basics", 2002, Skybox, ISBN: 078214120X

[12] "Internet and Intranet Security" Second edition, 2002, Artech House, 2001 ISBN: 1580531660

[13] *John E. Canavan* , "Fundamentals of Network Security", Artech House,2001,ISBN-13: 978-1580531 764

[14] Data centre services, URL, http://www.sun.com/service/storage/datacenterdatasheet.pdf

[15] Practical Large-Scale Network Design With Variable Costs for Links and Switches, URL: http://whitepapers.silicon.com/0,39024759,60304468p,00.htm

[16] *Mitchell Ashley* "LAYERED NETWORK SECURITY 2006: A best-practices approach", URL: http: //www.stillsecure.com/docs/StillSecure_LayeredSecurity.pdf.

[17] Juniper networks layered security solution, URL: http: http://cn.juniper.net/solutions /literature /white _papers/2005.pdf.