IA 5010
Alexander Semaan

Enterprise Network Architecture Paper

Part 1

1. Network Diagram

Attached as visio file.

2. Diagram Description

The network architecture utilized for Farm-Vacations' web app hosting is very carefully designed to maximize efficiency and security. The network was dissected into 7 zones, as advised by the SANS Institute:

- Internet Zone: It is quite simply used to symbolize the internet; all web server requests come from this zone, as well as the B2B VPN connection from Farm-Vacations' team.
- External DMZ: This zone contains all servers that users from the internet zone need to directly access; this includes the IIS Web Servers, DNS Server, Inventory Management Server, RDP Server, as well as FTP Server and Mail Server (that were added although not required, because they are definitely needed for good service to Farm-Vacations' team).
- Restricted Zone: It contains all the Databases (SQL 2016 DB) and sensitive information.
- Enterprise Zone: It contains Connected Network's web server and application server maintenance team. Using company computers, this team can modify and update the website and all three tiers of the website deployment that will be discussed later.
- Extranet Zone: It contains Farm-Vacations' team that VPNs into the network from their offices elsewhere (crossing through the internet) in order to use an inventory management portal, using company computers.
- Internal DMZ: This zone segregates less secure zones from the Restricted Zone where all the data is stored in order to increase security through proper tiering; this zone includes the Application Server and the Authentication Server.

- Management Zone: This is one of the most important zones and the one in need of the highest security, besides the Restricted Zone. It contains all the system logs gathered from all the systems and components on the network, and it is where the security and admin team analyze and review logs. Additionally, this zone is used to manage and configure all the networking and security components on the network, including firewalls and IDS/IPS.

3. Systems and Components Description

First, the use of the different servers will be analyzed. In order to provide Farm-Vacations with a proper website infrastructure, the use of 3-tiered website deployment was invoked. In tier 1, we have 3 IIS Web Servers integrated with a load balancer to manage high-traffic or to act as minor protection against DoS attacks. Once a user accesses the web servers, any actions and commands that require invoking the database, go through the Application Server that is in tier 2, that in turn gets or manipulates the required information from the SQL Database Server 2016, which is considered as tier 3.

On another note, the DNS server's job is pretty straightforward in terms of resolving the URL "www.farmvacations.com" to the IP 54.168.122.129.

The Inventory Management Server is used by Farm-Vacations' team, that logs in to the inventory management portal using credentials. Access to this server is uniquely granted to the Farm-Vacations' offices, and the credentials are authenticated by the Authentication Server, which in turn grants the Inventory Management Server access to the SQL Database.

Per the requirements, the Connected Network's team in charge of maintaining and updating the website needs to Remote-in to the IIS Web Servers and the Application Server. To do that efficiently and in a well monitored fashion enhancing security, an RDP Server, with authentication and redirecting abilities, is deployed and placed in the External DMZ. In return, an RDP client process must be running on the IIS Web Servers and the Application Server, with proper firewall configurations.

Even though not mentioned in the requirements, an IMAP Mail Server and an FTP server were added for convenience, customer support, file-sharing and communication.

Regarding the integration of Farm-Vacations' offices and team, a TLS Full Tunnel VPN was designed for the Business-to-Business connection over the internet. TLS was chosen instead of IPSec because it has slightly better security in this case, especially since IPSec only uses datagrams, whereas TLS uses TCP sessions over port 443, which was a requirement.

For log management, a Compartmentalized Log Management Architecture was deployed using a 3-tier system; logs from every Network Zone were separately collected for better management and analysis. All logs from each zone (tier 1) go through a load balancer before being stored in two log collectors per zone (tier 2). The stored logs are then analyzed and monitored by Connected Network's security and admin team (tier 3). This all belongs to the Management Zone, which also collects logs of itself. For management and configuration purposes, an IDS/IPS admin and a Firewall admin have access to the IDS/IPS and Firewalls respectively; they reside in the Management Zone as well.

Firewalls, IPSs and IDSs were deployed as well, but these will be detailed in further steps.

4. Network Subnets Description

The Network was subnetted in a rather straightforward manner, using IPv4 addressing scheme. Subnets were formed after analyzing the needs of each zone in terms of number of devices connected. Each Zone has its separate set of IPs:

- 10.24.10.0/24 was divided into three subnets for each of the following zones: 10.24.10.0/28 for the External DMZ (up to 14 devices on the subnet), 10.24.10.16/29 for the Internal DMZ (up to 6 devices on the subnet), 10.24.10.24/29 for the Restricted Zone (up to 6 devices on the subnet).

- 10.54.90.0/24 was not divided but was limited to the use of 6 devices (10.54.90.0/29) since not more are needed right now (could be increased if the Farm-Vacations team increases over 6 users)
- 10.10.10.0/24 was divided into two to satisfy the needs of each zone: 10.10.10.0/27 for the Management Zone since it doesn't have over 30 devices and 10.10.10.32/29 for the Enterprise Zone since it doesn't need more than 6 devices right now.

5. Firewall Rules and Policies

(The configurations covered are for the firewalls that are required, not the ones added, in order to meet length requirements)

First-Line Firewall – This firewall is the first line of defense facing the Internet Zone and should have carefully administered rules.

Rule	Type	Source Address	Destination Address	Port	Action
1	TCP	*	10.24.10.3	443	Allow
2	TCP	10.24.10.3	*	443	Allow
3	TCP	10.10.10.0/27	(This firewall's IP)	22	Allow
4	TCP	(This firewall's IP)	10.10.10.0/27	22	Allow
5	*	*	10.24.10.4	53	Allow
6	*	10.24.10.4	*	53	Allow
7	TCP	*	10.0.0.0/8	*	Deny
8	UDP	*	10.0.0.0/8	*	Deny

Inventory Management Firewall

Rule	Type	Source Address	Destination Address	Port	Action
1	TCP	10.54.90.*	10.24.10.7	443	Allow
2	TCP	10.24.10.7	10.54.90.*	443	Allow
3	UDP	10.24.10.7	10.10.10.0/27	514	Allow
4	TCP	10.10.10.0/27	(This firewall's IP)	22	Allow
	TCP	(This firewall's IP)	10.10.10.0/27	22	Allow
5	TCP	*	10.0.0.0/8	*	Deny
6	UDP	*	10.0.0.0/8	*	Deny

These were two examples of how the firewall rules and policies should look like for proper control.

In general, all firewalls must allow access on port 22 to and from subnet 10.10.10.0/27 belonging to Management Zone.

RDP firewall, IIS Web firewall and Application firewall must allow subsequent traffic on port 3389 for subnet 10.10.10.0/27.

Restricted Zone firewall and Application firewall must allow subsequent traffic on ports 1433 for IPs 10.24.10.18 (App server), 10.24.10.26 (DB1) and 10.24.10.27 (DB2).

Management firewall must accept subsequent traffic on port 22 from its subnet 10.10.10.0/27 to all firewall IPs in the network, as well as incoming traffic on port 514 from 10.0.0.0/8 to 10.10.10.0/7 for log management.

Part 2

1. **Security Controls Implemented**

The most notable security control that was integrated in this network, was the redundant use of Firewalls to maximize security and access control. By adding a firewall after each server, it extremely mitigates the likelihood that an infected server can access other resources on the network freely, and it maximizes assurance to the system.

Adding an RDP Server was done to increase security, since it allows more precise and efficient monitoring of access requiring an RDP connection (done by Connected Network's team).

Again, as extra security measure, an Authentication Server was added to verify login credentials and other secure connections like the inventory management portal used by Farm-Vacations' team.

A Compartmentalized Log Management Architecture was deployed to increase security over a regular Baseline Log Management Architecture, because it splits log management in a more efficient manner, by zone.

Next, IDS and IPS sensors were deployed to further increase security and to better monitor and prevent attacks on the network where required. The hard part is knowing how and where to deploy

IPS sensors specifically, because as good a tool as they might seem to be, they can work against the network. In fact, a lot of false positives tend to happen, and some legitimate traffic can be blocked and some essential processes and services can be blocked, that could result in down-times, tarnishing the website's reputation. Additionally, IPS sensors can considerably increase latency which could impact services that are sensitive to response-time. Hence, Host-Based and Network-Based IDS sensors were deployed for two zones: External DMZ, Internal DMZ and Internet Zone. These areas are more risk tolerant areas in the network, where a lot of traffic passes through. In the other zones that have access to highly sensitive areas of the network, IPS sensors were deployed, notably in the Restricted Zone, Enterprise Zone, Extranet Zone and Management Zone.

2. **Additional threats and mitigation**

   Some weaknesses that are seen in the system are mostly along the lines of backing up the systems, servers and databases that are deployed. For the SQL Database Server, it is advised implement a RAID 10 Server to store the website's data. As for the servers, it is advised to have at least one backup server for each running server, that would be on standby in case one of the servers fails.

References

- Northeastern University IA 5010 Week 8 Course Slides.
- Obregon, Luciana. *Infrastructure Security Architecture for Effective Security Monitoring.* Sans Institute Information Security Reading Room.