Short Paper:

Enterprise Network Architecture

Sonam Ghatode

Foundation of Information Assurance (CY5010)

October 31, 2019

Abstract

Asset evaluation is a tedious and time taking task, the reason why many organizations stick to uniformity i.e. treat each asset equally, and hence increasing cost of architecture. A better approach to design a network is to divide the assets into categories or tiers and then implement the security measures needed for a tier to be secure. A web server which serves pages is not as valuable as a database server, which stores the financial information of customers. Therefore, a tiered architecture will ensure proper security measures are implemented for each tier and make auditing more focused.

Introduction

Building a network architecture that provides Confidentiality, Integrity, and Availability is a task that every enterprise should do keenly. But to build a network architecture, the asset evaluation has to be done to identify the value of each asset in the organization. In this paper, a network architecture for a website is depicted. A website for ”Farm-vacations” client is to be deployed by the Connected Networks firm. The network architecture required for the deployment of the website is explained with diagram in the paper.

Solution for Requirement 1

The architecture is divided into 5-tiers namely: Internet, External DMZ(De-Militarized Zone), Enterprise Zone or Internal DMZ, Management Zone, Restricted Zone.[1] The security features implemented in each tier is dependent on the value of assets the tier has and com-

[1] **Infrastructure Security Architecture for Effective Security Monitoring**; **by Luciana Obregon**.

munication between layers is allowed based on trust level. The trust level for Internet and Web server is low and hence they cannot directly communicate to the Restricted zone or management zone with the highest trust. The Web Server has to go through the application server to reach the Database Server located in Highest Trust Zone.

The customers request the URL *"www.farmvacations.com"* and the request is transferred to DNS server of Connected Networks, which resolves the IP of the URL to 54.168.122.129. Since the request include the authentication data, the communication is encrypted. Before request can reach the web server located at 54.168.122.129, an external firewall is placed to check the traffic, and block the known exploiters from entering the network. Once request reaches the web server, the web server transfers the request to port 443 of the Application Server. This communication is encrypted since it is outside internal network, and hence insecure. Before request can reach Application, a firewall is placed to check the incoming traffic and block requests that tries to access port other than 443. Other function that is implemented here is Network Address Translation(NAT), which replaces the destination address(public IP: 54.168.122.129) with private IP 10.24.10.0/24 and creates an entry in Translation table. If the request is made on other port than 443, the request is denied. The rule that is implemented in *Firewall 1*, depicted in Figure 1, is that allow incoming requests on port 443 on https and deny all other requests. This ensures that the incoming request cannot access other ports.

Once Application Server gets the request, authentication of the user is done, if the user is authorized, the request is processed further. If the user has requested the profile information or financial information, the requested is forwarded to port 1433 of the database server. A firewall is placed before request reach the database server with a rule to deny all requests that are on other ports than 1433. The Application Server is placed in the Internal DMZ and the Database Server is placed in the Restricted Zone.

A secondary application server is also placed in the Internal DMZ to provide higher availability. This server will remain on standby mode until primary application server is down. If primary application server is down, the requests will be forwarded to the secondary application server.

The reason for separating the Application Server and Database Server is that the internal communication is not encrypted and can be prone to insider threat and even outsider threat. To protect the user data stored in the database server, database server is placed behind yet another firewall to increase the security.

Once the database server receives the request, it transfers the request to the requested type database and process the data to send the response back. Here the firewalls not only monitors the incoming traffic, but outside traffic as well. The databases are categorized to provide the least privilege needed to carry out the operation requested.

The Management Zone consists of the systems used by the administration people to monitor the system and keep the systems updated.

Solution for Requirement 2

To monitor the website and keep it secure, logging of the traffic, be it incoming or outgoing, and Intrusion Detection System is necessary. In the architecture explained above, network tap, IDS sensor, and zone's core switch are added to each tier inside internal network.

The reason for choosing the network tap instead of SPAN tap is that the SPAN tap is prone to packet loss. To provide service reliably, the network tap works more efficiently than

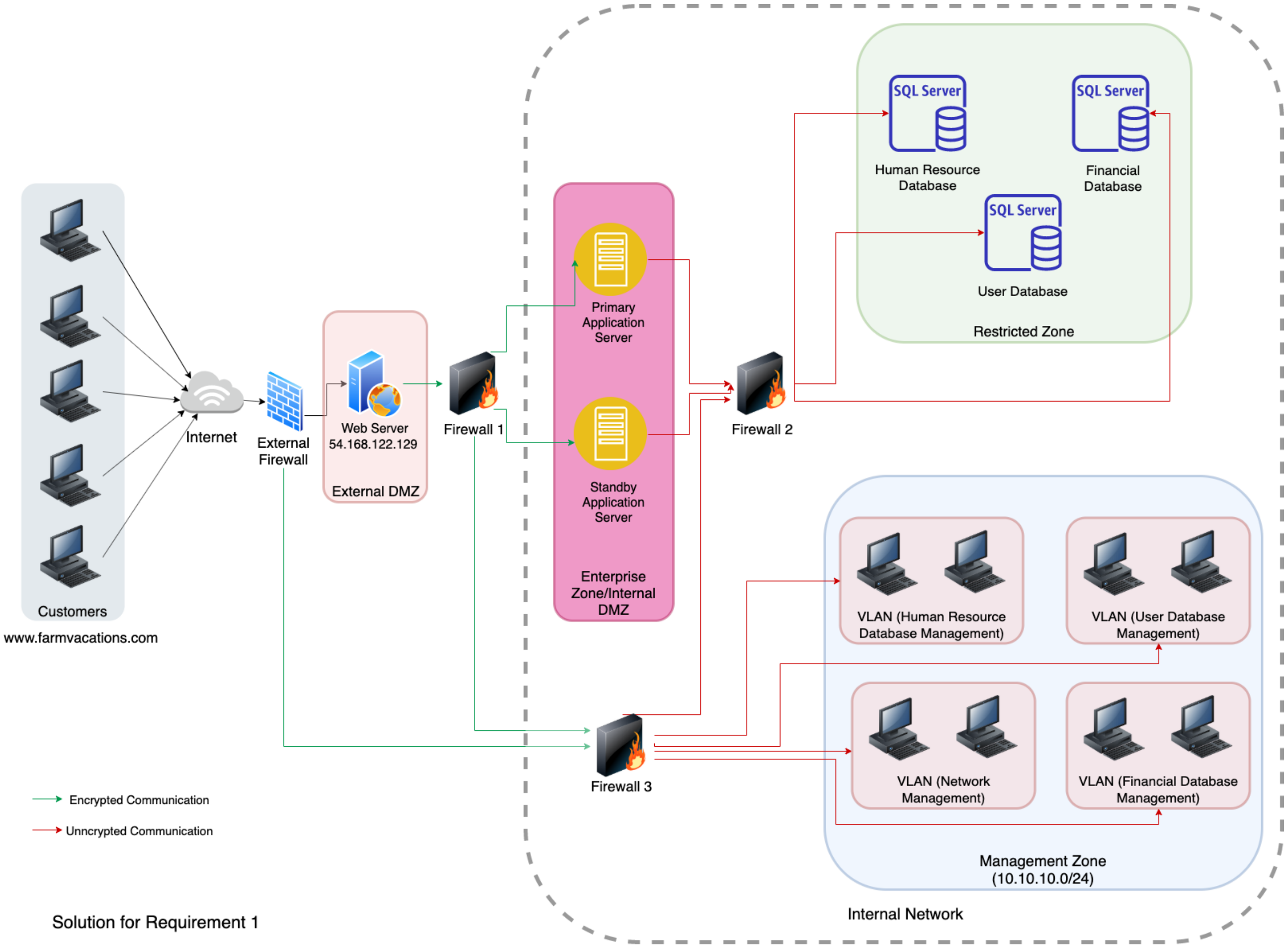

Figure 1: Network Architecture for Requirement 1

the SPAN tap. An IDS sensor is connected to the network TAP to monitor the dropped packets, increase visibility, and provide flexibility to add additional monitoring tools to watch the same type of traffic.

Once the request first reaches external firewall, the logging of the traffic starts. External firewall, *Firewall 1*, and *Firewall 2* sends the traffic log to management servers using UDP over port 514 of *Firewall 3*. *Firewall 3* is configured to drop the traffic which come on port other than UDP port 514 and RDP on port 3389. The *Firewall 3* is accessed by the management(administration) people over port 22.

The Management Zone is divided into four VLANs to provide minimal privilege needed to monitor a type of database. A person monitoring the Financial log cannot access HR database log. This segmentation is useful while an attacker passes through all the firewalls, he would not be able to access other databases than the one he got access to.

The encrypted web server logs are sent to management zone using RDP on port 3389 because again, the web server is outside internal network, so need encryption to avoid sniffing. The configuration of firewall drops other traffic. The restricted zone logs are sent by the IDS directly to the Log Management Server which is located on IP 10.10.10.0/24.

The advantage of dividing a network into tier is that the logs are separate for each tier. The logs of the internal firewalls are important than the logs of external firewalls. The size data leaving a zone should also be monitored to check for the possible exploitation.

The threats in this network architecture is that the internal communications are not encrypted and is prone to insider threat. This can be eliminated by encrypting internal communication as well, but cost and performance overhead will increase subsequently because

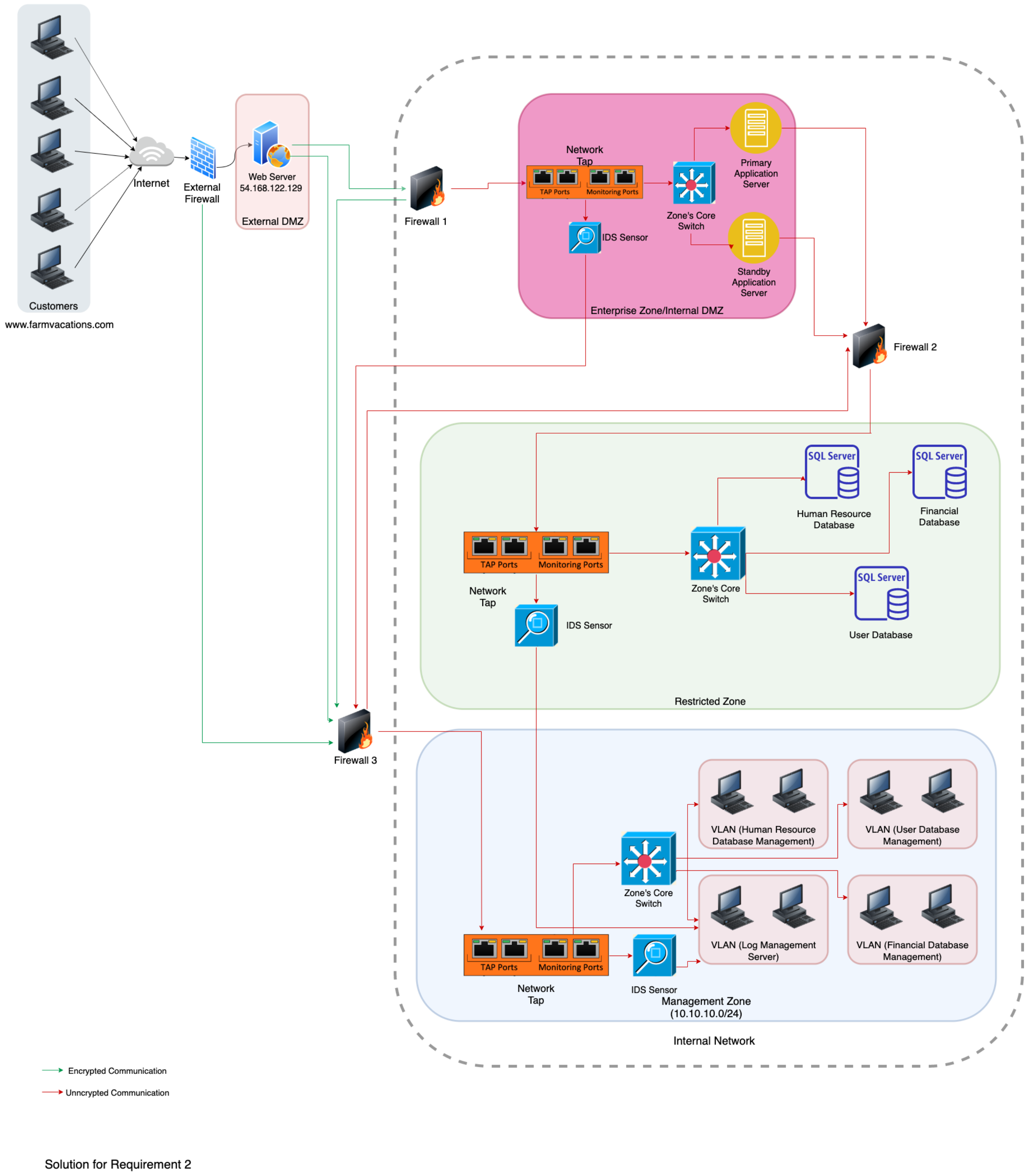

Figure 2: Network Architecture for Requirement 2

of this. Other vulnerability is the usage of UDP to send logs, which can be exploited easily because of the inherent security problems associated with UDP.

Concluding Remarks

The architecture depicted in this paper gives a possible solution to create a secure network architecture for a website deployment, but is still prone to the attack because of the inherent risk in the protocols or insider threats. However, it explains the necessary security mechanisms to be implemented.