**Network Security Consultant**

**Problem Statement:**

You are working as a network security consultant for El Banco Bank. Your primary responsibility is to secure the bank's assets by designing, integrating, and implementing complex network architecture solutions after reviewing the network security.

You should be able to troubleshoot very complex network issues spanning various types of technologies.

**Background of the problem statement:**

El Banco Bank is one of the fastest-growing banks in Europe with more than 1200 branches across the country and manages €200 billion in assets.

Handling millions of dollars of banking transactions per day, its customers hugely depend upon the security of their banking data. The recent surge in cyber-attacks and data breaches has become a significant issue for every organization.

**Expected Deliverables:**

**TASK 1:**

As a network security consultant, you have to review tickets raised by users due to digital certificate issues. To help them resolve these issues, you need to understand the organization's certificate information. Identify the likely issue and the possible solution for the following tickets:

**Ticket 1:**

Date: 10/11/2021

Submitted by: Bob Wood (Pen tester)

I am trying to browse this website using an IP address, but my browser displays a certificate error. What should I do?

Graphical user interface, text, application, email

Description automatically generated

**Possible Issue:** There can be multiple reason you are encountering this issues like.

* There’s an invalid SSL certificate installed on server.
* Website is using self-signed SSL certificate which is cost effective but browsers being unable to authenticate its legitimacy.
* SSL certificate has been expired.
* The certificate is from a trusted source..

**Solution :**

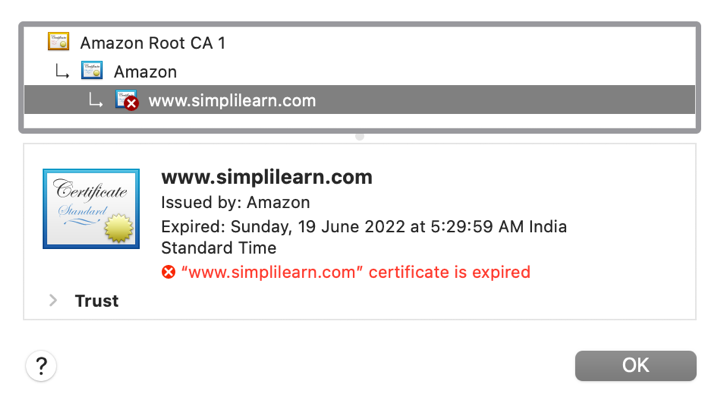
* Use a valid SSL certificate.
* Use certificate from trusted source .
* Re-new the certificate in case of expired certificate.

**Ticket 2:**

Date: 1/10/2021

Submitted By: Sheila Shaz (System Administrator)

I am trying to browse this website, but my browser displays an error that the certificate is expired. We have just renewed the certificate, and I am certain that the certificate will only expire in June 2022. What could be the reason for this error?



**Issue :** The date and time of PC are not in **sync** with the server.

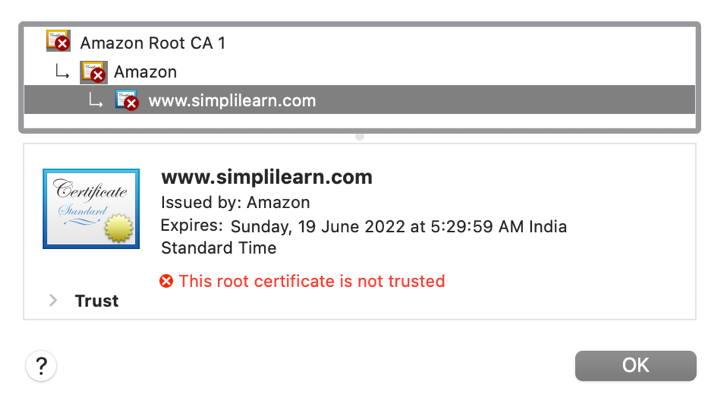
**Solution :** Check your PC’s date and time and correct it as it has wrong date or time.

**Ticket 3:**

Date: 2/12/2021

Submitted By: James Clay (Software Developer)

I am trying to browse this website, but my browser displays an error that the root certificate is not trusted. Is this issue client related?



Client Machine Root Certificates

Table

Description automatically generated

**Issue:** Yes this is a client related issue. This error suggests that you browser does not recognize or trust the root certificate authority (CA) associated with the SSL certificate used by the website you are trying to access.

**Solution:**

* Check date and time setting.
* Check browser update.
* Check system update.
* Try different browser.

**TASK 2:**

You are reviewing the inbound rules of a VM in the cloud. The VM is used to host the bank’s website. For additional security, a valid digital certificate has been configured.

The cloud administrator is authorized to access the VM using RDP and SSH connections, but access should only be allowed from the authorized system with a fixed public IP (18.66.78.112).

Add the appropriate Inbound rules in the given format.

**Note:**

1. Use 0.0.0.0/0 to indicate anywhere (IPv4).
2. Sub-net mask /32 indicates only one host whereas /0 indicates all the hosts in the network.

**Solution:** To ensure the security of the VM that is hosting the bank's website, the following inbound rules should be configured.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** |
| **RDP** | **TCP** | **3389** | **18.66.78.112** |
| **SSH** | **TCP** | **22** | **18.66.78.112** |

The rules mentioned in the table will make sure that Remote Desktop Protocol (RDP) traffic on port 3389 and Secure Shell (SSH) traffic on port 22 should only be allowed from the authorized system with the fixed public IP address 18.66.78.112. This ensures that only authorized administrators with access from the specified IP address can remotely access the VM for management purposes preserving the integrity of the system.

**TASK 3:**

As a network security consultant, you are designing the VPN connectivity requirements so that users working remotely from home can access the corporate network. The business has provided the following connectivity requirements:

**VPN Connection 1:**

This VPN will be used by software developers working on Ubuntu 20.04 from home to connect only to the main software repository server in the enterprise network. Use an open-source VPN protocol that is designed for speed. Configure all the network traffic to go through the enterprise network.

**VPN Connection 2:**

This VPN will be used by remote users working on Windows 10 from home to connect to the enterprise network. Use a Microsoft proprietary VPN protocol for ease of configuration. Users should be able to watch Netflix directly without connecting through the enterprise network, which would otherwise block this kind of traffic.

Diagram

Description automatically generated

For these VPN connections, you will need to perform the following:

1. Determine the VPN types, VPN protocols, and the tunnel methods
2. Select the Firewall ports to allow
3. Both VPN connections must support strong 256-bit encryption and use the SSL/TLS for key exchange

**Solution:**

**For VPN Connection1:**

VPN Connection 1 (Software Developers):

1. VPN Type: Remote Access VPN (Connects individual users to the corporate network)

VPN Protocol: OpenVPN,

Tunnel Method: User Datagram Protocol (UDP) (Offers better performance compared to TCP for OpenVPN)

1. Firewall Ports: Allow incoming connection on UDP port 1194 (default OpenVPN port)
2. Encryption: AES-256 (256-bit) with SHA-256 hashing for strong encryption and integrity. Key Exchange: Use TLS 1.3 for secure key exchange

**For VPN Connection2:**

VPN Connection 2 (Remote Users):

* + - 1. VPN Type: Remote Access VPN

VPN Protocol: L2TP/IPsec (More secure than PPTP but slightly more complex)

Tunnel Method: L2TP/IPsec: L2TP encapsulates user data, and IPsec encrypts and authenticates the data within the L2TP tunnel.

* + - 1. Firewall Ports: L2TP/IPsec: Allow incoming connections on UDP port 500 (IKEv2) and ESP (Encapsulating Security Payload) port (dynamically assigned by the server)
      2. Encryption: AES-256 (256-bit) with SHA-256 hashing for both options

Key Exchange: Use TLS 1.3 for secure key exchange