**CAPSTONE 3 Network Security Consultant**

**Done by: Sanjana Inchalmath**

**Ticket 1**

**Issue:**

* The user is trying to access a website using its IP address, and the browser displays a certificate error.

**Likely Cause:**

* SSL/TLS certificates are domain-specific and do not validate IP addresses unless explicitly configured to do so. The certificate’s Common Name (CN) or Subject Alternative Name (SAN) does not match the IP address.

**Solution:**

* Advise the user to access the website using its domain name rather than the IP address.
* If IP address access is required, ensure the SSL certificate includes the IP address in its SAN field during the certificate generation.

**Ticket 2**

**Issue:**

* The user’s browser shows a certificate expiration error, although the certificate has been recently renewed and is valid until June 2022.

**Likely Cause:**

1. The server might still be using the old, expired certificate due to misconfiguration.
2. Browser cache may still hold the details of the expired certificate.

**Solution:**

* Restart the web server to ensure it uses the updated certificate.
* Clear the browser’s cache and SSL state to remove outdated certificate information.
* Verify the certificate chain using online tools or OpenSSL to ensure proper configuration.

**Ticket 3**

**Issue:**

* The browser displays an error that the root certificate is not trusted.

**Likely Cause:**

* The root certificate authority (CA) that issued the server’s certificate is not included in the client’s trusted root CA store.

**Solution:**

* Confirm if the certificate was issued by a public or private CA.
  + If private: Ensure the organization’s root CA is installed in the client’s trusted root certificate store.
  + If public: Update the client’s operating system or browser to obtain the latest root certificates.
* Use a publicly trusted CA to avoid compatibility issues.

**Task 2: Inbound Rules for Cloud VM**

**Requirements:**

* Allow only the cloud administrator to access the VM via RDP and SSH from a fixed public IP.
* Configure the following rules:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** |
| SSH | TCP | 22 | 18.66.78.112/32 |
| RDP | TCP | 3389 | 18.66.78.112/32 |
| HTTPS | TCP | 443 | 0.0.0.0/0 |
| HTTP | TCP | 80 | 0.0.0.0/0 |

**Explanation:**

* SSH (port 22) and RDP (port 3389) are restricted to the administrator’s IP address for secure access.
* HTTP and HTTPS traffic is open to all (0.0.0.0/0) to allow public access to the website.

**Task 3: VPN Connectivity Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **OS** | **VPN Type** | **VPN Protocol** | **Tunnel Method** | **Firewall Port** |
| Ubuntu 20.04 | Remote Access VPN | WireGuard | Full tunnel | UDP port 51820 |
| Windows 10 | Split Tunnel VPN | SSTP | Split tunnel | TCP port 443 |

**VPN Connection 1 (For Software Developers):**

**Requirements:**

* Ubuntu 20.04 users accessing the main software repository.
* Use an open-source VPN protocol focused on speed.
* Route all traffic through the enterprise network.

**Solution:**

* **VPN Type:** Remote Access VPN.
* **Protocol:** WireGuard (open-source and optimized for speed).
* **Tunnel Method:** Full tunnel (routes all traffic through the enterprise network).
* **Firewall Ports:**
  + UDP port 51820 for WireGuard traffic.
* **Encryption:** Use AES-256 encryption with SSL/TLS for key exchange.

**VPN Connection 2 (For Remote Windows Users):**

**Requirements:**

* Windows 10 users accessing the enterprise network.
* Use a Microsoft proprietary VPN protocol.
* Allow Netflix and similar traffic to bypass the VPN.

**Solution:**

* **VPN Type:** Split Tunnel VPN.
* **Protocol:** SSTP (Secure Socket Tunneling Protocol).
* **Tunnel Method:** Split tunnel (only enterprise traffic goes through the VPN; other traffic bypasses).
* **Firewall Ports:**
  + TCP port 443 for SSTP traffic.
* **Encryption:** Use AES-256 encryption with SSL/TLS for key exchange.