Q1..

Install iptables:
CentOS 7 uses firewalld as the default firewall management tool. To switch to iptables, we need to disable and remove firewalld:

```
systemctl stop firewalld
systemctl disable firewalld
yum remove firewalld
```

- Install iptables using the following command:

```
yum install iptables-services
```

- Enable iptables to start on system boot:

```
systemctl enable iptables
```

Configure firewall rules using iptables:
- Start by flushing existing iptables rules:

```
iptables -F
iptables -X
iptables -Z
```

- Set the default policy to deny all incoming connections and allow all outgoing connections:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

(a) Allow incoming RDP traffic from the IP address 196.1.113.4 only:

```
iptables -A INPUT -p tcp --dport 3389 -s 196.1.113.4 -j ACCEPT
iptables -A INPUT -p tcp --dport 3389 -j DROP
```

(b) Allow incoming HTTP (port 80) and HTTPS (port 443) traffic for your website:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

(c) Log packets directed to port 3389 (RDP):

```
iptables -A INPUT -p tcp --dport 3389 -j LOG --log-prefix "log Packet: "
```

- Save the iptables rules to persist across reboots:

```
service iptables save
```

Test the configuration:
- Restart the iptables service to apply the new rules:

```
systemctl restart iptables
```