**1. Firewalls**

* Firewalls are resistant to network attacks.
* They are the only transit point for internal and external network traffic.
* Enforce access control policies to filter data flow.

**2. Types of Firewalls**

**2.1 Packet Filtering (Stateless) Firewalls**

* Use Layer 3 and 4 criteria for filtering (source/destination IP address, ports, protocols).
* **Benefits**:
  + Simple rules and low network performance impact.
  + Provides basic network-layer security.
* **Limitations**:
  + Vulnerable to IP spoofing.
  + Cannot dynamically filter services.
  + Stateless and relies on ACLs.

**2.2 Stateful Firewalls**

* Track individual sessions using a state table and monitor TCP connections.
* **Benefits**:
  + Strong defense against spoofing/DoS.
  + Improved session tracking and data logging.
* **Limitations**:
  + No Layer 7 inspection.
  + Limited ability to handle dynamic ports.

**2.3 Application Gateway (Proxy) Firewalls**

* Operates across Layers 3, 4, 5, and 7.
* Proxy servers hide client IP addresses for secure remote connections.

**2.4 Next-Generation Firewalls**

* Combines stateful firewall features with intrusion prevention, application awareness, and advanced threat control.

**3. Common Security Architectures**

**3.1 Private/Public Zones**

* Public (untrusted) and Private (trusted) network segmentation.

**3.2 DMZ**

* A dedicated network for selectively accessible resources.

**3.3 Zone-Based Policy Firewalls (ZPF)**

* Uses zones to apply policies between network segments for greater flexibility.

**4. Layered Defense**

1. **Network Core**: Prevent malicious traffic anomalies.
2. **Perimeter**: Secure the boundary between zones.
3. **Communications**: Use encryption for privacy.
4. **Endpoints**: Ensure security policy compliance for devices.

**Extracted Packet Tracer Commands**

**1. Zone Creation Commands**

**Router(config)#** **zone security PRIVATE**

**Router(config-sec-zone)#** **exit**

**Router(config)#** **zone security PUBLIC**

**Router(config-sec-zone)#**  **exit**

**2. Class-Map: Identifying Traffic of Interest**

**Router(config)#** **class-map type inspect match-any Web-Traffic**

**Router(config-cmap)#** **match protocol http**

**Router(config-cmap)#** **match protocol https**

**Router(config-cmap)#** **match protocol dns**

**Router(config-cmap)#** **exit**

**3. Policy-Map: Defining Actions for Traffic**

**Router(config)#** **policy-map type inspect PRIV-PUB-POLICY**

**Router(config-pmap)#** **class type inspect Web-Traffic**

**Router(config-pmap-c)#**  **inspect**

**Router(config-pmap-c)#** **exit**

**4. Zone-Pair Configuration**

**Router(config)#** **zone-pair security Private-to-Public-Traffic source Private destination Public**

**Router(config-sec-zone-pair)#** **service-policy type inspect PRIV-PUB-POLICY**

**Router(config-sec-zone-pair)#** **exit**

**5. Interface Zone Assignments**

**Router(config)#** **interface GigabitEthernet0/0**

**Router(config-if)#**  **zone-member security Private**

**Router(config-if)#** **exit**

**Router(config)#** **interface GigabitEthernet0/1**

**Router(config-if)#** **zone-member security Public**

**Router(config-if)#**  **exit**

**6. Verification Commands**

**Router#** **show class-map type inspect**

**Router#** **show zone security**

**Router#** **show zone-pair security**

**Router#** **show policy-map type inspect**

**Router#** **show run | begin class-map**

**Router#** **show policy-map type inspect zone-pair sessions**

**AAA Configuration**

**1. Enable AAA Globally**

**Router(config)#** **aaa new-model**

**2. Specify the Server**

* **TACACS+:**

**Router(config)#** **tacacs-server host 192.168.1.101**

**Router(config)#** **tacacs-server key TACACS-Pa55w0rd**

* **RADIUS:**

**Router(config)#** **radius-server host 192.168.1.100**

**Router(config)#** **radius-server key RADIUS-Pa55w0rd**

**3. Configure Authentication**

* **TACACS+:**

**Router(config)#** **aaa authentication login default group** **tacacs+ local-case**

* **RADIUS:**

**Router(config)#** **aaa authentication login default group** **radius local-case**

**4. Fine-Tuning AAA**

* **Limit Failed Attempts:**

**Router(config)#** **aaa local authentication attempts max-fail 3**

**Router#** **clear aaa local user lockout**

* **Show AAA Users:**

**Router#** **show aaa user**

**Zone-Based Policy Firewall (ZPF) Configuration**

**1. Zone Creation**

**Router(config)#** **zone security PRIVATE**

**Router(config-sec-zone)#** **exit**

**Router(config)#**  **zone security PUBLIC**

**Router(config-sec-zone)#** **exit**

**2. Class-Map: Identifying Traffic of Interest**

**Router(config)#** **class-map type inspect match-any Web-Traffic**

**Router(config-cmap)#** **match protocol http**

**Router(config-cmap)#** **match protocol https**

**Router(config-cmap)#** **match protocol dns**

**Router(config-cmap)#** **exit**

**3. Policy-Map: Defining Actions for Traffic**

**Router(config)#** **policy-map type inspect PRIV-PUB-POLICY**

**Router(config-pmap)#** **class type inspect Web-Traffic**

**Router(config-pmap-c)#** **inspect**

**Router(config-pmap-c)# exit**

**4. Zone-Pair Configuration**

**Router(config)#** **zone-pair security Private-to-Public-Traffic** **source Private destination Public**

**Router(config-sec-zone-pair)#** **service-policy type inspect PRIV-PUB-POLICY**

**Router(config-sec-zone-pair)#** **exit**

**5. Interface Zone Assignments**

**Router(config)#** **interface GigabitEthernet0/0**

**Router(config-if)#** **zone-member security PRIVATE**

**Router(config-if)#** **exit**

**Router(config)#** **interface GigabitEthernet0/1**

**Router(config-if)#** **zone-member security PUBLIC**

**Router(config-if)#** **exit**

**6. Verification Commands**

**Router#** **show class-map type inspect**

**Router#** **show zone security**

**Router#** **show zone-pair security**

**Router#** **show policy-map type inspect**

**Router#** **show run | begin class-map**

**Router#** **show policy-map type inspect zone-pair** **sessions**

**Access Control Lists (ACLs)**

**1. Extended Numbered ACLs**

* **Block all IP traffic between two networks:**

**Router(config)#** **access-list 100 deny ip 10.0.0.0** **0.255.255.255 172.16.0.0 0.0.255.255**

* **Block only TCP traffic but allow others:**

**Router(config)#**  **access-list 100 deny tcp 10.0.0.0** **0.255.255.255 172.16.0.0 0.0.255.255**

**Router(config)#**  **access-list 100 permit ip any any**

* **Block only HTTP traffic:**

**Router(config)#**  **access-list 100 deny tcp 10.0.0.0** **0.255.255.255 172.16.0.0 0.0.255.255 eq 80**

**Router(config)#**  **access-list 100 permit ip any any**

**2. Named Extended ACLs**

* **Create and configure a named extended ACL:**

**Router(config)#**  **ip access-list extended FIREWALL**

**Router(config-ext-nacl)#**  **permit tcp any host 192.168.20.254 eq 80**

**Router(config-ext-nacl)#**  **permit tcp any any established**

**3. Securing SSH and Telnet Access**

* **Allow only specific hosts for SSH and Telnet:**

**Router(config)#**  **ip access-list extended VTY**

**Router(config-ext-nacl)#**  **permit tcp host 172.16.1.100 host** **192.168.2.1 eq 22**

**Router(config-ext-nacl)#**  **permit tcp host 172.16.1.100 host** **192.168.2.1 eq 23**

**Router(config-ext-nacl)#**  **deny tcp any any eq 22**

**Router(config-ext-nacl)#**  **deny tcp any any eq 23**

**Router(config-ext-nacl)#**  **permit ip any any**

* **Apply the ACL:**

**Router(config)#** **int g0/0/1**

**Router(config-if)#** **ip access-group VTY in**

**4. Mitigating ICMP Attacks**

* **Allow specific ICMP messages inbound:**

**Router(config)#** **access-list 112 permit icmp any any echo-reply**

**Router(config)#** **access-list 112 permit icmp any any source-quench**

**Router(config)#** **access-list 112 permit icmp any any unreachable**

**Router(config)#** **access-list 112 deny icmp any any**

**Router(config)#** **access-list 112 permit ip any any**

* **Allow ICMP messages outbound:**

**Router(config)#** **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo**

**Router(config)#** **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem**

**Router(config)#** **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big**

**Router(config)#** **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench**

**Router(config)#** **access-list 114 deny icmp any any**