

Perimeter Design & Implementation Issues

Ramandeep Singh
Project Leader, E-Secure
HCL Comnet

- **Lockdown Rule, also called as Stealth Rule**
- **Cleanup Rule**
- **Anti-Spoof Rules**
 - RFC 1918
 - RFC 2827 (optional)

- Always place the most frequently used rules in the top to bottom order in the policy
- Always place the lockdown rule in the top and the cleanup rule in the bottom.
- Always enable the application intelligence/intrusion prevention rules
- Always log the access rules, anti-spoof rules and cleanup rule
- Always place a subset rule above the superset rule

- **Never create ALLOW ANY ANY rule**
- **Never log the NetBIOS, outbound DNS query kind of rules**
- **Never all ANY services on any INBOUND rule**

- Place the user authentication rules above the Lockdown Rule
- Use the Object Groups in the rules
- Enable the Java & ActiveX code filtering for the outbound HTTP rule(s)
- Deploy the URL filtering server and expand the HTTP access rule to be redirected to URL filtering Server.
- Enable DoS/DDoS protection rules

- **Security Policy Rules, also called as access rules**
- **NAT policy Rules**
- **User Authentication Rules**
- **VPN rules**
- **Remote Access Rules**
- **Audit Policy Rulesc**

- Always enable the Anti-Spoofing Rules along with the Logging.
- Always perform the Port Address Translation on the Outbound Traffic
- Never enable the service that is NOT required for an Inbound Access
- Always enable the DoS/DDoS prevention features of perimeter firewall
- Never enable a HTTP/Telnet functionality on the perimeter firewall. Instead use the SSH or any other encrypted access
- Place a perimeter NIDS before the Firewall

- All the public access servers, like Web Server, SMTP Gateway, DNS Server, etc need to be placed as a separate LAN connected to the firewall, called as DMZ
- All the DMZ servers may be statically NATed
- Placing a NIDS in DMZ is very vital
- Access from the DMZ to the TRUSTED zones servers has to be stringently allowed across the firewall
- Optionally Configure the Private VLAN for the DMZ.

- **Perimeter Firewall Should be deployed with the High Availability**
- **Perimeter Firewall Should have multiple arms - Untrusted, Trusted, DMZ, RAS, and Security Admin Zone**
- **There has to be 2 NIDS in minimum configuration, i.e. DMZ and Trusted Zone**
- **User Authentication has to be with AAA Server**

- **Single Firewall Gateway Design**
- **High Available Firewall Cluster Design with Active/Standby Configuration**
- **High Available Firewall Cluster Design with Active/Active Load Sharing**
- **High Available Firewall Cluster Design with Active/Active Load Balancing**

Checkpoint FW-1

- Software Firewall by architecture
- Requires a Hardware/OS platform
- Extensive Integration with Antivirus software, etc
- Complex Licensing
- Very Easy GUI

Cisco PIX

- Hardware Firewall by architecture
- Proprietary Hardware/OS
- Limited Integration with the Antivirus software, etc
- Simple Licensing
- Moderately Easy GUI

Thanks!