Appendix

D Firewall Rulebase

This section presents the firewall rulebase which is used for restructuring based on its utilization as described in Section 5.3.

D.1 Initial Rulebase

pass quick from <admin> to self
pass quick from <admin> to <protected>
pass quick from <admin> to <restricted>
pass quick from (vlan1243:network) to (vlan1243:network)
block in quick from <aggressive> to any label drop-aggressive
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.34 port 80
pass quick proto tcp from 172.16.1.2 to 10.0.9.45 port 139
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.45 port 445
pass quick proto tcp from 172.16.1.2 to 10.0.9.45 port 445
pass quick proto tcp from 217.158.179.5 to 10.0.9.46 port 2301
pass quick proto tcp from 217.158.179.5 to 10.0.9.46 port 2381
pass quick proto udp from 217.158.179.5 to 10.0.9.46 port 161
pass quick proto udp from 217.158.179.5 to 10.0.9.46 port 162
pass quick from 10.22.16.1 to 10.0.9.46
pass quick from 10.22.16.2 to 10.0.9.46
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.71 port 1688
pass quick proto tcp from any to 10.0.9.73 port 80
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.34 port 443
pass quick proto tcp from any to 10.0.9.73 port 443
pass quick proto tcp from 217.158.179.5 to 10.0.9.73 port 8081
pass quick proto tcp from 217.158.179.5 to 10.0.9.73 port 8082
pass quick from <monitoring-network> to 10.0.8.0/22
pass quick from 10.100.0.0/16 to 10.0.12.0/24
pass quick from 10.70.78.0/23 to 10.0.14.207
pass quick from 10.70.78.0/23 to 10.0.14.238
pass quick from 10.70.78.0/23 to 10.0.14.254
pass quick from 10.70.78.0/23 to 10.0.107.5
pass quick from 10.70.78.0/23 to 10.0.107.6
pass quick from 10.70.78.0/23 to 10.0.107.84
pass quick from 10.70.78.0/23 to 10.0.107.85
pass quick from 10.70.78.0/23 to 10.0.107.51
pass quick from 10.13.0.0/22 to 10.12.0.0/22
pass quick from 10.13.4.0/22 to 10.12.0.0/22
pass quick from 10.15.0.0/22 to 10.12.0.0/22
pass quick from 10.16.0.0/22 to 10.12.0.0/22
pass quick from 10.100.0.0/16 to 10.12.0.0/22
pass quick from 194.204.124.0/24 to 10.12.0.0/22
pass quick from <admin> to 10.12.0.0/22
pass quick proto tcp from 10.21.6.18 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.7.200 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.8.5 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.8.12 to 10.12.7.10 port 22
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.6.18 to 10.12.7.10 port 1521
pass quick proto tcp from 10.21.8.5 to 10.12.7.10 port 1521
pass quick proto tcp from 10.21.8.6 to 10.12.7.10 port 1521
pass quick proto tcp from 10.21.8.12 to 10.12.7.10 port 1521
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.10 port 1521
pass quick from <officeit-network> to 10.12.7.10
pass quick proto tcp from 10.21.6.18 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.6.163 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.7.30 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.7.200 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.8.5 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.8.6 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.8.12 to 10.12.7.11 port 22
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.6.18 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.6.163 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.7.30 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.7.200 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.8.5 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.8.6 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.8.12 to 10.12.7.11 port 1521
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.11 port 1521
pass quick proto tcp from <neverland-network> to 10.12.7.11/32 port 8400:8403
pass quick proto tcp from <neverland-network> to 10.12.7.11/32 port 53200:53400
pass quick from <officeit-network> to 10.12.7.11
pass quick proto tcp from 10.100.8.20 to 10.12.12.13 port 21
pass quick proto tcp from 46.59.78.68 to 10.12.12.13 port 22
pass quick proto tcp from <officeit-network> to 10.12.12.13 port 22
pass quick proto tcp from <officeit-network> to 10.12.12.13 port 80
pass quick proto tcp from <officeit-network> to 10.12.12.13 port 443
pass quick proto tcp from 10.100.8.117 to 10.12.12.13 port 22
pass quick proto tcp from 10.100.8.117 to 10.12.12.13 port 2222
pass quick proto tcp from 46.59.78.68 to 10.12.12.13 port 2222
pass quick proto tcp from any to 10.12.12.13 port 25
pass quick proto tcp from any to 10.12.103.11 port 22
pass quick proto tcp from any to 10.12.103.11 port 80
pass quick proto tcp from any to 10.12.103.11 port 443
pass quick proto tcp from <neverland-network> to 10.12.103.0/24 port 8400:8403
pass quick proto tcp from <neverland-network> to 10.12.103.0/24 port 53200:53400
pass quick from 10.70.78.0/23 to 10.22.6.16
pass quick from 10.70.78.0/23 to 10.22.6.17
pass quick proto tcp from 10.23.0.0/16 to 10.12.14.129 port 22
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.1 port 80
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.1 port 443
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 80
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 443
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 13280
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 13281
pass quick proto tcp from 10.69.10.0/29 to 10.100.7.15 port 88
pass quick proto tcp from 217.158.174.240/29 to 10.100.7.15 port 88
pass quick proto tcp from 10.69.10.0/29 to 10.100.7.15 port 389
pass quick proto tcp from 217.158.174.240/29 to 10.100.7.15 port 389
pass quick proto udp from 10.69.10.0/29 to 10.100.7.15 port 88
pass quick proto udp from 217.158.174.240/29 to 10.100.7.15 port 88
pass quick proto udp from 10.69.10.0/29 to 10.100.7.15 port 389
pass quick proto udp from 217.158.174.240/29 to 10.100.7.15 port 389
pass quick from <admin> to 10.210.14.0/26
pass quick from <monitoring-network> to 10.210.14.0/26
pass quick proto icmp from 176.124.224.0/23 to 80.168.58.212
pass quick proto icmp from 195.178.165.224/27 to 80.168.58.212
pass quick proto icmp from 195.178.169.0/27 to 80.168.58.212
pass quick proto icmp from 195.178.176.208/29 to 80.168.58.212
pass quick proto icmp from 212.112.186.173 to 80.168.58.212
pass quick proto icmp from 213.115.204.0/24 to 80.168.58.212
pass quick proto tcp from 176.124.224.0/23 to 80.168.58.212 port 22
pass quick proto tcp from 195.178.165.224/27 to 80.168.58.212 port 22
pass quick proto tcp from 195.178.169.0/27 to 80.168.58.212 port 22
pass quick proto tcp from 195.178.176.208/29 to 80.168.58.212 port 22
pass quick proto tcp from 176.124.224.0/23 to 80.168.58.212 port 3839
pass quick proto udp from 195.178.165.224/27 to 80.168.58.212 port 3839
pass quick proto udp from 195.178.169.0/27 to 80.168.58.212 port 3839
pass quick proto udp from 195.178.176.208/29 to 80.168.58.212 port 3839
pass quick proto udp from 176.124.224.0/23 to 80.168.58.212 port 3839
pass quick from any to 172.16.1.0/24
pass quick proto tcp from 10.100.0.145 to 192.168.18.0/26 port 80
pass quick proto tcp from 10.100.0.145 to 192.168.18.0/26 port 443
pass quick proto tcp from 10.100.0.145 to 192.168.18.0/26 port 7682
pass quick proto tcp from 10.100.3.199 to 192.168.18.0/26 port 24800
pass quick proto udp from 10.0.9.71 to 192.168.18.0/26 port 67
pass quick proto tcp from 10.0.3.13 to 192.168.100.5 port 3389
pass quick proto tcp from 10.0.9.39 to 192.168.100.5 port 3389
pass quick proto udp from 10.0.14.37 to 192.168.100.253 port 161
pass quick proto udp from 10.0.14.37 to 192.168.100.254 port 161
pass quick proto tcp from <neverland-network> to 192.168.100.0/24 port 8400:8403
pass quick proto tcp from <neverland-network> to 192.168.100.0/24 port 53200:53400
pass quick proto tcp from any to 213.253.22.156 port 80
pass quick proto tcp from any to 213.253.22.156 port 443
pass quick from 10.0.9.51 to 213.253.22.156
pass quick proto tcp from any to 213.253.22.157 port 80
pass quick proto tcp from any to 213.253.22.157 port 443
pass quick from 10.0.9.51 to 213.253.22.157
pass quick proto tcp from any to 213.253.22.158 port 80
pass quick proto tcp from any to 213.253.22.158 port 80
pass quick proto tcp from any to 213.253.22.158 port 3389
pass quick proto tcp from any to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.2.0/23 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.8.0/23 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.12.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.14.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.15.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.20.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.24.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.12.0.0/23 to 213.253.22.158 port 82
pass quick proto tcp from 10.15.0.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.16.0.0/23 to 213.253.22.158 port 82
pass quick proto tcp from 10.100.0.0/16 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 135
pass quick proto tcp from any to 213.253.22.158 port 443
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 445
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 1239
pass quick proto tcp from 10.0.2.0/23 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.8.0/22 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.12.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.14.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.15.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.20.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.24.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.12.0.0/23 to 213.253.22.158 port 3389
pass quick proto tcp from 10.15.0.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.16.0.0/23 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 4759
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 6101
pass quick proto tcp from <neverland-network> to 213.253.22.158 port 8400:8403
pass quick proto tcp from 10.0.3.13 to 213.253.22.158 port 8530
pass quick proto tcp from 10.100.8.20 to 213.253.22.158 port 8530
pass quick proto tcp from 10.100.8.20 to 213.253.22.158 port 8630
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 10000
pass quick proto tcp from <neverland-network> to 213.253.22.158 port 53200:53400
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 80
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 80
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 161
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 161
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 2301
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 2301
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 2381
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 2381
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 5989
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 5989
pass quick proto udp from 10.0.9.45 to 213.253.22.152/29 port 161
pass quick proto udp from 10.0.9.46 to 213.253.22.152/29 port 161
pass quick from <admin> to 213.253.22.152/29
pass quick from (vlan618:network) to 217.158.143.32/29
pass quick proto icmp from any to 217.158.143.36
pass quick proto tcp from 195.81.247.129 to 217.158.143.36 port 5060
pass quick proto tcp from 195.81.247.148 to 217.158.143.36 port 5060
pass quick proto tcp from 195.81.247.129 to 217.158.143.36 port 5061
pass quick proto tcp from 195.81.247.148 to 217.158.143.36 port 5061
pass quick proto udp from 195.81.247.129 to 217.158.143.36 port 5060
pass quick proto udp from 195.81.247.148 to 217.158.143.36 port 5060
pass quick proto udp from 195.81.247.129 to 217.158.143.36 port 5061
pass quick proto udp from 195.81.247.148 to 217.158.143.36 port 5061
pass quick proto udp from any to 217.158.143.36 port 60000:64000
pass quick proto tcp from <neverland-network> to 217.158.143.32/29 port 8400:8403
pass quick proto tcp from <neverland-network> to 217.158.143.32/29 port 53200:53400
pass quick proto ah from any to 217.158.174.245
pass quick proto esp from any to 217.158.174.245
pass quick proto tcp from 10.0.2.0/23 to 217.158.174.245 port 443
pass quick proto udp from any to 217.158.174.245 port 443
pass quick proto udp from any to 217.158.174.245 port 500
pass quick proto udp from any to 217.158.174.245 port 4500
pass quick from 10.100.8.45 to 217.158.174.240/29
pass quick from 10.0.9.46 to 217.158.174.245
pass quick from <admin> to 217.158.174.240/29
pass quick proto icmp from { <bmview0> <bmview1> } to <protected>
pass quick proto icmp from <protected> to <protected>
pass quick proto icmp from <restricted> to <protected>
pass quick proto icmp from <ubpublic> to <protected>
pass quick proto icmp from <whitelist> to <protected>
pass quick proto icmp from { <bmview0> <bmview1> } to <restricted>
pass quick proto icmp from <protected> to <restricted>
pass quick proto icmp from <restricted> to <restricted>
pass quick proto icmp from <ubpublic> to <restricted>
pass quick proto icmp from <whitelist> to <restricted>
block log quick from { <bmview0> <bmview1> } to <protected>
block log quick from <protected> to <protected>
block log quick from <restricted> to <restricted>
block log quick from <ubpublic> to <protected>
block log quick from <whitelist> to <protected>
block log quick from any to <protected> label drop-protected
block log quick from { <bmview0> <bmview1> } to <restricted>
block log quick from <protected> to <restricted>
block log quick from <restricted> to <restricted>
block log quick from <ubpublic> to <restricted>
block log quick from <whitelist> to <restricted>
block log quick from <protected> to <restricted>

D.2 Rulebase post re-ordering

pass quick proto tcp from <officeit-network> to 10.12.12.13 port 443
pass quick from (vlan1243:network) to (vlan1243:network)
pass quick proto tcp from <officeit-network> to 10.12.12.13 port 80
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 80
pass quick proto tcp from any to 213.253.22.158 port 80
pass quick proto tcp from 10.21.6.122 to 10.70.78.164 port 443
pass quick proto tcp from any to 213.253.22.158 port 443
pass quick proto tcp from 10.21.8.5 to 10.12.7.11 port 1521
pass quick from 10.21.8.12 to 10.12.7.10 port 22
pass quick proto tcp from 195.178.176.208/29 to 80.168.58.212 port 22
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 80
pass quick proto tcp from any to 213.253.22.156 port 80
pass quick proto tcp from 10.21.7.200 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.2.0/23 to 213.253.22.158 port 82
pass quick proto tcp from any to 213.253.22.156 port 443
pass quick proto tcp from any to 10.12.103.11 port 22
pass quick from <admin> to self
pass quick proto tcp from <officeit-network> to 10.12.12.13 port 22
pass quick proto tcp from 10.21.6.123 to 10.70.78.164 port 443
pass quick proto tcp from 10.21.8.5 to 10.12.7.11 port 22
pass quick from <admin> to <protected>
pass quick proto esp from any to 217.158.174.245
pass quick proto tcp from 10.21.8.6 to 10.12.7.11 port 1521
pass quick proto udp from 10.200.50.1/32 to 10.69.2.0/27 port 123
pass quick proto icmp from any to 10.100.0.0/16
pass quick from <admin> to 10.12.0.0/22
pass quick proto tcp from 10.100.8.117 to 10.12.12.13 port 2222
pass quick from 10.70.78.0/23 to 10.22.6.16
pass quick from 10.70.78.0/23 to 10.0.107.84
pass quick proto udp from 10.70.78.0/23 to 10.69.2.0/27 port 123
pass quick proto udp from 192.168.100.0/24 to 10.69.2.0/27 port 123
pass quick proto tcp from 192.168.100.0/24 to 10.0.9.45 port 445
pass quick proto tcp from 10.0.100.0.145 to 192.168.18.0/26 port 443
pass quick from <admin> to 10.210.14.0/26
pass quick from <admin> to 10.70.78.0/23
pass quick from 10.70.78.0/23 to 10.0.107.6
pass quick proto tcp from 46.59.78.68 to 10.12.12.13 port 2222
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 80
pass quick proto tcp from 10.21.6.18 to 10.12.7.10 port 1521
pass quick proto tcp from 172.16.1.2 to 10.0.9.45 port 139
pass quick from <admin> to <restricted>
pass quick proto ah from any to 217.158.174.245
pass quick proto udp from 217.158.179.5 to 10.0.9.46 port 162
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.45 port 445
pass quick from 10.22.16.1 to 10.0.9.46
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.10 port 22
pass quick from 10.22.16.2 to 10.0.9.46
pass quick from 10.0.9.51 to 213.253.22.156
pass quick from 10.70.78.0/23 to 10.0.107.85
block in quick from <aggressive> to any label drop-aggressive
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.34 port 80
pass quick proto tcp from 217.158.179.5 to 10.0.9.46 port 2301
pass quick proto tcp from 217.158.179.5 to 10.0.9.46 port 2381
pass quick proto udp from 217.158.179.5 to 10.0.9.46 port 161
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.71 port 1688
pass quick proto tcp from any to 10.0.9.73 port 80
pass quick proto tcp from 10.61.1.0/24 to 10.0.9.34 port 443
pass quick proto tcp from any to 10.0.9.73 port 443
pass quick proto tcp from 217.158.179.5 to 10.0.9.73 port 8081
pass quick proto tcp from 217.158.179.5 to 10.0.9.73 port 8082
pass quick from <monitoring-network> to 10.0.8.0/22
pass quick from 10.100.0.0/16 to 10.0.12.0/24
pass quick from 10.70.78.0/23 to 10.0.14.207
pass quick from 10.70.78.0/23 to 10.0.14.238
pass quick from 10.70.78.0/23 to 10.0.14.254
pass quick from 10.0.9.73 to 10.0.9.73
pass quick from 10.0.9.73 to 10.0.9.73
pass quick from 10.100.0.0/16 to 10.0.12.0/22
pass quick from 10.0.100.0.0/16 to 10.12.0.0/22
pass quick from 194.204.124.0/24 to 10.12.0.0/22
pass quick proto tcp from 10.21.6.18 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.7.200 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.8.5 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.8.6 to 10.12.7.10 port 22
pass quick proto tcp from 10.21.8.5 to 10.12.7.10 port 1521
pass quick proto tcp from 10.21.8.6 to 10.12.7.10 port 1521
pass quick proto tcp from 10.21.8.12 to 10.12.7.10 port 1521
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.10 port 1521
pass quick from <officeit-network> to 10.12.7.10
pass quick proto tcp from 10.21.6.18 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.6.163 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.7.30 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.8.6 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.8.12 to 10.12.7.11 port 22
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.11 port 22
pass quick proto tcp from 10.21.6.18 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.6.163 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.7.30 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.7.200 to 10.12.7.11 port 1521
pass quick proto tcp from 10.21.8.12 to 10.12.7.11 port 1521
pass quick proto tcp from 10.69.69.0/24 to 10.12.7.11 port 1521
pass quick proto tcp from <neverland-network> to 10.12.7.11/32 port 8400:8403
pass quick proto tcp from <neverland-network> to 10.12.7.11/32 port 53200:53400
pass quick from <officeit-network> to 10.12.7.11
pass quick proto tcp from 10.100.8.20 to 10.12.12.13 port 21
pass quick proto tcp from 46.59.78.68 to 10.12.12.13 port 22
pass quick proto tcp from any to 10.12.12.13 port 25
pass quick proto tcp from any to 10.12.103.11 port 80
pass quick proto tcp from any to 10.12.103.11 port 443
pass quick proto tcp from <neverland-network> to 10.12.103.0/24 port 8400:8403
pass quick proto tcp from <neverland-network> to 10.12.103.0/24 port 53200:53400
pass quick proto tcp from 10.70.78.0/23 to 10.22.6.17
pass quick proto tcp from 10.23.0.0/16 to 10.12.14.129 port 22
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.1 port 80
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.1 port 443
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 443
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 13280
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.60 port 13281
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.136 port 80
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.136 port 443
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.138 port 80
pass quick proto tcp from 192.168.18.0/26 to 10.23.32.138 port 443
pass quick proto tcp from 192.168.18.0/26 to 10.23.33.1
pass quick from 10.70.78.0/23 to 10.32.26.8
pass quick from 10.70.78.0/23 to 10.32.26.9
pass quick from <admin> to 10.42.2.0/24
pass quick proto udp from <protected> to 10.69.2.0/27 port 123
pass quick proto udp from 10.12.103.0/24 to 10.69.2.0/27 port 123
pass quick proto udp from 10.12.255.0/30 to 10.69.2.0/27 port 123
pass quick proto udp from 10.201.0.188/30 to 10.69.2.0/27 port 123
pass quick proto udp from 10.203.1.184/30 to 10.69.2.0/27 port 123
pass quick proto udp from 10.210.14.0/26 to 10.69.2.0/27 port 123
pass quick proto udp from 192.168.18.0/26 to 10.69.2.0/27 port 123
pass quick proto udp from 217.158.143.32/29 to 10.69.2.0/27 port 123
pass quick proto icmp from 172.31.2.0/24 to 10.69.7.44
pass quick proto tcp from 172.31.2.0/24 to 10.69.7.44 port 80
pass quick proto tcp from 172.31.2.0/24 to 10.69.7.44 port 443
pass quick proto tcp from 172.31.2.0/24 to 10.69.7.44 port 623
pass quick proto tcp from 172.31.2.0/24 to 10.69.7.44 port 5120
pass quick proto tcp from 172.31.2.0/24 to 10.69.7.44 port 5900
pass quick proto tcp from 172.31.2.0/24 to 10.69.7.44 port 5901
pass quick proto ah from any to 10.69.10.4
pass quick proto esp from any to 10.69.10.4
pass quick proto tcp from any to 10.69.10.4 port 443
pass quick proto udp from any to 10.69.10.4 port 443
pass quick proto udp from any to 10.69.10.4 port 500
pass quick proto udp from any to 10.69.10.4 port 4500
pass quick from 10.100.8.45 to 10.69.10.4
pass quick from <admin> to 10.69.10.0/29
pass quick from 10.0.2.0/23 to 10.70.78.0/23
pass quick from 10.0.12.0/24 to 10.70.78.0/23
pass quick from 10.0.14.0/23 to 10.70.78.0/23
pass quick from 10.0.24.10 to 10.70.78.0/23
pass quick from 10.0.107.0/23 to 10.70.78.0/23
pass quick from 10.2.3.0/28 to 10.70.78.0/23
pass quick from 10.2.3.16/28 to 10.70.78.0/23
pass quick from 10.2.3.32/28 to 10.70.78.0/23
pass quick from 10.2.3.48/28 to 10.70.78.0/23
pass quick from 10.2.129.16/28 to 10.70.78.0/23
pass quick from 10.2.129.32/28 to 10.70.78.0/23
pass quick from 10.2.129.48/28 to 10.70.78.0/23
#pass quick from 10.12.14.0/23 to 10.70.78.0/23
pass quick from 10.21.6.0/24 to 10.70.78.0/23
pass quick from 10.21.11.0/24 to 10.70.78.0/23
pass quick from 10.22.6.0/24 to 10.70.78.0/23
pass quick from 10.23.11.0/24 to 10.70.78.0/23
pass quick from 10.32.26.0/24 to 10.70.78.0/23
pass quick from <admin> to 10.100.0.0/16
pass quick proto tcp from 10.69.10.0/29 to 10.100.7.15 port 88
pass quick proto tcp from 217.158.174.240/29 to 10.100.7.15 port 88
pass quick proto tcp from 10.69.10.0/29 to 10.100.7.15 port 389
pass quick proto tcp from 217.158.174.240/29 to 10.100.7.15 port 389
pass quick proto udp from 10.69.10.0/29 to 10.100.7.15 port 88
pass quick proto udp from 217.158.174.240/29 to 10.100.7.15 port 88
pass quick proto udp from 10.69.10.0/29 to 10.100.7.15 port 389
pass quick proto udp from 217.158.174.240/29 to 10.100.7.15 port 389
pass quick from <monitoring-network> to 10.210.14.0/26
pass quick proto icmp from 176.124.224.0/23 to 80.168.58.212
pass quick proto icmp from 195.178.165.224/27 to 80.168.58.212
pass quick proto icmp from 195.178.176.208/29 to 80.168.58.212
pass quick proto icmp from 195.178.169.0/27 to 80.168.58.212
pass quick proto icmp from 212.112.186.173 to 80.168.58.212
pass quick proto icmp from 213.115.204.0/24 to 80.168.58.212
pass quick proto tcp from 176.124.224.0/23 to 80.168.58.212 port 22
pass quick proto tcp from 195.178.165.224/27 to 80.168.58.212 port 22
pass quick proto tcp from 195.178.169.0/27 to 80.168.58.212 port 22
pass quick proto tcp from 213.115.204.0/24 to 80.168.58.212 port 22
pass quick proto udp from 176.124.224.0/23 to 80.168.58.212 port 88
pass quick proto udp from 195.178.165.224/27 to 80.168.58.212 port 88
pass quick proto udp from 195.178.169.0/27 to 80.168.58.212 port 88
pass quick proto udp from 213.115.204.0/24 to 80.168.58.212 port 88
pass quick from any to 172.16.1.0/24
pass quick proto tcp from 10.100.0.145 to 192.168.18.0/26 port 80
pass quick proto tcp from 10.100.0.145 to 192.168.18.0/26 port 7682
pass quick proto tcp from 10.100.3.199 to 192.168.18.0/26 port 24800
pass quick proto udp from 10.0.9.71 to 192.168.18.0/26 port 67
pass quick proto tcp from 10.0.3.13 to 192.168.100.5 port 3389
pass quick proto tcp from 10.0.3.39 to 192.168.100.5 port 3389
pass quick proto udp from 10.0.14.37 to 192.168.100.253 port 161
pass quick proto udp from 10.0.14.37 to 192.168.100.254 port 161
pass quick proto tcp from <neverland-network> to 192.168.100.0/24 port 8400:8403
pass quick proto tcp from <neverland-network> to 192.168.100.0/24 port 53200:53400
pass quick proto tcp from any to 213.253.22.157 port 80
pass quick proto tcp from any to 213.253.22.157 port 443
pass quick from 10.0.9.51 to 213.253.22.157
pass quick proto tcp from 10.100.8.20 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.8.0/23 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.12.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.14.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.15.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.20.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.24.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.12.0.0/23 to 213.253.22.158 port 82
pass quick proto tcp from 10.15.0.0/24 to 213.253.22.158 port 82
pass quick proto tcp from 10.16.0.0/23 to 213.253.22.158 port 82
pass quick proto tcp from 10.100.0.0/16 to 213.253.22.158 port 82
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 135
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 445
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 1239
pass quick proto tcp from 10.0.2.0/23 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.8.0/22 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.12.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.14.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.15.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.20.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.24.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.12.0.0/23 to 213.253.22.158 port 3389
pass quick proto tcp from 10.15.0.0/24 to 213.253.22.158 port 3389
pass quick proto tcp from 10.16.0.0/23 to 213.253.22.158 port 3389
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 4759
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 6101
pass quick proto tcp from <neverland-network> to 213.253.22.158 port 8400:8403
pass quick proto tcp from 10.0.10.0/24 to 213.253.22.158 port 8530
pass quick proto tcp from 10.0.10.0/24 to 213.253.22.158 port 8530
pass quick proto tcp from 10.0.9.57 to 213.253.22.158 port 10000
pass quick proto tcp from <neverland-network> to 213.253.22.158 port 53200:53400
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 161
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 161
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 2301
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 2301
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 2301
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 2301
pass quick proto tcp from 10.0.9.45 to 213.253.22.152/29 port 5989
pass quick proto tcp from 10.0.9.46 to 213.253.22.152/29 port 5989
pass quick proto udp from 10.0.9.45 to 213.253.22.152/29 port 161
pass quick proto udp from 10.0.9.46 to 213.253.22.152/29 port 161
pass quick from <admin> to 213.253.22.152/29
pass quick from [vian618:network] to 217.158.143.32/29
pass quick proto icmp from any to 217.158.143.36
pass quick proto tcp from 195.81.247.129 to 217.158.143.36 port 5060
pass quick proto tcp from 195.81.247.148 to 217.158.143.36 port 5060
pass quick proto tcp from 195.81.247.129 to 217.158.143.36 port 5061
pass quick proto tcp from 195.81.247.148 to 217.158.143.36 port 5061
pass quick proto udp from 195.81.247.129 to 217.158.143.36 port 5060
pass quick proto udp from 195.81.247.148 to 217.158.143.36 port 5060
pass quick proto udp from 195.81.247.129 to 217.158.143.36 port 5061
pass quick proto udp from 195.81.247.148 to 217.158.143.36 port 5061
pass quick proto udp from any to 217.158.143.36 port 60000:64000
pass quick proto tcp from <neverland-network> to 217.158.143.32/29 port 8400:8403
pass quick proto tcp from <neverland-network> to 217.158.143.32/29 port 53200:53400
pass quick proto tcp from any to 217.158.174.245 port 443
pass quick proto udp from any to 217.158.174.245 port 443
pass quick proto udp from any to 217.158.174.245 port 500
pass quick proto udp from any to 217.158.174.245 port 4500
pass quick from 10.0.2.0/23 to 217.158.174.240/29
pass quick from 10.100.8.45 to 217.158.174.245
pass quick from <admin> to 217.158.174.240/29
pass quick proto icmp from { <bmview0> <bmview1> } to <protected>
pass quick proto icmp from <protected> to <protected>
pass quick proto icmp from <restricted> to <protected>
pass quick proto icmp from <ubpublic> to <protected>
pass quick proto icmp from <whitelist> to <protected>
pass quick proto icmp from { <bmview0> <bmview1> } to <restricted>
pass quick proto icmp from <protected> to <restricted>
pass quick proto icmp from <restricted> to <restricted>
pass quick proto icmp from <ubpublic> to <restricted>
pass quick proto icmp from <whitelist> to <restricted>

block log quick from { <bmview0> <bmview1> } to <protected>
block log quick from <protected> to <protected>
block log quick from <restricted> to <protected>
block log quick from <ubpublic> to <protected>
block log quick from <whitelist> to <protected>
block log quick from any to <protected> label drop-protected
block log quick from { <bmview0> <bmview1> } to <restricted>
block log quick from <protected> to <restricted>
block log quick from <restricted> to <restricted>
block log quick from <ubpublic> to <restricted>
block log quick from <whitelist> to <restricted>
block log quick from <protected> to <restricted>
Appendix

E OpenBSD Configurations for interconnections of firewalls at multiple geographic locations.

This section represents the detailed setup used for testing the design of interconnections of firewalls at multiple geographic location through a standalone network for measuring performance of OpenBSD firewall as mentioned in Fig. 6.2. It consists of two sites having OpenBSD firewall device and routing device at each site along with other supporting systems. Firewall device has three interfaces -

(1) To connect to Internet (via Internet routers),

(2) To connect to the Core network (via Routing device, through GRE tunnel)

(3) To connect to the protected (Intranet) networks.

Detailed connectivity diagram is shown in Fig. E.1.
Fig. E.1 – Laboratory testing setup used for interconnections of firewalls at multiple geographic locations through a standalone network.
E.1 OpenBSD Firewall Device 1 Configurations

The hardware devices used for configuration are Supermicro X9SRD-F having base operating system OpenBSD 5.5 installed. Below are the major configuration steps performed to build them.

E.1.1 Initial Setup

A full installation of OpenBSD software is performed on the server with creation of below basic partitions.

<table>
<thead>
<tr>
<th>Partition</th>
<th>16 Gb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swap</td>
<td>4 Gb</td>
</tr>
<tr>
<td>/var</td>
<td>The rest</td>
</tr>
</tbody>
</table>

Once installation is completed, below steps are performed to configure the devices.

(1) User with username “theroot” is added in group wheel to be able to become root. Then, configuration of user and root prompt is performed.

Respective user’s .profile is updated by appending the following lines:

```
/root/.profile
export PS1="$(hostname | cut -d. -f1,2)#"
```

```
/home/theroot/.profile
export PS1="$USER@$\{hostname | cut -d. -f1,2\}$"
```

(2) Directory /root/local/bin is created and /root/local/bin is appended in /root/.profile’s PATH variable.

```
/root/.profile
...snip...
PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin:/usr/local/sbin:/usr/local/bin:/root/local/bin...
...snip...
```
(3) File /etc/login.conf is updated and openfiles-cur is raised to 512 in the daemon section.

```
/root/.profile
...
 daemon:\
   :ignorenologin:\
   :databsize=infinity:\
   :maxproc=infinity:\
   :openfiles-cur=512:\
   :stacksize-cur=8M:\
   :localcipher=blowfish,8:\
   :tc=default:
...
```

(4) File /etc/sysctl.conf is created, in order to define below non-default settings.

- Enable IP forwarding
- Set the box to reboot on kernel panic
- Increase ifq to 1024
- Increase maxclusters to 24576
- Enable CARP preempt

```
/etc/sysctl.conf
net.inet.ip.forwarding=1
ddb.panic=0
net.inet.ip.ifq.maxlen=1024
kern.maxclusters=24576
net.inet.carp.preempt=1
```

(5) System is rebooted and console is further verified to ensure it boots up without errors.

(6) File /etc/ssh/sshd_config is updated with below section added at the top of the file.
Also, file is updated by adding below section at end of the file.

```
/etc/ssh/sshd_config

...snip...

# LOCALHOST IPv4
Match Address 127.0.0.0/8
  PasswordAuthentication yes
  PermitRootLogin yes
# MANAGEMENT NETWORKS
Match Address 10.69.4.0/23
  PasswordAuthentication yes
```

(7) Service sshd is restarted using the sshd rc.d script.

```
/etc/rc.d/sshd restart
```

Note that the update does not affect existing sessions. Verification is done with new session to confirm login is possible after updating the configuration.

### E.1.2 Interfaces Configurations

OpenBSD keeps the configuration for each interface in files named `/etc/hostname.<INTERFACE>`. The interface file is a list of commands beginning with “!” Static routes are also added in these files.
1. Physical Interfaces

Enable the physical interfaces, with IPv6 processing disabled. Also, description is added to mention where interface is connected.

```
/etc/hostname.ix0
! ifconfig $1 description "EXT-SWITCH-304 PORT 37" up
```

```
/etc/hostname.ix1
! ifconfig $1 description "EXT-SWITCH-305 PORT 38" up
```

2. Trunk Interfaces

```
/etc/hostname.trunk0
! ifconfig $1 trunkproto lacp description "LACP TRUNK" up
! ifconfig $1 trunkport IX0
! ifconfig $1 trunkport IX1
```

3. Internet Interface

Default route is added to this interface.

```
/etc/hostname.vlan301
! ifconfig $1 description "INTERNET-RTR-1" vlandev trunk0 vlan 301 up
! ifconfig $1 192.0.2.2/24
## IPv4 default route. We do not use /etc/mygate
! route add 0/0 192.0.2.254
```

```
/etc/hostname.carp301
! ifconfig $1 -inet6 192.0.2.24 vhid 10 advskew 50 up
```
“Performance Evaluation and Optimization for Distributed Network Firewall Design”

4. Intranet Interface

/etc/hostname.vlan1240

! ifconfig $1 description "ROUTING DEVICE 1" vlandev trunk0 vlan 1240 up
! ifconfig $1 192.0.3.2/24

/etc/hostname.carp1240

! ifconfig $1 -inet 192.0.3.1/24 vhid 20 advskew 50 up

5. NTP Interface

/etc/hostname.vlan302

! ifconfig $1 description "NTP" vlandev trunk0 vlan 302 up
! ifconfig $1 10.69.2.253/24

/etc/hostname.carp302

! ifconfig $1 -inet6 10.69.2.254/24 vhid 30 advskew 50 up

6. DNS Interface

/etc/hostname.vlan303

! ifconfig $1 description "DNS" vlandev trunk0 vlan 303 up
! ifconfig $1 10.69.8.2/24

/etc/hostname.carp303

! ifconfig $1 -inet6 10.69.8.1/24 vhid 40 advskew 50 up

E.1.3 BGP configuration

/etc/bgpd.conf

### global configuration
AS 65171
connect-retry 30
router-id 192.0.2.2
network inet connected
network inet static
### peers
group "IBGP-V4" {
    remote-as 65171
    announce IPv4 unicast
    announce IPv6 none
    announce restart no
    set nexthop self
demote carp
holdtime 50
neighbor 192.0.3.4 {
    descr "ROUTING DEVICE 1"
    local-address 192.0.3.2
    set med +127
}
}
### FILTERS
# don't accept default from any peer
deny quick from any prefix 0/0
# don't advertise the local Internet uplink lan
deny quick to any prefix 192.0.2.0/24 prefixlen <= 32
# rewrite nexthop to the ROUTING DEVICE interface CARP address out
allow quick to group "IBGP-V4" set nexthop 192.0.2.1
# allow any in from BMR, copy each view to pf tables
allow quick from 192.0.3.4 set pftable bmview0

In order to enable the BGP software on start-up, bgpd_flags="" is added to /etc/rc.conf.local.
Also, following lines is added to /etc/pf.conf, without this the BGP software will not start.

```bash
/etc/pf.conf

...snip...

table <bmview0> persist

table <bmview1> persist

...snip...

#Reload pf, and start the bgp software:
pfctl -f /etc/pf.conf
/etc/rc.d/bgpd start
```

### E.1.4 DNS Configurations

Internal configured DNS is used as resolvers.

```bash
/etc/resolv.conf

search chirag.com

nameserver 10.69.8.254

lookup file bind
```

### E.1.5 NTP Configurations

```bash
/etc/ntpd.conf

listen on 127.0.0.1

server 10.69.2.1

server 10.69.2.2
```

### E.1.6 SNMP Configurations

```bash
/etc/snmpd.conf

read-only community snow

read-write community feed

# Adjust the local system information

system contact "Chirag"
```
system location "<SITE>"
system services 74

E.1.7 Services Configurations

```
/etc/rc.conf.local
ntpd_flags=""
snmpd_flags=""
bgpd_flags=""
```

E.2 OpenBSD Routing Device 1 Configurations

The hardware devices used for configuration are Supermicro X9SRD-F having base operating system OpenBSD 5.5 installed. Below are the major configuration steps performed to build them.

A routing device has three types of interfaces

1. Core interface – connects to other routing devices.
2. Edge Interface - connects to firewall edge devices. An edge interface may be a physical interface or a VLAN interface.
3. Uplink interface - connects to a packet switched network, like the Internet, and is used to provision tunnels.

E.2.1 Interfaces Configurations

1. Physical Interfaces

```
/etc/hostname.ix0
! ifconfig $1 description "EXT-SWITCH-304 PORT 37" up
```

```
/etc/hostname.ix1
! ifconfig $1 description "EXT-SWITCH-305 PORT 38" up
```
2. Trunk Interfaces

```
/etc/hostname.trunk0

! ifconfig $1 trunkproto lACP description "LACP TRUNK" up
! ifconfig $1 trunkport IX0
! ifconfig $1 trunkport IX1
```

3. Internet Interface

```
/etc/hostname.vlan301

! ifconfig $1 description "INTERNET-RTR-1" vlandev trunk0 vlan 301 up
! ifconfig $1 192.0.2.4/24
### peer routes
! route add 192.0.1.4/32 192.0.2.254
```

4. Intranet Interface

```
/etc/hostname.vlan1240

! ifconfig $1 description "ROUTER-1" vlandev trunk0 vlan 1240 up
! ifconfig $1 192.0.3.5/24
```

```
/etc/hostname.carp1240

! ifconfig $1 -inet6 192.0.3.4/24 vhid 60 adskew 50 up
```

5. Loopback Interface

```
/etc/hostname.lo1

! ifconfig $1 description "MANAGEMENT" up
! ifconfig $1 172.30.255.251/32
```

6. GRE interface

```
/etc/hostname.gre1
```
E.2.2 BGP Configurations

/etc/bgpd.conf

```conf
### global configuration
AS 65171
connect-retry 30
router-id 192.0.2.4
network 172.30.255.251/32 # lo1
network inet connected
network inet static
### add tunnel networks here, sort by ip
### neighbors and peers

group "IBGP-RR-PEER-V4" {
  remote-as 65171
  announce IPv4 unicast
  announce IPv6 none
  announce restart no
  set nexthop self
  route-reflector
  holdtime 50
  neighbor 192.0.3.2 {
    descr "FIREWALL DEVICE 1"
    local-address 192.0.3.5
    set med +100
  }
  neighbor 172.30.251.225 {
```
### Filters

- `descr "ROUTING DEVICE 2"
- `local-address 172.30.251.224`
- `set med +100`

### Deny Rules
- `deny quick from any prefix 0/0`
- `deny quick to any prefix 192.0.2.0/24 prefixlen <= 32`
- `deny quick to any prefix 192.0.1.4/32`

### Maintenance Mode Rule
- `match to any set metric +987654321`
- `permit any`

### DNS Configurations

```bash
/etc/resolv.conf
```

- `search chirag.com`
- `nameserver 10.69.8.254`
- `lookup file bind`

### NTP Configurations

```bash
/etc/ntpd.conf
```

- `listen on 127.0.0.1`
- `server 10.69.2.1`
- `server 10.69.2.2`
E.2.5 Syslog configurations

/etc/syslog.conf

...snip...

*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none @10.69.160.1

*.info;authpriv,kern.debug @10.69.160.1

...snip...

E.2.6 SNMP configurations

/etc/snmpd.conf

read-only community snow
read-write community feed

# Adjust the local system information
system contact "Chirag"

system location "<SITE>"

system services 74

E.2.7 Services configurations

/etc/rc.conf.local

ntpd_flags=""

ipsec=YES

snmpd_flags=""

isakmpd_flags="-K"

bgpd_flags=""
1. Configuration

   ! ifconfig $1 description "EXT-SWITCH-304 PORT 37" up
   ! ifconfig $1 description "EXT-SWITCH-305 PORT 38" up

   /etc/hostname.ix1

   ! ifconfig $1 description "EXT-SWITCH-304 PORT 37" up
   ! ifconfig $1 description "EXT-SWITCH-305 PORT 38" up

   /etc/hostname.trunk0

   ! ifconfig $1 trunkproto lacp description "LACP TRUNK" up
   ! ifconfig $1 trunkport IX0
   ! ifconfig $1 trunkport IX1

   /etc/hostname.vlan301

   ! ifconfig $1 description "INTERNET-RTR-2" vlandev trunk0 vlan 301 up
   ! ifconfig $1 192.0.0.2/24
   ## IPv4 default route. We do not use /etc/mygate
   ! route add 0/0 192.0.0.254

   /etc/hostname.carp301

   ! ifconfig $1 -inet6 192.0.0.1/24 vhid 10 advskew 50 up

   /etc/hostname.vlan1240

   ! ifconfig $1 description "ROUTING DEVICE 2" vlandev trunk0 vlan 1240 up
   ! ifconfig $1 192.0.1.2/24

   /etc/hostname.carp1240

   ! ifconfig $1 -inet6 192.0.1.1/24 vhid 20 advskew 50 up

3. Internet

4. Intranet
5. SYSLOG

```bash
/etc/hostname.vlan302

! ifconfig $1 description "SYSLOG" vlandev trunk0 vlan 302 up
! ifconfig $1 10.69.160.253/24

/etc/hostname.carp302

! ifconfig $1 -inet6 10.69.160.254/24 vhid 30 advskew 50 up

6. SNMP

```bash
/etc/hostname.vlan303

! ifconfig $1 description "SNMP" vlandev trunk0 vlan 303 up
! ifconfig $1 10.69.12.2/24

/etc/hostname.carp303

! ifconfig $1 -inet 10.69.12.1/24 vhid 40 advskew 50 up

E.3.2 BGP configuration

```bash
/etc/bgpd.conf

### global configuration
AS 65171
connect-retry 30
router-id 192.0.1.2
network inet connected
network inet static
### peers
group "IBGP-V4" {
    remote-as 65171
    announce IPv4 unicast
    announce IPv6 none
```
```
announce restart no
set nexthop self
demote carp
holdtime 50
neighbor 192.0.0.4 {
    descr "ROUTING DEVICE 2"
    local-address 192.0.0.2
    set med +127
}
}
### FILTERS
# don't accept default from any peer
deny quick from any prefix 0/0
# don't advertise the local Internet uplink lan
deny quick to any prefix 192.0.1.0/24 prefixlen <= 32
# rewrite nexthop to the ROUTING DEVICE interface CARP address out
allow quick to group "IBGP-V4" set nexthop 192.0.1.1
# allow any in from BMR, copy each view to pf tables
allow quick from 192.0.1.4 set pftable bmview0
```

### E.3.3 DNS Configurations

<table>
<thead>
<tr>
<th>/etc/resolv.conf</th>
</tr>
</thead>
<tbody>
<tr>
<td>search chirag.com</td>
</tr>
<tr>
<td>nameserver 10.69.8.254</td>
</tr>
<tr>
<td>lookup file bind</td>
</tr>
</tbody>
</table>

### E.3.4 NTP Configurations

<table>
<thead>
<tr>
<th>/etc/ntpd.conf</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen on 127.0.0.1</td>
</tr>
<tr>
<td>server 10.69.2.1</td>
</tr>
<tr>
<td>server 10.69.2.2</td>
</tr>
</tbody>
</table>
### E.3.5 SNMP Configurations

```
/etc/snmpd.conf

read-only community snow
read-write community feed

# Adjust the local system information
system contact "Chirag"

system location "<SITE>"

system services 74
```

### E.3.6 Services Configurations

```
/etc/rc.conf.local

ntpd_flags=""

snmpd_flags=""

bgpd_flags=""
```

### E.4 OpenBSD Routing Device 2 Configurations

#### E.4.1 Interfaces Configurations

1. **Physical Interfaces**

```
/etc/hostname.ix0

! ifconfig $1 description "EXT-SWITCH-304 PORT 37" up
```

```
/etc/hostname.ix1

! ifconfig $1 description "EXT-SWITCH-305 PORT 38" up
```

2. **Trunk Interfaces**

```
/etc/hostname.trunk0

! ifconfig $1 trunkproto lACP description "LACP TRUNK" up
```
1. ifconfig $1 trunkport IX0
   ifconfig $1 trunkport IX1

3. Internet Interface

/etc/hostname.vlan301

   ifconfig $1 description "INTERNET-RTR-2" vlandev trunk0 vlan 301 up
   ifconfig $1 192.0.1.4/24
   ## ## peer routes
   route add 192.0.2.4/32 192.0.1.254

4. Intranet Interface

/etc/hostname.vlan1240

   ifconfig $1 description "ROUTING DEVICE 2" vlandev trunk0 vlan 1240 up
   ifconfig $1 192.0.0.5/24

/etc/hostname.carp1240

   ifconfig $1 -inet6 192.0.0.4/24 vhid 6 advskew 50 up

5. Loopback Interface

/etc/hostname.lo1

   ifconfig $1 description "MANAGEMENT" up
   ifconfig $1 172.30.255.251/32

6. GRE interface

/etc/hostname.gre1

   ifconfig $1 description "ROUTING DEVICE 1" mtu 1400 up
   ifconfig $1 172.30.251.225 172.30.251.224 netmask 255.255.255.254
   ifconfig $1 tunnel 192.0.1.4 192.0.2.4
## E.4.2 BGP Configurations

```
# etc/bgpd.conf

### global configuration
AS 65171
connect-retry 30
router-id 192.0.1.4

network 172.30.255.251/32  # lo1
network inet connected
network inet static

### neighbors and peers

#### group "IBGP-RR-PEER-V4"
remote-as 65171
announce IPv4 unicast
announce IPv6 none
announce restart no
set nexthop self
route-reflector
holdtime 50

neighbor 192.0.0.2 {
descr "FIREWALL DEVICE 1"
local-address 192.0.0.5
set med +100
}

neighbor 172.30.251.224 {
descr "ROUTING DEVICE 1"
local-address 172.30.251.225
set med +100
}

### filters

### don't accept default from any peer
```
deny quick from any prefix 0/0

## site specific
# don't advertise the local uplink lan
deny quick to any prefix 192.0.1.0/24 prefixlen <= 32
# don't advertise statics for bmr peers
deny quick to any prefix 192.0.2.4/32        # ROUTING DEVICE 1

## maintenance mode rule
#match to any set metric +987654321
## permit any
allow from any
allow to any

E.4.3 DNS configurations

/etc/resolv.conf

search chirag.com
nameserver 10.69.8.254
lookup file bind

E.4.4 NTP configurations

/etc/ntpd.conf

listen on 127.0.0.1
server 10.69.2.1
server 10.69.2.2

E.4.5 Syslog configurations

/etc/syslog.conf

...snip...
*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none  @10.69.160.1
*.info;authpriv,kern.debug  @10.69.160.1
...snip...
### E.4.6 SNMP configurations

```
/etc/snmpd.conf

read-only community snow
read-write community feed
# Adjust the local system information
system contact "Chirag"
system location "<SITE>"
system services 74
```

### E.4.7 Services configurations

```
/etc/rc.conf.local

ntpd_flags=""
ipsec=YES
snmpd_flags=""
isakmpd_flags="-K"
bgpd_flags=""
```