Type Name

Sequence Comment

Action L3 Protocol

Source IP Address Source L4 Port(s)

Destination IP Address Destination L4 Port(s)

Additional Parameters

-------------------------------------------------------------------------------

IPv4 Network\_Team\_Access

1 ALLOW SSH, HTTPS AND SNMP FROM ADMIN PCS, BLOCK ALL OTHERS

10 ALLOW NETWORK TEAM DESKTOPS

11

permit tcp

10.80.211.23

any = ssh

12

permit tcp

10.80.211.23

any = https

13

permit tcp

10.80.211.40

any = ssh

14

permit tcp

10.80.211.40

any = https

15

permit tcp

10.80.211.77

any = ssh

16

permit tcp

10.80.211.77

any = https

20 ALLOW NETWORK TEAM VMS

21

permit tcp

10.80.152.7

any = ssh

22

permit tcp

10.80.152.7

any = https

23

permit tcp

10.80.152.11

any = ssh

24

permit tcp

10.80.152.11

any = https

25

permit tcp

10.80.152.133

any = ssh

26

permit tcp

10.80.152.133

any = https

30 ALLOW ORION

31

permit tcp

10.80.2.60

any = ssh

32

permit tcp

10.80.2.60

any = https

33

permit udp

10.80.2.60

any = snmp

34

permit udp

10.80.2.60

any = snmp-trap

40 DENY SSH

41

deny tcp

any

any = ssh

Hit-counts: enabled

50 DENY HTTPS

51

deny tcp

any

any = https

Hit-counts: enabled

60 DENY SNMP

61

deny udp

any

any = snmp

Hit-counts: enabled

62

deny udp

any

any = snmp-trap

Hit-counts: enabled

90 ALLOW ANYTHING ELSE

91

permit any

any

any

-------------------------------------------------------------------------------

IPv4 Test

10

deny tcp

10.80.211.23

10.80.119.175 = ssh

20

permit any

any

any

-------------------------------------------------------------------------------

IPv4 vl2-fileserver

10

permit any

10.95.9.9

10.80.2.219

14

permit tcp

any

10.80.2.219 = rdp

20

deny any

any

10.80.2.219

30

permit any

any

any