Table: ACLs sample configurations

Action - ALLOW	
Tasks	**Steps**
Create an extended ACL rule to allow a particular host to access the servers.	>add ns acl allow-client ALLOW -srcIP = 40.40.40.1 Done
Create an extended ACL rule to allow a particular network to access the servers.	>add ns acl allow-client-net ALLOW -srcIP = 40.40.40.0-40.40.40.255 Done
Create extended ACL rules to allow HTTP, TFTP, and ICMP traffic.	>add acl allow-http ALLOW -protocol tcP -destport 80 Done >add acl allow-tftp ALLOW -protocol udp -destport 69 Done >add acl allow-icmp ALLOW -protocol icmp Done
Create an extended ACL rule to allow access to a particular destination/network.	>add acl allow-dest-access ALLOW -destip 20.20.20.0-20.20.20.255 Done
Create an extended ACL rule to allow traffic coming from a particular VLAN.	>add acl allow-vlan ALLOW -vlan 3000 Done
Action - DENY	
Tasks	**Steps**
Create an extended ACL rule to deny access to the servers by a particular host.	>add ns acl deny-client DENY -srcIP = 50.50.50.1 Done
Create an extended ACL rule to deny access to the servers from a particular network.	> add ns acl deny-client-net DENY -srcIP = 50.50.50.0-50.50.50.255 Done

Create extended ACL rules to deny Telnet and FTP traffic.	>add ns acl deny-client-Telnet DENY -protocol TCP -destPort 23 Done > add ns acl deny-client-FTP DENY -protocol TCP -destPort 20-21 Done
Create an extended ACL rule to deny TCP traffic to port 80 from a particular host/network.	>add ns acl deny-client-TCP DENY -protocol TCP -destPort 80 -destIP 20.20.20.0-20.20.20.255 Done
Create an extended ACL rule to deny traffic from a particular VLAN.	> add acl deny-vlan DENY -vlan 2000 Done
Action - BRIDGE	
Tasks	**Steps**
Create an extended ACL rule to bridge FTP traffic.	>add ns acl bridge-ftp BRIDGE -protocol TCP -destport 21 Done >add ns acl bridge-ftp-data BRIDGE -protocol TCP -destport 21 Done
Create an extended ACL rule to bridge all traffic from a particular VLAN.	>add ns acl bridge-client-vlan BRIDGE -vlan 1000 Done
MAC Address Filtering	
Tasks	**Steps**
Create an extended ACL rule to allow traffic from a particular MAC address to a particular host.	>add ns acl allow-mac-host ALLOW -srcMAC 2a:c1:69:92:a0:7b -destIP 10.10.10.1 Done
Create an extended ACL rule to allow traffic from hosts with a specific MAC UUID.	> add ns acl allow-mac-uuid ALLOW -srcMAC 2a:c1:69:92:a0:7b -srcMacMask 000000111111 Done

ACL with RNAT (Typically, RNAT is used to allow servers configured with private non-routable IP addresses to initiate connections to the Internet.)	
Tasks	**Steps**
Create an RNAT rule for a particular host.	>add ns acl rnat-acl-host ALLOW -srcIP 40.40.40.1 Done >apply ns acls Done >set rnat rnat-acl Done
Create an RNAT rule for a particular network.	>add ns acl rnat-acl-network ALLOW -srcIP 40.40.40.0-40.40.40.255 Done >set rnat rnat-acl-network -NATIP 5.5.5.1 Done
ACL with Forwarding Session	
Create a forwarding session rule for a case in which a client request forwarded to a server results in a response that has to return by the same path.	>add ns acl forward-acl-host ALLOW -srcIP 20.20.20.1 Done >add forwardingSession fs -aclname forward-acl-host Done