How to configure reflexive access lists

This post describes how to configure reflexive access lists on your router. Reflexive access lists provide the ability to filter network traffic at a router, based on IP upper-layer protocol "session" information. **?Lab Topology?**

?Lab Object? Technical characteristics: *1.* Reflexive Access List allows for IP packet-filter on the basis of high-level session. *2.* Use the Reflexive Access List to allow for the outbound traffic and block the inbound traffic generated by the external network in order to protect our network. *3.* Reflexive Access List will be generated temporarily when the traffic are generated, the items will be cleared after finishing session *4.* Reflexive Access List is nested in an extended name access list instead of applying to some interface directly. **?Lab Process? Basic Route:** IN: ip route 0.0.0.0 0.0.0.0 192.168.1.1 OUT: ip route 0.0.0.0 0.0.0.0 218.18.1.1 *1.* Use the basic access list GW(config)#access-list 101 permit tcp any any established GW(config)#interface s0/0 GW(config-if)#ip access-group 101 in Thus, you can telnet the outside from the inside but can't telnet inside from the outside. Because the TCP packet matching with the establish field *2.* The configuration steps of Reflexive Access List: First, use NO to deny all the above basic access lists and access-group GW(config)#ip access-list extended ACLOUT GW(config-ext-nacl)#permit tcp any any reflect REF GW(config-ext-nacl)# permit udp an an reflect REF GW(config)#ip access-list extended ACLIN GW(config-ext-nacl)#evaluate REF GW(config)#interface s0/0 GW(config-if)#ip access-group ACLOUT out GW(config-if)#ip access-group ACLIN in *3.* Test: Telnet the outside router from the inside router, examine the generation of the list on the gateway router. Characteristics of the Reflexive Access List (a) List is in the permit state forever. (b) The list and the original outbound traffic have the same protocol numbers (eg:TCP) (c) The list and the original traffic have the same source addresses, only exchange the source addresses, so do the port numbers. Adjust timeout time. GW(config)#ip reflexive-list timeout 20 Adjust when writing list GW(config)#ip access-list extended ACLOUT GW(config-ext-nacl)#permit tcp any any reflect REF timeout 50 The timeout value is prefered when both are written.