Simple configuration of Context-Based Access Control

Technical characteristics: *1.* Traffic filtering CBAC checks not only the information of the network layer and the transport layer but also the information of the application layer. It can also filter the http traffic and block java plug-in *2.* Traffic monitoring CBAC monitors the traffic passing through the router and handles the TCP and UDP state information which can be used to generate the temporary list to release the rebound traffic and other traffic allowed. *3.* Alert and audit *4.* Intrusion Prevention **?Lab Topology?**

?Lab Process? *1.* Configuration of GW GW(config)#ip inspect alert-off GW(config)# ip inspect audit-trail GW(config)#ip access-list ex ACLIN GW(config-ext-nacl)#permit ospf any any GW(config)# ip inspect name CBAC tcp alert on audit-trail off / *Switch for some protocol alert and audit* GW(config)# ip inspect name CBAC udp GW(config)# ip inspect name CBAC ftp GW(config)#ip inspect name CBAC icmp / *The higher version can inspect ICMP without releasing ICMP on the external interface* GW(config)# ip inspect name CBAC http java-list 2 urlfilter GW(config)#access-list 2 deny 218.18.1.0 0.0.0.255 GW(config)#access-list 2 permit any GW(config)#interface s0/0 GW(config-if)#ip access-group ACLIN in GW(config-if)#ip inspect CBAC out

- Adjust the values of timeout and threshold: ip inspect tcp synwait-time *seconds* - The default time is 30 seconds, if a TCP connection is not established within this time, this connection will be dropped out. - ip inspect tcp finwait-time seconds - The default time is 5 seconds, if a TCP connection is not established within this time, this connection will be dropped out. ip inspect tcp idle-time *seconds* - The default time is 3600 seconds. ip inspect udp idle-time *seconds* - The default time is 30 seconds. Monitor the UDP traffic and release the rebound UDP traffic within 30 seconds. ip inspect dns-timeout *seconds* - The default time is 5 seconds. The DNS query time. ip inspect max-incomplete high *number* - The default number is 500. If the number exceeds 500, the original Half-open connection will be deleted. ip inspect max-incomplete low *number* - The default number is 400. Stop deleting if the number is lower than 400. ip inspect one-minute high *number* - The default number is 500. Begin to delete the original Half-open connections when the new connection number is up to 500 within a minute. ip inspect one-minute low *number* - The default number is 400. Stop deleting the original Half-open connections when the new connection number is lower than 400 within a minute. ip inspect tcp max-incomplete host *number* block-time *minutes* - Control the number of the half-open connections based on the single host, the default is host 50 block-time 0. - block-time = 0, if the TCP half-open connection number based on the single host exceeds the configured value, the oldest half-open connections will be cleared when there are new connection requests. - block-time >0, when the TCP half-open connection number based on the single host exceeds the configured value, clear all the original half-open connections if there are new connection requests and block all the new connection requests within the block-time. *2.* Test: Telnet the outside router form the inside router and examine the generation of the list on the gateway router. show ip access-list show ip inspect config show ip inspect all show ip inspect sessions detail Configure logging: GW(config)#logging host 192.168.1.254 GW(config)#logging trap informational GW(config)#no ip inspect / *Close CBAC and clear CBAC configurations*