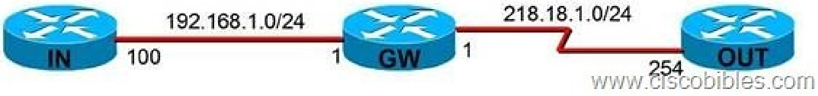
CCSP SNRS Lab5 - TCP Intercept

?Lab Topology?



?Lab Object? Technical characteristics: *1*?The feature of TCP Intercept is used to protect TCP Server from being attacked by TCP-SYN flood, this attack is also called DOS attack. *2.* TCP Intercept has two modes: active intercept mode and passive watch mode. (1) In intercept mode, the router will substitute the destination server to establish three-way handshake with the client, after connecting successfully, it will replace the client to connect to the server. At last, combine the two connections. (2) In watch mode, the router only monitors the process of establishing TCP passively, if the connection is not established within the specified time, the connection will be stopped. **?Lab Process?** GW(config)#access-list 101 permit tcp any host 192.168.1.100 GW(config)#ip tcp intercept list 101 GW(config)#ip tcp intercept mode watch &#160; [k1] GW(config)#ip tcp intercept watch-timeout 20&#160;&#160; [k2] GW(config)#ip tcp intercept connection-timeout 5&#160; [k3] The following four parameters are to configure when enter and exit the aggressive mode. After entering the aggressive mode ? Each new connection will lead to deleting the old connection.(or delete any connection by adjusting the following commands) GW(config)#ip tcp intercept drop-mode random [k4] ? In watch mode, the watch timeout time will be half reduced. GW(config)#ip tcp intercept max-incomplete high 1000 [k5] GW(config)#ip tcp intercept max-incomplete low 800 [k6] Enter the aggressive mode when the number of the half-open connection exceeds high and exit when the number of the half-open connection is below the low. GW(config)#ip tcp intercept one-minute high 1000 [k7] GW(config)#ip tcp intercept one-minute low 800 [k8] Enter the aggressive mode when the new connection request number exceeds the high and exit when the number is below the low. [k1]The default is the intercept mode [k2]In watch mode, if the TCP connection has not established within this time, then clear all the existing connections. The default is 30s [k3]Only in Intercept mode, the value of connection-timeout will function, that is the IDLE time of the TCP session. [k4]The default is the oldest. [k5]The default is 1100 [k6]The default is 900 [k7]The default is 1100 [k8]The default is 900