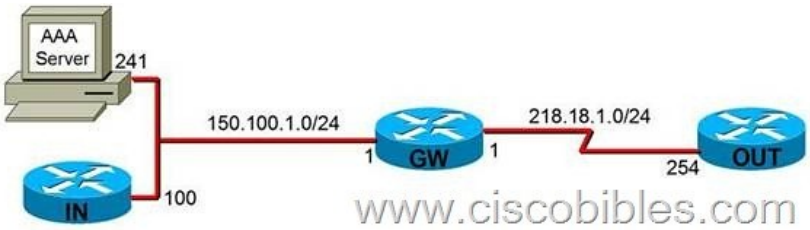
CCSP SNRS Lab7 - IOS IDS

?Lab Topology?



?Lab Object? Technical characteristics: *1.* IOS IDS is an in-line intrusion sensor and scan each packet crossing the router which matches any one of these signatures. *2.* When discovering suspicious activities, you can take the following actions: (1) alarm?send alarm to syslog server or Cisco Secure IDS Director (2) Drop?Drop this packet (3) Reset?reset this TCP connection(but it will continue to forward this packet, so it is recommended to perform forwarding and dropping simultaneously), when IOS IDS is enabled, IOS Firewall will be enabled automatically. Some parameters will function at this time. For example: ip inspect max-incomplete high ip inspect max-incomplete low ip inspect one-minute high ip inspect one-minute low **?Lab Process?** *1.* Configuration of GW. GW(config)#ip audit smtp spam 20 [k1] GW(config)# ip audit notify nr-director [k2] GW(config)#ip audit notify log [k3] GW(config)#ip audit name MYIDS info action alarm GW(config)#ip audit name MYIDS attack action alarm drop reset GW(config)#inter s0/0 GW(config-if)#ip audit MYIDS in GW(config)#logging 150.100.1.241 GW(config)#logging trap informational GW(config)#ip audit po local hostid 10 orgid 1000 GW(config)#ip audit po remote hostid 11 orgid 1000 rmtaddress 150.100.1.241 localaddress 150.100.1.1 GW(config)#config-register 0x2102 GW#wr GW#reload *2.* Test: Create alarm system on syslog server to check the alarm information. GW#ping 218.18.1.254 GW#ping 218.18.1.254 size 1025 show ip audit all show ip audit statistics clear ip audit configuration [k4] [k1]The maximum number of e-mail receivers, the default is 250 [k2]Send log to director [k3]Send log to syslog server [k4]Disable IDS and clear all IDS configurations.