CCSP SNRS - Lab6 Authentication Proxy

?Lab Topology?

?Lab Object? Technical characteristics: *1.* Similar to PIX cutthrough technology, Auth-proxy can authenticate and authorize the traffic passing through the router. *2.* Auth-proxy working process When a user initializes http session crossing a router, auth-proxy will be triggered. Then it is required to input the user name and the password. After the success of the authentication, the user can obtain an authorized profile form the AAA server. Authentication proxy uses this profile to establish dynamic access list items and add them into the access list of the interface. **?Lab Process?** GW(config)#aaa new-model GW(config)#aaa authentication login noau line none GW(config)#line con 0 GW(config-line)#login authen noau GW(config)#line aux 0 GW(config-line)# login authen noau GW(config)#line vty 0 4 GW(config-line)# login authen noau GW(config)#tacas-server host 150.100.1.241 GW#test aaa group tacacs+ auth.proxy cisco new-code GW(config)#aaa authentication login default group tacacs+ GW(config)#aaa authorization auth-proxy default group tacacs+ GW(config)#ip http server GW(config)#ip http authentication aaa GW(config)#ip http access-class 1 GW(config)#access-list 1 deny any GW(config)#ip access-list ex ACLIN GW(config-ext-nacl)#permit tcp host 150.100.1.241 eq tacacs host 150.100.1.1 GW(config)#ip auth-proxy name AUTH http GW(config)#inter e0/0 GW(config-if)#ip access-group ACLIN in GW(config-if)#ip auth-proxy AUTH OUT(config)#username cisco privilege 15 password cisco OUT(config)#ip http server OUT(config)#ip http authentication local Configure authentication and authorization on the AAA server. *1.* Click TACACS+ (Cisco) under the Interface Configuration mode. *2.* Establish a new service name: auth-proxy *3.* Authenticate in user or group mode: *4.* Tick the established auth-proxy and write as follows: Priv-lvl=15 proxyacl#1=permit tcp any any proxyacl#2=permit udp any any The privilege level must be set to 15 for all users. *5.* Proxyacl is the list to be dynamically created after authorization. Only use the permit sentence: The source address must be any. *6.* Test: When accessing http://218.18.1.254 on the AAA server, it is required to input the user name and the password on the gateway router. After the success of the authentication, the user can access the out routers. Use the following commands to check auth-proxy on the gateway router. show ip access-lists show ip auth-proxy configuration show ip auth-proxy cache clear ip auth-proxy cache {* | host ip address}   [k1] [k1]Clear cache