**CCNA 3 Lab 3c / Configuring ACLs / Lab Manual**

**Block a slacker from using Facebook on the job**

Introduction: You are a team of network engineers working at the company called ABC.

# Company ABC has a User LAN

# Company ABC has a Server Farm LAN that holds company ABC’s websites and web services.

# The main router in the company has three interfaces. Each interface does the following:

* Router interface Gig 1/0/1 is the default gateway of the Server Farm LAN
* Router interface Gig 0/0/0 is the default gateway of the ABC User LAN
* Router interface Gig0/0/1 is the external interface that is connected to the internet.

On the internet there are four different hosts:

* 8.8.8.8 is a DNS server that can be reached over the internet
* Cisco.com web server
* facebook.com web server
* The outside PC1 is a customer of ABC

**Task 1 enforce productivity)** Inside user on PC2 has been caught slacking, he is visiting facebook.com instead of doing the work he was hired to do. The company would like you to create an ACL on Router1 that will prevent the user on PC2 from accessing the Facebook server, then apply the ACL to the Default Gateway interface of Router 1’s ABC user LAN to make the ACL active. **PC2 is allowed to ping the FB server but he must be blocked from loading the web page in his browser**.

Open the web browser on PC2 and go to facebook.com - notice that the Facebook web page loads (confirm).

Use the following commands to complete Task 1:

A-) Log into router 1 and create ACL 100 for blocking Facebook. Add the ACE (access control entry) "deny" statement in ACL 100 to block PC2 from accessing facebook on port 80 **\*put the correct wild card mask in the command / user your wild card mask cheat sheet - remove the brackets and just put the number down\* : hint look at FB’s subnet mask slash value then check your cheat sheet…**

**Router Commands:**

en

config t

access-list 100 deny tcp host 10.1.2.102 8.8.8.10 (wild-card-mask/32) eq 80

access-list 100 permit ip any any **\* NOTE YOU NEED TO add this command at the end of every ACL that you create as there is an invisible “deny ip any any” ACE at the bottom of every ACL, that causes the ACL to block all traffic after doing the rule check. Putting a permit ip any any before the invisible dney statement will cancel out the invisible deny statement.**

do the command show access-list to view the access list and the ACEs inside of the ACL. Or use the command show access-lists # to home in on the ACL number that you created.

B-) Apply ACL 100 to Router 1's LAN1 interface. ACLs must be applied to a router interface in order for the ACL to begin inspecting packets. When the router sees traffic that matches an ACE entry in the ACL the router will “permit” or “deny” the traffic depending on how you crafted your ACE statement. In this case you created a deny statement, so it will perform a block action.

**Router Commands: Apply the ACL to the routers1’s user LAN interface**

Config t

int gi0/0/0

ip access-group 100 in

**NOTE: We chose the key word in, in the command above because from the perspective of the router, traffic is flowing “into” the router from user LAN 1.**

#The ACL that you created is now in effect, the second you bind the ACL to an interface in starts to inspect IP traffic.

#Use the show run command to review interface gi0/0/0 and find your ACL config in the running-config…

C-) Log into Inside PC2 and try accessing Facebook.com via the web browser. Notice that it does not work (try several times for good measure). Try browsing to cisco.com, it works because we did not put cisco.com’s IP in the ACL, we only specified the Facebook server’s IP address. Now go back into the router and run the command show access-lists or show access-lists # (the number of your ACL). You will notice that the ACE entries are taking hits, this means that the router is tracking each time the network packets match your ACE. **Take a screenshot of the ACL hits as evidence that you have completed Task 1 enforce productivity)**

**Freelance:**

Everything in this network environment can ping each other. Try playing around with ACLs and see what kind of access rules you can create. Make a few ACLs and explain their purpose/how they work. Test the functionality of the ACLs you create by showing the hit count (take a screen shot of the hit count).