

## Cyber Security Lab 5 – Additional Notes

### ACS Server

The Radius server, running the Cisco Access Control Server (ACS) software, is on 192.168.100.110. It is directly available from the console at Sclass5 with the switch labeled “Dead DMV”. Since the video driver on that machine only goes to 800x600, it is probably better to access it remotely from one of the other machines.

The ACS administrative interface shows up through a web interface, <http://192.168.100.110:2002>. Enter user name “root” and password “class-test”. You can look at user definitions. The ACS client definitions (the routers) show up under the network tab. There is also a reports tab. I have not looked at this with traffic. I would be interested to here what is there. It could be that we are not enabled enough accounting/auditing to generate interesting reports, but it would be interesting to know.

You should not need to change the values in the ACS server unless you want to play with group authorization.

### VPN Client

I installed the VPN client software on the windows images on sclass2 and sclass3. Each installation has a vpn client profile installed. For sclass2, it is called “to rtr1”, and for sclass3, it is called “to rtr4”. You want to configure the tunnel to the peer router so the tunneled traffic goes across the pre-out network, so you can see the packets with the sniffer on sclass5.

### Router Configuration for Part 2

There are a couple changes and additions to the lab writeup for the configuration of the router for part 2.

1. When defining the local IP pool, the addresses must **not** be the same as the target network. For example, if rtr1 is terminating the tunnel, the IP pool addresses cannot be in the 192.168.1.0/24 network. Something in the 192.168.10.0/24 network would work. *Extra points if you can explain why this is the case in your lab writeup.*
2. One you enter the “aaa new-model” command, the router will expect to have a local administrative user defined. Enter “username root password 0 class-test” to define an administrative user root with password class-test. When telneting in, you will be prompted for both a user name and password.
3. “Debug AAA authentication” is also a useful value to look at for logging and debugging.