Instructor Notes for the VPN Scenario
September 2006

Students should be provided with the "CyberCIEGE VPN Scenario Lab Manual".

The VPN scenario introduces basic concepts of using VPNs to authenticate communications and to protect the secrecy of communications over packet switched networks. The scenario is divided into two phases:

- Phase 1: Students must deploy VPN gateways to authenticate modifications to moderately valuable assets.

- Phase 2: Students must protect high value assets using high assurance VPN gateways.

Solution steps:

The student lab manual largely describes the solution steps.

Getting Student's Started
Students should be provided with a copy of the "CyberCIEGE VPN Lab Manual". This scenario is intended to follow the "Link Encryptor" scenario.

Student Assessment
Student progress and results can be assessed using the Campaign Analyzer. From the CyberCIEGE desktop folder, select the "ccse" directory and then start the "Campaign Analyzer". It defaults to the "Starting Scenarios" campaign. Use the "Select" button to select the "Encryption" campaign. Select the "VPN Scenario". Each student that has played the game will appear in the list, along with summary status. If the student did not "win" the game, the status identifies the most advanced phase the student had reached. To view details of a student's play, select that student entry and press the "View Log" button.