Instructor Notes for the DMZ Scenario
May 2013

Students are expected to have completed the Network Filters scenario

The scenario is intended to illustrate the use of a DMZ to protect internal systems, including internal email servers, from attack by deploying externally accessible email servers to a DMZ. The scenario also requires deployment of a web server to the DMZ and permitting that web server to access an internally located database server.

The first phase requires the player to permit web access from the company. The initial filter settings block this access. The player need not make any other changes to advance to the next phase – but players may not know that and may start making defensive choices.

The second phase requires the player to allow a remote user (Bev) to send email to one of the users in the main office (Ann). The initial filter blocks email from the Internet. The enterprise server has an email application that will always have a flaw leading to a compromise as long as it is exposed to the Internet. Even if the player adjusts patch management, compromises will continue. If the player conducts a "Discovery / Scan" function, the resulting report will show the vulnerable email application.

The player is given hints to create a DMZ and the encyclopedia is taken to a page that describes how. The player must deploy a second router and a second email server. The second email server should be configured as a "proxy" for the enterprise server. The outer router filter should allow all inbound email and the inner router filter should restrict inbound email traffic to only that originating from the proxy.

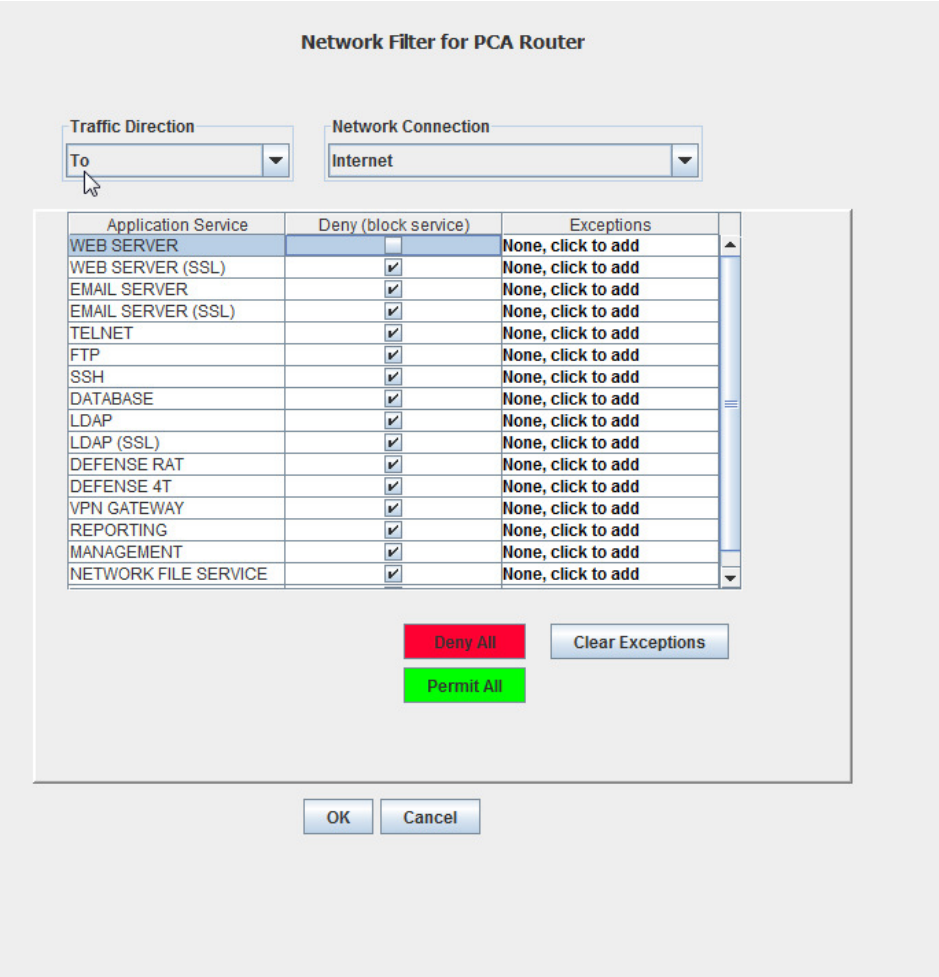
The player might attempt to avoid deploying a DMZ by limiting incoming email to the remote user's SMTP server. However the scenario will rename the SMTP server, thereby breaking the player's filter exception. If the player persists, the scenario will be lost. Similarly, the player might choose to encrypt the email. However the scenario will launch denial-of-service attacks on the server if it is exposed to the Internet and the objective will not complete.

In the third phase, a remote user must access a web page that is backed by a database asset. If the player permits web traffic into the internal server, then flaws in its web server application will expose assets. The player must buy a web server for the DMZ, move the web page onto the new web server, and then permit database traffic from the DMZ into the internal server.

Note that wiretaps and spoofing attacks are not present in this scenario, otherwise the player would be required to enable SSL for the web page to ensure remotely supplied passwords are encrypted. The player may not have yet played the encryption scenarios to learn about PKI and SSL, and so those attacks do not occur.

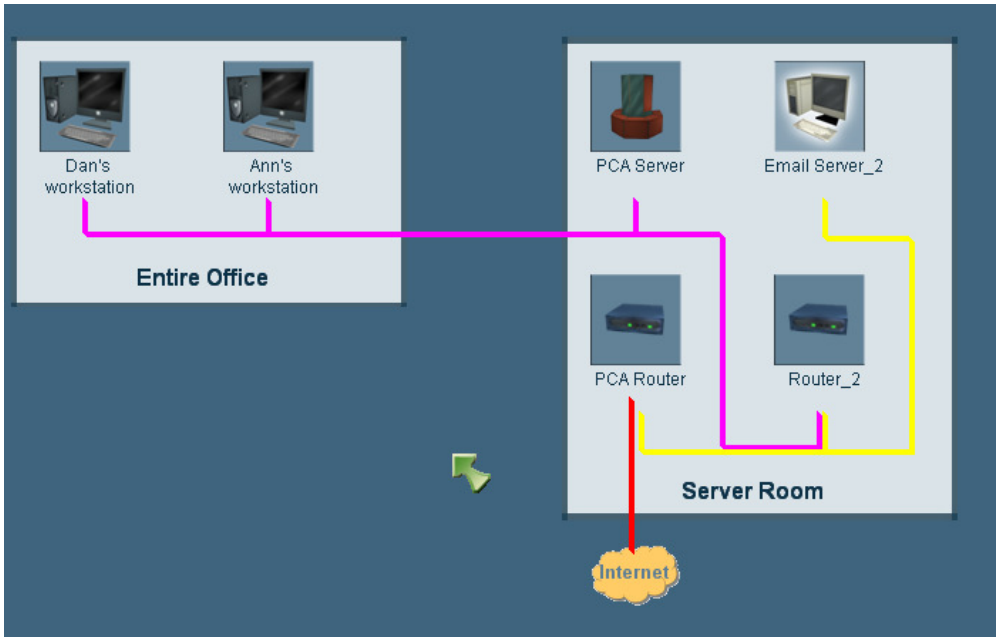
Solution:

Phase 1: Configure the PCA Router to permit web traffic "To" the Internet. Right click on the PCA Router (e.g., in the NETWORK screen) and select "Network Filters".

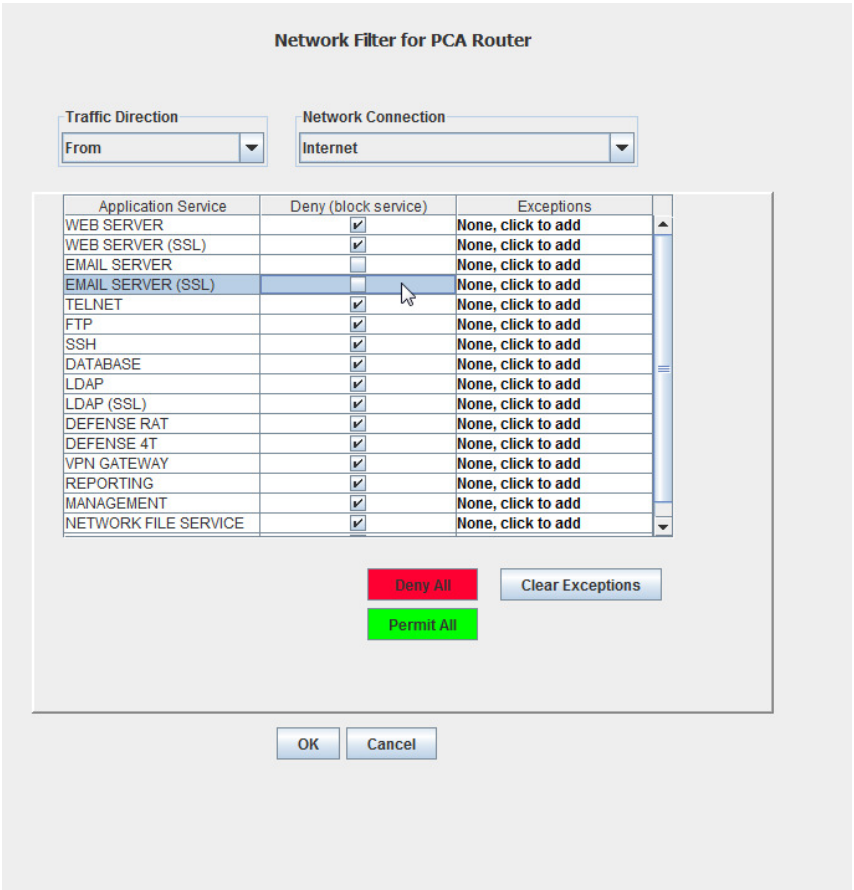


Run until you reach the next phase.

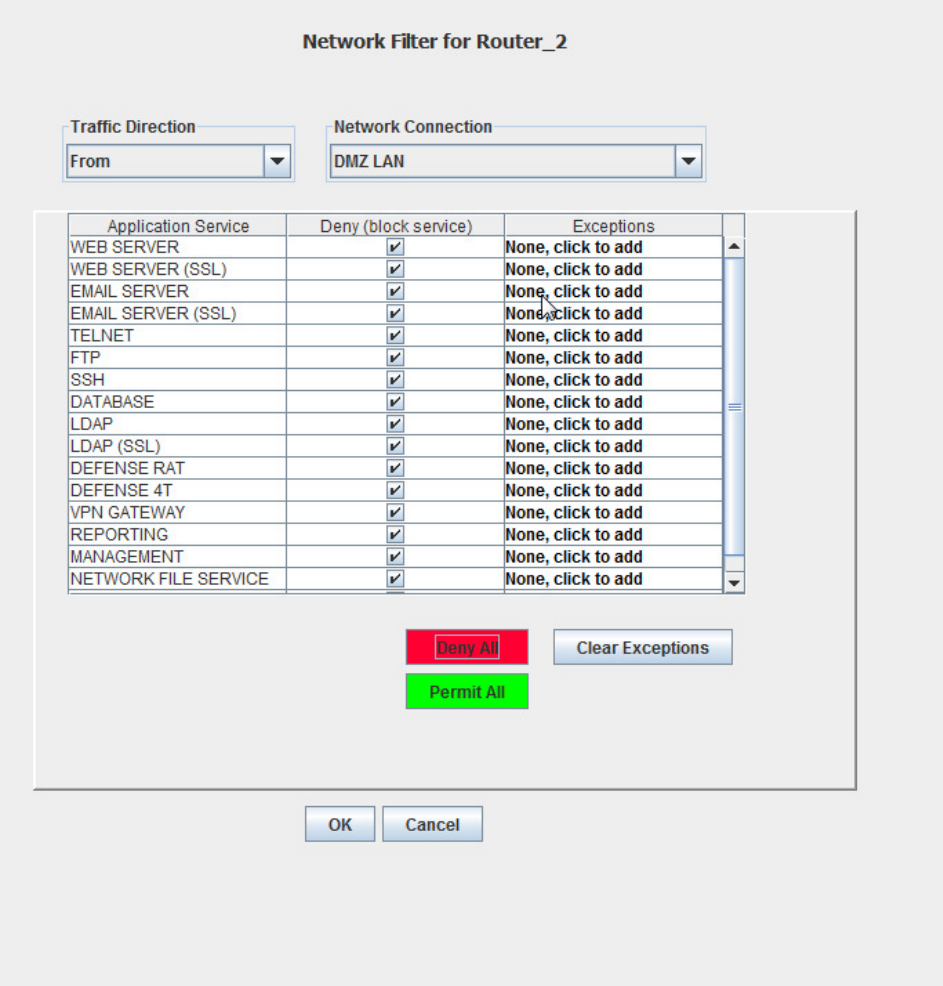
Phase 2: Run briefly and note the complaint about email from Bev. Open the EMAIL SERVER port "From the Internet" on the PCA Router. Run until you get attacked. Right click on an Internet Icon in the Network screen and run a scan on the PCA server. Note that you can now see the Email Server application, and it is unpatched. Configure the PCA Server for patch management. Run the scan again and note it has the latest patch. Unpause the scenario and run until another attack. Press F1 to learn about DMZs. Buy a router and an email server for the Entire Office; connect them per the encyclopedia entry, leaving the PCA Router as the outer router and using the DMZ LAN as the DMZ LAN. The topology should look like:



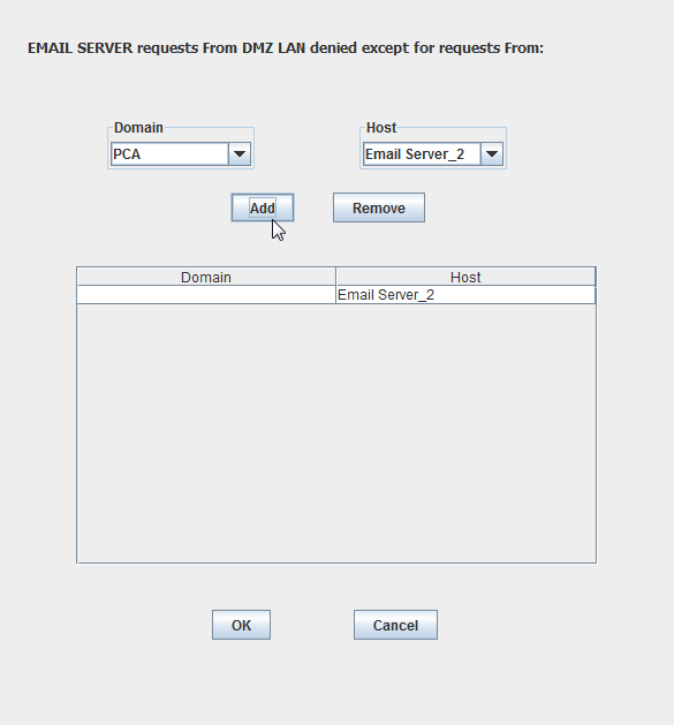
Configure the PCA router to allow email & email SSL from the Internet. .



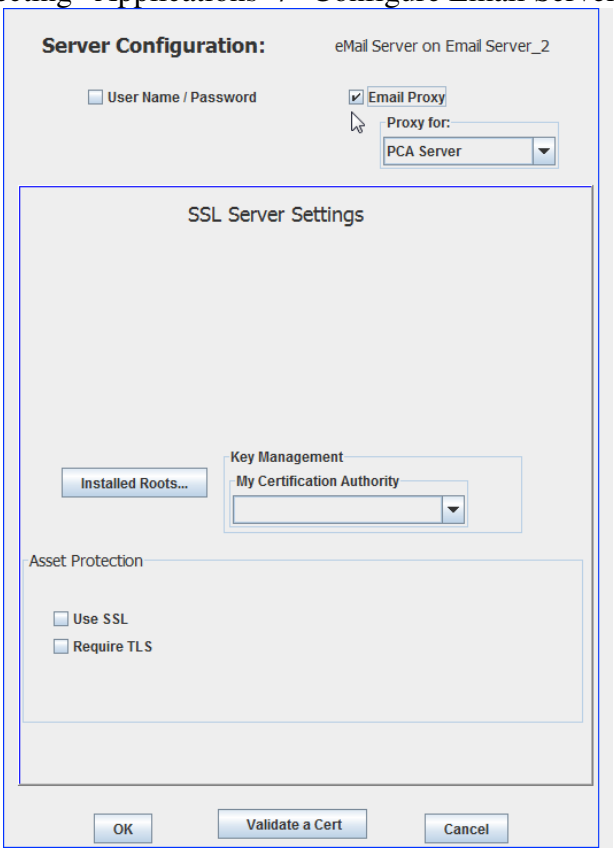
Configure the inner router to deny all traffic from the DMZ LAN.



Add exceptions for email and email SSL traffic from the new email server by clicking on the Exceptions column for each service.

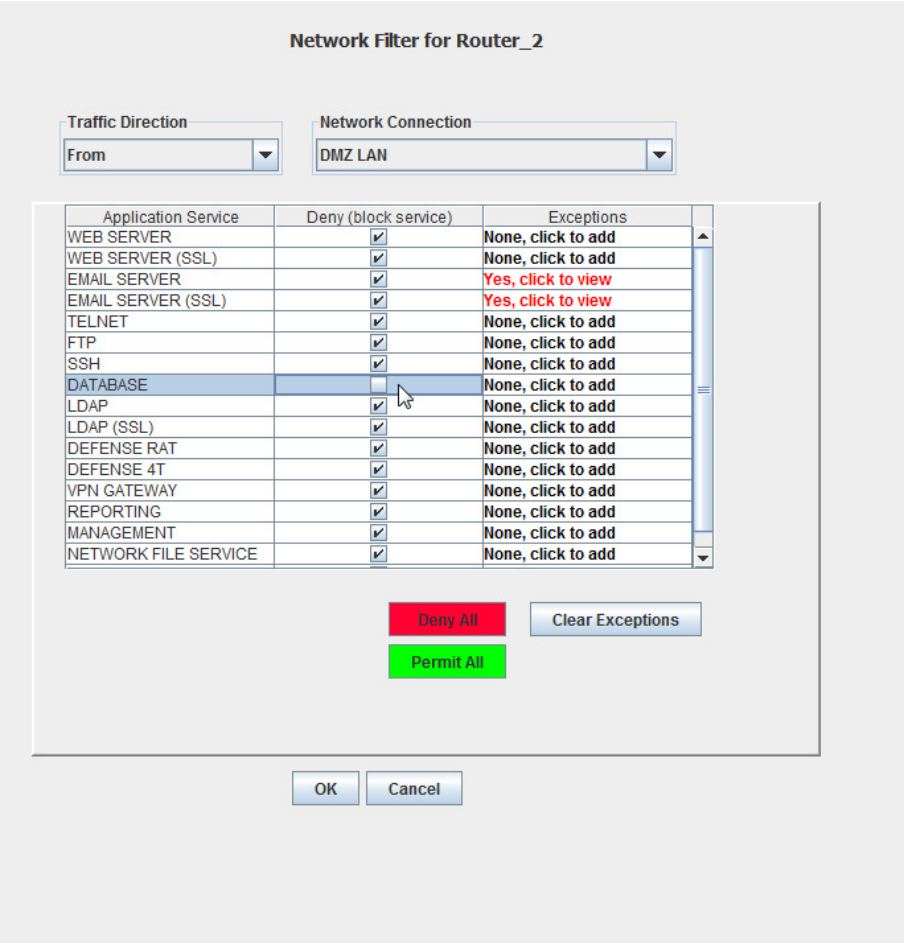


Configure the new email server to act as a proxy by right clicking on it and selecting “Applications” / “Configure Email Server”.

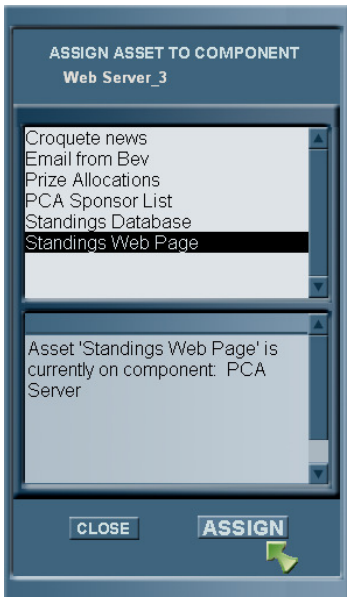


Configure the new email server to use regular or automatic patch management. Run the scenario and answer the question.

Phase 3: Run until Bobby Jack complains. Open the Web Server and Web Server SSL ports "From the Internet" on the PCA router, and "From the DMZ" on the inner router. Run until you get attacked. Look at the Attack Log, and run a scan on the PCA Server. Note how you can now see the Web Server application because the ports are open. Buy a web server and connect it to the DMZ LAN. Alter inner router traffic from the DMZ to deny Web Server and SSL (what you had previously allowed), and to permit DATABASE traffic From the DMZ.



Right click on the new web server and move the standings web page asset to the web server.


ASSIGN ASSET TO COMPONENT
Web Server_3
Croquete news
Email from Bev
Prize Allocations
PCA Sponsor List
Standings Database
Standings Web Page
Asset 'Standings Web Page' is currently on component: PCA Server
CLOSE
ASSIGN

Run and win.