Database server security demands opnet ilab

As you can see, all of the four permitted demand flows conform to the Security Policy. Use to capture the Conformance web report and use V to paste it into your lab document. Click on Violations and notice that the denied database traffic is reaching the Attack PC. Use to capture the Violations web report and use V to paste it into your lab What is needed to bring the network into compliance with the Security Policy? Explain. Unordered to bring the network into compliance with security policy they both have to be defined.

After they are defined then setup network automation and scans of the system that will detect violations. Once the violations have been detected they must e prioritize and reanimated. Policy f enforcements must also be in placed to ensure that the network in in compliance with the security policy. Press . Enter configure terminal command to go into global configuration mode. From global configuration mode, create the necessary CAL and apply it to the OF/O interface using the commands shown below.

It shows any Calls that are impacting protected traffic. Use to capture the Configurations web report and use V to paste it into your lab document. Notice that there is no Violations option. Open the Conformance report and verify that all of our Security Policy demands have been met. Use to capture the Conformance web report and use V to paste it into your lab document. Expand the Object Tables tree. Select Public Server -> Attack PC DB and Security Demand Routing. No Database traffic is allowed to the Attack PC, it is filtered by CAL 100.

Use to Capture the Security Demands Routing web report and use V to paste it into your lab document. Select the commands you entered in the Virtual CLIP using the mouse and click on the Copy button. Use V to paste the commands into your Lab Document. Then close Virtual CUE. Enter configuration commands, one per line.