IAM3 — IAM3 TASK 1: SECURE NETWORK DESIGN

SECURE NETWORK DESIGN — C700
PRFA — IAM3

TASK OVERVIEW SUBMISSIONS EVALUATION REPORT

EVALUATION REPORT — ATTEMPT 1 — REVISION NEEDED

Overall Evaluator Comments

EVALUATOR COMMENTS

You have successfully described multiple network security and infrastructure problems with Company A, including the Cisco PIX 515E firewall being obsolete. Please see comments in the report below about revisions needed.

A. Company A’s Network Problems

Competent The submission accurately describes Company A’s security and infrastructure problems. The submission includes appropriate details of the network security and infrastructure problems found in the attached “Company A Organizational Chart,” “Company A Risk Analysis,” and/or “Company A Visio Diagram.”

There are no comments for this aspect.

B. ZenMap and OpenVAS

Competent [Intentionally left blank. Not part of the Assessment]

There are no comments for this aspect.

C. Company B’s Network Problems

Competent The description accurately identifies 2 of Company B’s network security or infrastructure problems and the impact of *each* problem, including logical rationale for why *each* is a network security or infrastructure problem using appropriate details from the Zenmap and OpenVAS outputs.

There are no comments for this aspect.

C1. Correcting Problems and Improvement

Approaching Competence The submission does not logically or accurately explain the potential positive effect(s) of correcting 1 or more of the problems in part C for the functioning of the merged network.

EVALUATOR COMMENTS: ATTEMPT 1

The provided response includes discussions on the use of default authentication on pfSense and port 80 being available on the Linux server. What is unclear are the positive effects of correcting each problem in part C.

D. Merged Network Topology

Approaching Competence The merged network topology diagram using Microsoft Visio or a similar software tool is not accurate or does not represent the merging requirements from the scenario. Or the merged network topology diagram does not remediate *all* existing infrastructure issues described in part A and part C.

EVALUATOR COMMENTS: ATTEMPT 1

The provided response include a merged network topology that includes a an Cisco 5506x ASA and Cisco 2811 router. What cannot be found is a merged network topology diagram that address the merging requirements found in the scenario and remediates all infrastructure issues descried in parts A and C.

E. OSI model and TCP/IP protocol stack layers

Approaching Competence The submission inaccurately identifies the OSI model layer or TCP/IP protocol stack layer for *each* component in the merged network topology diagram.

EVALUATOR COMMENTS: ATTEMPT 1

The response provided includes the accurate identification of the OSI and TCP/IP model layers relevant to multiple components of the merged network topology diagram, including the Windows 10 PCs, remote desktops, and printer. What cannot be found is the accurate identicaiton of the OSI and TCP/IP model layers relevant to each component of an appropriate merged network topology diagram.

F. Justification of Merged Network Topology

Approaching Competence The justification of retaining or deleting 4 existing components does not accurately and logically discuss the retention or deletion of 4 existing components reflected in the candidate's proposed network topology diagram. Or the justification does not logically explain how *each* component's retention or deletion, including any newly required additions to the network as a result of a deletion, addresses *both* the relevant security concerns and budgetary restrictions found in the scenario.

EVALUATOR COMMENTS: ATTEMPT 1

The provided response includes discussions on removing the PIX 515E firewall introducing the Cisco 5506X ASA firewall to replace the PIX 515E. What cannot be found are accurate discussions on the retention or deletion of three additional components from an appropriate merged network topology diagram. What also cannot be found are logical discussions on how newly required additions address the relevant security concerns and budgetary restrictions found in the scenario.

G. Secure Network Design Principles

Competent The explanation accurately identifies 2 secure network design principles and logically discusses how *each* principle is included in the proposed merged network topology diagram.

There are no comments for this aspect.

H. Secure Hardware/Software Components

Competent The explanation accurately describes 2 secure hardware and/or software components that are integrated into the proposed network topology diagram and logically discusses how *each* component will address the security needs of the merged organization.

There are no comments for this aspect.

I. Regulatory Compliance Requirement

Competent The explanation accurately identifies a relevant regulatory compliance requirement and logically discusses how the proposed network topology diagram for the merged organization addresses security safeguards based on the identified regulatory compliance requirement.

There are no comments for this aspect.

J. Integration Problems

Competent The explanation accurately describes 1 security threat and 1 potential network problem that would become a risk as part of the implementation of the proposed network topology diagram and logically discusses the risks *each* would pose, including a logical rationale for why *each* would become a risk.

There are no comments for this aspect.

J1. Managing or Mitigating Integration Problems

Approaching Competence The submission does not logically explain how *both* the security threat and potential network problem from part J should be managed or mitigated, or a method of management or mitigation proposed is not logical as part of the implementation of the proposed topology diagram.

EVALUATOR COMMENTS: ATTEMPT 1

The response provided includes discussions on lack of network redundancy being a security threat and cutting of network cables being a network problem. What is unclear are logical explanations of how both the security threat and potential network problem are to be managed and mitigated.

K. Sources

Competent The submission includes in-text citations for sources that are properly quoted, paraphrased, or summarized and a reference list that accurately identifies the author, date, title, and source location as available.

There are no comments for this aspect.

L. Professional Communication

Competent Content reflects attention to detail, is organized, and focuses on the main ideas as prescribed in the task or chosen by the candidate. Terminology is pertinent, is used correctly, and effectively conveys the intended meaning. Mechanics, usage, and grammar promote accurate interpretation and understanding.

There are no comments for this aspect.