# Experiential Learning Portfolio for 10151101 Firewall and VPN Management

**Student Contact Information:**

Name: ______________________________________ Student ID#: ____________________

Email: ______________________________________ Phone: ________________________

Before attempting to complete this portfolio, the following prerequisites and/or corequisites must be met: PREREQUISITE: 10150113 Cisco CCNA 2 Routing and Switching Essentials

## Directions

Consider your prior work, military, volunteer, education, training and/or other life experiences as they relate to each competency and its learning objectives. Courses with competencies that include speeches, oral presentations, or skill demonstrations may require scheduling face-to-face sessions. You can complete all of your work within this document using the same font, following the template format.

1. Complete the Student Contact Information at the top of this page.
2. Write an Introduction to the portfolio. Briefly introduce yourself to the reviewer summarizing your experiences related to this course and your future goals.
3. Complete each "Describe your learning and experience with this competency" section in the space below each competency and its criteria and learning objectives. Focus on the following:
   - What did you learn?
   - How did you learn through your experience?
   - How has that learning impacted your work and/or life?
4. Compile all required and any suggested artifacts (documents and other products that demonstrate learning).
   - Label artifacts as noted in the competency
   - Scan paper artifacts
   - Provide links to video artifacts
   - Attach all artifacts to the end of the portfolio
5. Write a conclusion for your portfolio. Briefly summarize how you have met the competencies.
6. Proofread. Overall appearance, organization, spelling, and grammar will be considered in the review of the portfolio.
7. Complete the Learning Source Table. Provide additional information on the business and industry, military, and/or volunteer experiences, training, and/or education or other prior learning you mentioned in your narrative for each competency on the Learning Source Table at the end of the portfolio. Complete this table as completely and accurately as possible.

The portfolio review process will begin when your completed portfolio and Credit for Prior Learning Form are submitted and nonrefundable processing fees are paid to your local Credit for Prior Learning contact. Contact Student Services for additional information.

Your portfolio will usually be evaluated within two weeks during the academic year; summer months may be an exception. You will receive an e-mail notification regarding the outcome of the portfolio review from the Credit for Prior Learning contact. NOTE: Submission of a portfolio does not guarantee that credit will be awarded.

You have 6 weeks to appeal any academic decision. See your student handbook for the complete process to appeal.

**To receive credit for this course, you must receive "Met" on 8 of the 9 competencies.**

**10151101 Firewall and VPN Management, 3 Associate Degree Credits**

**Course Description:** This course covers the configuration and management of firewall and VPN technologies. Students will be exposed to products from manufacturers like: CISCO, Palo Alto, Sonic Wall and Check Point. In depth hands-on exercises are used to instruct the student in the related technologies including NAT, PAT, ACL construction, application gateways, stateful packet inspection, application layer and URL filtering. Student will configure and test VPN connection for remote access and site-to-site connections.

PREREQUISITE: 10150113 Cisco CCNA 2 Routing and Switching Essentials

**Introduction:** **Briefly introduce yourself to the reviewer summarizing your experiences related to this course and your future goals.**

**Competency 1: Identify firewall functions**

Criteria: Performance will be satisfactory when:

- you identify types of firewalls
- you identify placement of firewalls
- you identify the use of NAT/PAT
- you identify firewall zones and architecture
- you identify features of a firewall
- you identify capabilities of defense

Learning Objectives:

a. Explain firewall architecture
b. Identify zones
c. Identify the use of NAT and PAT
d. Identify supported firewall features
e. Identify threat types and the use of firewalls as defense
f. Identify firewall placements
g. Identify capabilities to meet security policy

**Required Artifacts: None**
**Suggested Artifacts: Screenshot of firewall meeting criteria in Competency 1**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 2: Configure host based firewalls**

Criteria: Performance will be satisfactory when:

- you setup firewall software
- you configure firewalls to block or allow protocols
- you configure firewalls to block or allow ports
- you configure firewalls to block or allow programs
- you configure firewalls to block or allow networks or hosts
- you use a host file to implement filtering

Learning Objectives:

a. Install firewall software
b. Implement filtering with HOST file
c. Configure firewall to block or allow protocols
d. Configure firewall to block or allow ports
e. Configure firewall to block or allow programs
f. Configure firewall to block or allow networks/hosts

**Required Artifacts: None**
**Suggested Artifacts: Screenshot of firewall meeting criteria in Competency 2**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 3: Configure network based firewalls**

Criteria: Performance will be satisfactory when:

- you configure basic firewall settings
- you configure static NAT and PAT
- you configure decryption of firewall traffic
- you configure port forwarding
- you configure APP and content ID
- you configure URL filtering
- you configure user ID
- you configure global intelligence
- you configure ingress and egress filtering
- you configure white and black lists
- you configure high availability
- you configure interfaces
- you implement ACLs
- you setup and utilize certificates
- you setup zones, including a DMZ
- you configure setting to meet security policy

Learning Objectives:

a. Configure initial settings
b. Configure security to meet policy
c. Configure dynamic and static NAT and PAT
d. Configure decryption of firewall traffic
e. Configure port forwarding
f. Configure App ID
g. Configure Content ID
h. Configure URL filtering
i. Configure user ID
j. Configure global threat awareness/intelligence
k. Apply Ingress and egress filtering
l. Configure white and black lists
m. Configure high availability
n. Configure interfaces
o. Implement ACLs
p. Utilize certificates
q. Setup zones including DMZ

**Required Artifacts: None**
**Suggested Artifacts: Screenshot of firewall meeting criteria in Competency 3**

**Competency 3: Configure network based firewalls**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 4: Configure site to site VPNs**

Criteria: Performance will be satisfactory when:

- you create a site to site VPN
- you identify VPN protocols
- you identify encryption protocols and keys
- you identify traffic allowed on VPN
- you identify a hairpin VPN
- you test VPN connections

Learning Objectives:

a. Create a site to site VPN
b. Identify VPN protocols
c. Identify encryption protocols and keys
d. Identify traffic allowed on VPN
e. Identify Hairpin VPN
f. Test VPN traffic

**Required Artifacts: None**
**Suggested Artifacts: Screenshot of VPN tunnel settings**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 5: Configure remote access VPNs**

Criteria: Performance will be satisfactory when:

- you setup a remote access VPN
- you identify hairpin in a remote access VPN
- you configure a split tunnel
- you install VPN clients
- you create a SSL portal
- you test the remote access VPN

Learning Objectives:

a. Setup remote access VPN
b. Identify Hairpin Remote VPN
c. Configure split tunnel
d. Install VPN client
e. Create a SSL portal
f. Test remote access VPN

**Required Artifacts: None**
**Suggested Artifacts: Screenshot showing remotely connected client utilizing VPN**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 6: Test firewall implementations**

Criteria: Performance will be satisfactory when:

- you identify software used for security testing
- you test access to firewall zones
- you scan firewalls for open ports/services
- you identify WEB resources for securing firewalls
- you test high availability and failover

Learning Objectives:

a. Identify software for security testing
b. Test access to firewall zones
c. Execute port scans
d. Identify web resources for security scanning
e. Test high availability and failover

**Required Artifacts: None**
**Suggested Artifacts: Output of software used to test firewall**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 7: Monitor and report baselines and threats**

Criteria: Performance will be satisfactory when:

- you monitor devices statics and setting
- you create a threat report
- you identify threat activity
- you configure NTP
- you identify normal traffic
- you create alarms or notification

Learning Objectives:

a. Configure logging settings
b. Monitor device statics and settings
c. Create a threat reports
d. Identify threat activity
e. Configure NTP
f. Identify normal traffic
g. Create alarms or notifications

**Required Artifacts: None**
**Suggested Artifacts: Screenshots demonstrating each criteria in Competency 7**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 8: Maintain firewall software**

Criteria: Performance will be satisfactory when:

- you upgrade firewall software
- you configure threat intelligence updates
- you review firewall settings
- you update geo locations database
- you backup device configurations
- you maintain device licenses
- you document device installations/configuration

Learning Objectives:

a. Upgrade firewall software
b. Configure threat intelligence updates
c. Review firewall settings
d. Update geo location database
e. Backup device configurations
f. Maintain device licenses
g. Document device installation/configuration

**Required Artifacts: None**
**Suggested Artifacts: Screenshot showing automated updates of firewall**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Competency 9: Evaluate protocols and services**

Criteria: Performance will be satisfactory when:

- you identify ports and applications
- you analyze protocol operations
- you identify traffic flows
- you identify the use and functions of protocols

Learning Objectives:

a. Identify protocols in use
b. Identify ports and applications
c. Analyze protocol operations
d. Identify traffic flows

**Required Artifacts: None**
**Suggested Artifacts: None**

**Describe your learning and experience with this competency:**

**Met/ Not Met Evaluator Feedback:**

**Conclusion:** **Summarize how you have met the competencies of the course.**

## Learning Source Table

| **Learning Source**<br>(name of employer, training, military, volunteer organization, etc.) | **Supervisor** | **Start-End Date** | **Total Hours** | **Related Competencies** |
|---|---|---|---|---|
| Ex: XYZ Corporation | Bucky Badger | 8/2012-9/2014 | 2000 | #1, 2, 3, and 7 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |