Next Generation Higher National Unit Specification

Firewall Technology (SCQF level 8)

Unit code: J7E5 48

SCQF level: 8 (16 SCQF credit points)

Valid from: session 2023–24

Prototype unit specification for use in pilot delivery only (version 1.0) June 2023

This unit specification provides detailed information about the unit to ensure consistent and transparent assessment year on year.

This unit specification is for teachers and lecturers and contains all the mandatory information required to deliver and assess the unit.

This edition: June 2023 (version 1.0)

Unit purpose

This unit provides learners with knowledge and understanding of:

- the setup, configuration and management of a next generation firewall
- how a firewall can protect both itself and a network against modern-day threats
- how a firewall provides useful information to administrators on what is happening within their network

This is a specialist unit, aimed at learners with an interest in computer networking or those studying network security. It is particularly suitable for learners who are studying an HND in Networking and Cloud Infrastructure.

Learners do not require any previous firewall configuration skills. However, they should have a basic understanding of networking and network devices, including what a firewall does.

When they complete the unit, learners know what protection and additional features a next generation firewall provides to a network, and how it can be configured to achieve this.

Learners can progress from the unit to more specialised security training, including vendor certifications in firewall technologies.

Unit outcomes

Learners who complete this unit can:

1 configure the initial setup of a next generation firewall
2 configure the operational setup of a next generation firewall
3 configure the security setup of a next generation firewall
4 analyse and interpret information from a firewall

Evidence requirements

Learners must provide both knowledge and product evidence.

The knowledge evidence is the underpinning theory required across all outcomes. Learners must produce the evidence without assistance. It must demonstrate that learners understand all the required knowledge statements.

You can sample the knowledge evidence when testing is used, but you must include at least one item from each knowledge statement. Testing can be multiple choice or short-response questions. Learners must produce evidence under exam conditions in terms of location, timing and access to reference materials.

If a learner needs to be re-assessed, you must use a different set of questions.

The product evidence is practical configurations of network firewalls that includes:

- interface configuration to facilitate traffic flow and internet connectivity
- security rule or policy configuration and testing to limit traffic based on IP-address and port numbers
- security rule or policy configuration and testing to perform deep packet inspection
- security rule or policy configuration and testing to analyse encrypted traffic
- firewall configuration to support backups, application of multiple configurations, admin account management and password policies
- firewall configuration to protect against direct attacks
- firewall configuration to support redundancy and high availability
- production of reports to show allowed traffic and threats encountered

The product evidence can be produced over an extended period of time in lightly-controlled conditions. Give learners access to learning materials. Authentication is required when evidence is produced in lightly-controlled conditions.

The unit's SCQF level provides additional context relating to the quality of evidence for both knowledge and product components.

Knowledge and skills

The following table shows the knowledge and skills covered by the unit outcomes:

Knowledge	Skills
Learners should understand: ♦ the functions of a firewall ♦ the characteristics of next generation firewalls ♦ initial firewall configuration settings ♦ interface architecture settings ♦ security rule or policy configuration ♦ security rule testing ♦ configuration file management ♦ administrator management ♦ firewall security ♦ firewall redundancy ♦ firewall reporting tools ♦ log file analysis	Learners can: ♦ configure a baseline ♦ perform licensing and update management ♦ configure firewall interfaces ♦ configure interface groups or zones ♦ configure wide area network (WAN) connectivity ♦ create security rules or policies ♦ test security rules or policies ♦ perform configuration file backup and restore ♦ manage the application of multiple configurations ♦ create multiple administrator accounts ♦ create string password policies ♦ protect the firewall (and hence, network) from direct attacks ♦ configure a pair of firewalls to provide redundancy ♦ test a redundancy configuration ♦ produce traffic and threat reports ♦ analyse traffic, threat and configuration logs

Meta-skills

Throughout this unit, learners develop meta-skills to enhance their employability in the computing sector.

Self-management

This meta-skill includes:

- focusing: interpreting firewall data
- adapting: critically reviewing actions to acquire insights into improvements
- initiative: displaying independent thinking

Social intelligence

This meta-skill includes:

- communicating: sharing threat information
- feeling: understanding how security hardware vendors use shared threat information to benefit everyone
- collaborating: working in coordination with others to share threat information

Innovation

This meta-skill includes:

- curiosity: staying aware of current threats and their consequences to successfully manage a firewall
- creativity: researching threats and thinking of ways of addressing any problems
- critical thinking: evaluating and drawing conclusions from information to make sure the firewall is configured correctly to mitigate any threats

Delivery of unit

This unit provides learners with an understanding of how to setup, configure and manage a next generation firewall. Although learners should have a basic understanding of networking and network devices, we expect that you include underlying networking concepts in lessons to provide important background information.

We suggest the following distribution of time:

Outcome 1 — Configure the initial setup of a next generation firewall
(10 hours)

Outcome 2 — Configure the operational setup of a next generation firewall
(40 hours)

Outcome 3 — Configure the security setup of a next generation firewall
(20 hours)

Outcome 4 — Analyse and interpret firewall information
(10 hours)

Professional recognition

Although this unit is not geared towards any specific firewall vendor or their examinations, learners could progress to the entry level examinations of any vendor — for example, the Palo Alto Firewall Configuration and Management (EDU-210) exam. See www.paloaltonetworks.com for more information.

Additional guidance

The guidance in this section is not mandatory.

Content and context for this unit

Configure the initial setup of a next generation firewall (outcome 1)

Teach learners how to take an unconfigured firewall and apply sufficient configuration settings to perform initial management tasks, such as licensing and updating to the latest threat prevention levels.

Show learners how to configure firewall interfaces to facilitate secure inter- and intra-network traffic flow and internet connectivity. You should include internal routing and network address translation (NAT) or port address translation (PAT) configuration. You should also cover interface group or zone allocation to simplify security rule or policy.

Configure the operational setup of a next generation firewall (outcome 2)

Demonstrate the different ways modern (next generation) firewalls can filter traffic to protect a network. Show learners how to create and test a range of security rules or policies that filter:

- traffic using transmission control protocol (TCP) and user datagram protocol (UDP) port numbers
- IP-addressing and subnets
- the URL being accessed
- pre-determined lists of known malicious web domains
- web-site classification (such as gambling, adult)
- application programs causing the traffic
- traffic to and from specific network users
- threats contained in encrypted traffic and traffic containing stolen credentials and/or other sensitive data.

Learners should also test the rules they have configured.

Configure the security setup of a next generation firewall (outcome 3)

Show learners how the firewall itself can be kept secure. They should know how to perform configuration file backup and restore. Teach learners how to configure multiple configuration files and apply specific configurations when needed.

Teach learners how to create multiple firewall administrator accounts with differing levels of ability, and why separation of duties is important. Show them how to apply appropriate password policies to these accounts to ensure secure passwords are enforced.

Explain to learners about the common attacks that can be carried out against the firewall and protected network. Teach them how to prevent the firewall (and hence network) from attack.

Teach learners about:

- reconnaissance attacks
- attacks involving non-IP-protocols
- flood attacks
- denial of service (DOS) and distributed denial of service (DDOS) attacks
- malformed packet attacks

Where possible, learners should test these configurations.

Learners should know why firewall redundancy is important in a network and how to configure a pair of firewalls for high availability and for redundancy.

Analyse and interpret firewall information (outcome 4)

Show learners how to use firewall reporting tools to produce a range of reports to a specified set of parameters. Explain how these reports allow network administrators to learn about genuine traffic flows and attacks that have occurred.

Learners should also know what firewall log files are available and how to analyse and report from them. They should be capable of accessing configuration, security and threat logs directly, and interpreting their information. For example, learners should know:

- the significance of multiple unsuccessful password attempts
- security policy violations
- update frequency
- attack detection

Equality and inclusion

This unit is designed to be as fair and as accessible as possible with no unnecessary barriers to learning or assessment.

You should take into account the needs of individual learners when planning learning experiences, selecting assessment methods or considering alternative evidence.

Guidance on assessment arrangements for disabled learners and/or those with additional support needs is available on the assessment arrangements web page: www.sqa.org.uk/assessmentarrangements.

Information for learners

Firewall Technology (SCQF level 8)

This section explains:

- what the unit is about
- what you should know or be able to do before you start
- what you need to do during the unit
- opportunities for further learning and employment

Unit information

This unit provides you with an understanding of how to set up, configure and manage a next generation firewall. Next generation firewalls use a variety of clever ways to protect against both known and unknown threats. You gain knowledge and hands-on experience in how they do this.

This is a specialist unit, intended for individuals with an interest in networking or cyber security. Although no previous firewall knowledge or experience is required and access to the unit is at the discretion of your centre, we recommend that you have a basic familiarity with networking concepts including routing, switching, and IP-addressing.

You are assessed on both your theoretical and practical knowledge of firewalls through a combination of written and practical tasks. When you finish, you can explain and apply the main methods used by security professionals in reducing the risk of attacks using firewalls. You are also able to identify, explain and suggest how networks can be protected against common vulnerabilities.

You have ample opportunity to enhance your self-management, social intelligence, and innovative skills.

When you finish, you can do further study to sit entry vendor certifications such as those provided by Palo Alto, and other vendors — for example, the Palo Alto Firewall Configuration and Management (EDU-210) exam. See www.paloaltonetworks.com for more information.

Administrative information

Published: June 2023 (version 1.0)

Superclass: CB

History of changes

Version	Description of change	Date

Note: please check SQA's website to ensure you are using the most up-to-date version of this document.