Higher National Unit Specification

General information

Unit title: Firewall Essentials (SCQF level 7)

Unit code: J2JW 34

Superclass: CB

Publication date: August 2019

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this unit is to provide learners with an understanding of how to configure and manage next-generation firewalls; to implement protection mechanisms against threats, factors and tools that can be leveraged by malicious hackers to target individuals and organisations. Learners will gain knowledge and hands-on experience in configuring, managing and monitoring a firewall.

This is a **specialist** unit, intended for learners with an interest in computing or computer science; it is particularly suitable for those with a vocational interest in cyber security.

On completion of this unit, learners will be able to explain and apply the main methods used by security professionals in reducing the risk of attacks using firewalls. They will also be able to identify, explain and suggest remediation for common vulnerabilities.

Progression from this unit could be to J0HB 34 *Penetration Testing* to test the effectiveness of the firewall and its configuration.

Outcomes

On successful completion of the unit, the learner will be able to:

1 Configure the essential features of next-generation firewalls.
2 Protect systems located outside of the enterprise perimeter by use of a firewall.
3 Manage firewall availability using redundancy.
4 Monitor network traffic.

Higher National Unit Specification: General information (cont)

Unit title: Firewall Essentials (SCQF level 7)

Credit points and level

2 Higher National unit credits at SCQF level 7: (16 SCQF credit points at SCQF level 7)

Recommended entry to the unit

No previous knowledge or experience is required and access to this unit will be at the discretion of the centre. However, it is recommended that learners have a basic familiarity with networking concepts including routing, switching and IP addressing. It would also be desirable for learners to be familiar with basic security concepts.

Experience with other security technologies (IPS, proxy and content filtering) would be an advantage. This may be evidenced by possession of relevant National Units, such as units from the NPA in Cyber Security or Network Fundamentals; HN Units such as *Network Concepts*; or experience in using networks or firewalls.

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

There is no automatic certification of Core Skills or Core Skill components in this unit.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

This unit could be delivered alongside J0HE 34 *Securing Network Devices*.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

Higher National Unit Specification: Statement of standards

Unit title: Firewall Essentials (SCQF level 7)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Configure the essential features of next-generation firewalls.

Knowledge and/or skills

- Platforms and architecture
- Initial configuration
- Interface configuration
- Security and NAT policies
- Local and remote threats
- Application control
- Content control (IPS)
- URL filtering
- Decryption
- Malware analysis
- User ID mapping

Outcome 2

Protect systems located outside of the enterprise perimeter by use of a firewall.

Knowledge and/or skills

- Protecting mobile devices
- VPN, including site to site VPN

Outcome 3

Manage firewall availability using redundancy.

Knowledge and/or skills

- Factors that influence the availability of a firewall
- Configuration of firewall availability using redundancy
- Management of firewall availability using redundancy
- Active redundancy
- Passive redundancy

Higher National Unit Specification: Statement of standards (cont)

Unit title: Firewall Essentials (SCQF level 7)

Outcome 4

Monitor network traffic.

Knowledge and/or skills

- Monitoring and reporting
- Monitoring via a web interface
- Firewall reports
- Active reporting
- Passive reporting

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms.

1 Knowledge evidence (Outcomes 1, 2, 3 and 4)
2 Product evidence (Outcomes 1, 2, 3 and 4)

The **knowledge evidence** will comprise the underpinning knowledge required in Outcomes 1, 2, 3 and 4. Knowledge evidence is required for all knowledge and/or skills statements. The evidence may be produced over an extended period of time in lightly controlled conditions. The amount of evidence may be the **minimum** required to infer competence. For example, learners need only describe some of the most common platforms that make up firewalls or demonstrate a basic understanding of interface configuration.

The knowledge evidence may be sampled when testing is used. In this case, the evidence must be produced under controlled conditions in terms of location (supervised), timing (limited) and access to reference materials (not permitted). The sampling frame must include the majority of knowledge and skill statements and must always include:

- Initial configuration
- Interface configuration
- Security and NAT policies
- Application control
- Content control (IPS)
- URL filtering
- Decryption
- Protecting mobile devices
- VPN and site to site VPN
- Factors that influence high availability
- Monitoring and reporting

The **product evidence** for Outcomes 1, 2, 3 and 4 will demonstrate that the learner can configure, maintain and monitor **at least one** firewall correctly according to the skills components of each outcome and contemporary requirements. This evidence will be produced over the life of the unit. Evidence must be generated by the learner independently.

Higher National Unit Specification: Statement of standards (cont)

Unit title: Firewall Essentials (SCQF level 7)

The SCQF level of this unit (Level 7) provides additional context on the nature of the required evidence and the associated standards. The following level descriptors are particularly relevant to the evidence:

- An overall appreciation of the body of knowledge
- Knowledge that is embedded in the main theories, concepts and principles
- Apply knowledge and skills in practical contexts
- Use some of the basic and routine professional skills, techniques, practices and materials
- Use a range of approaches to address defined and/or routine problems
- Exercise some initiative and independence in carrying out defined activities at a professional level
- Take account of own and others' roles and responsibilities when carrying out tasks

These level descriptors should be used (explicitly or implicitly) when making judgements about the evidence.

When evidence is produced in uncontrolled or loosely controlled conditions it must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The Guidelines on Approaches to Assessment (see the support notes section of this specification) provides specific examples of instruments of assessment.

The support notes section of this specification provides specific examples of instruments of assessment that will generate the required evidence.

Higher National Unit Support Notes

Unit title: Firewall Essentials (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 80 hours.

Guidance on the content and context for this unit

The aim of this unit is to provide learners with an understanding of how to configure and manage next-generation firewalls. Next generation firewalls have an essence of artificial intelligence and machine learning to help protect against threats, factors and tools that can be leveraged by malicious hackers to target individuals and organisations. During this unit learners will gain knowledge and get hands-on experience configuring, managing and monitoring a firewall.

The firewall used should be a hardware-based firewall, although this may be replicated by use of virtual firewall images.

This unit can be used to prepare learners for the Palo Alto Firewall Essentials: Configuration and Management exam. See **https://www.paloaltonetworks.com/** or **https://www.paloaltonetworks.com/services/education/academy** for more information.

Learners should have a basic familiarity with networking concepts including routing, switching and IP addressing. Learners should also be familiar with basic security concepts. Experience with other security technologies (IPS, proxy, and content filtering) would be an advantage, but is not essential. It is possible that this unit could lead to learners undertaking the penetration testing unit to test the security and robustness of the firewall.

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the educator. It seeks to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

Outcome 1: Configure the essential features of next-generation firewalls.

The first outcome focusses on the different platforms and architecture that make up firewalls; this is to aid in the understanding of how to configure them. Once this is understood, then the focus will move to how to perform the initial configuration of a firewall: passwords, security, etc. Subsequently, learners will gain knowledge and skills in interface configuration, internal and external. Once these two types of configuration are identified, then the security policies can be implemented; this could take the form of preventing threats from applications, via intrusion protection, URL filtering, decryption and malware analysis.

Higher National Unit Support Notes (cont)

Unit title: Firewall Essentials (SCQF level 7)

Although this outcome is intended to be quite practical, there will be a large amount of theory to be covered before the practical work can take place; learners should have acquired an understanding of the types of threats and mitigations before attempting any practical task.

Outcome 2: Protect systems located outside of the enterprise perimeter by use of a firewall.

Outcome 2 looks at protecting devices that are outside of the enterprise, such as mobile devices eg, laptops, tablets and mobile phones that access data. This outcome will also look at configuring a site to site VPN by using two connected firewall devices.

Outcome 3: Manage firewall availability using redundancy.

Outcome 3 looks at ensuring that a firewall is always running. If the firewall is not up and operational, then no data can flow in or out of an enterprise. This outcome explores some factors that influence the availability of a firewall, such as DDoS attacks or failover.

By configuring two firewalls using redundancy, this means that in the event that one fails the other one can take over. This can be achieved by placing two firewalls in a group and synchronising their configuration to prevent a single point of failure on the network.

In active redundancy, a heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down; this is usually utilised on same manufacturer firewalls, usually with a propriety protocol. Passive redundancy normally takes place between two firewalls from differing manufacturers and the process is likely to involve some common protocol instead of a propriety one.

Outcome 4: Monitor network traffic.

Outcome 4 looks at monitoring network traffic and its importance to firewalls. Throughout this outcome, learners will look at the types of monitoring and reporting that can be carried out. Different monitoring reports can be generated, often via a web interface. Some reports are active and serve as warnings, and some are passive and require the firewall to be asked to produce the report.

Guidance on approaches to delivery of this unit

Although sequencing of outcomes is at the discretion of the centre, it is recommended that outcomes are delivered sequentially, as this would follow the logical progression, with the knowledge assessment being carried out prior to the practical.

The required theory would be best delivered prior to practical work being undertaken.

A suggested distribution of time, across the outcomes, is:

Outcome 1: 30 hours
Outcome 2: 20 hours
Outcome 3: 16 hours
Outcome 4: 14 hours

Higher National Unit Support Notes (cont)

Unit title: Firewall Essentials (SCQF level 7)

Summative assessment may be carried out at any time. However, when testing is used (see evidence requirements) it is recommended that this is carried out towards the end of the unit (but with sufficient time for remediation and re-assessment). When continuous assessment is used (such as the use of a web log), this could commence early in the life of the unit and be carried out throughout the duration of the unit.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide assessors with an opportunity to diagnose misconceptions, and intervene to remedy them before progressing to the next outcome.

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

A traditional approach to assessment could satisfy the evidence requirements by using a test and a practical assignment.

Knowledge evidence could be produced using an end-of-unit test. This test would sample from the knowledge and understanding contained in Outcomes 1, 2, 3 and 4. The test could comprise a number of short answer questions and would be marked and assessed traditionally. For example, the test may be made up of 10 questions, requiring a response comprising no more than one or two paragraphs. The questions would be selected across all three outcomes, each worth five marks, with the learner responses marked out of 50 and a pass mark of 30. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across outcomes. This test would be taken, sight-unseen, in controlled and timed conditions, without reference to teaching materials. A suitable duration could be 60 minutes.

The product evidence could be produced using a practical assignment, which would require learners to protect devices using firewalls, manage availability and monitor network traffic, either in one practical task or spread throughout the life of the unit.

A more contemporary approach to assessment could satisfy the evidence requirements by using a web log (blog). This blog would provide knowledge and product evidence by describing the knowledge and skills acquired during the unit. The knowledge evidence would be apparent from the various posts describing and explaining what has been learned; the product evidence could be manifest in the descriptions, images and videos used to record practical activities. In this scenario, sampling would not be appropriate; all of the knowledge and skills would have to be evidenced in the blog.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Higher National Unit Support Notes (cont)

Unit title: Firewall Essentials (SCQF level 7)

Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment, as specified in the evidence requirements, are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

This unit provides opportunities to develop some components of the following Core Skill:

- Information and Communication Technology (ICT) (SCQF level 6)

Several components of the Core Skill in *Information and Communication Technology (ICT)* may be addressed in this unit. There are opportunities to start software, enter and edit data, locate and extract information, apply a complex search strategy and evaluate information.

History of changes to unit

Version	Description of change	Date

General information for learners

Unit title: Firewall Essentials (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

The purpose of this unit is to provide you with an understanding of how to configure and manage next-generation firewalls. Next generation firewalls have an essence of artificial intelligence and machine learning to help protect against threats, factors and tools that can be leveraged by malicious hackers to target individuals and organisations. In this unit, you will gain knowledge and hands-on experience in configuring, managing, and monitoring a firewall.

This is a **specialist** unit, intended for people with an interest in computing or computer science; it is particularly suitable if you have a vocational interest in cyber security.

No previous knowledge or experience is required and access to this unit will be at the discretion of your centre. However, it is recommended that you have a basic familiarity with networking concepts including routing, switching, and IP addressing. It would be desirable if you were familiar with basic security concepts.

Experience with other security technologies (IPS, proxy and content filtering) would be an advantage. This may be evidenced by possession of relevant national units, such as units from the NPA in Cyber Security or Network Fundamentals; HN units such as Network Concepts or experience in using networks or firewalls.

You will be assessed on both your theoretical and practical knowledge of firewalls and on completion of this unit, you will be able to explain and apply the main methods used by security professionals in reducing the risk of attacks using firewalls. You will also be able to identify, explain and suggest remediation for common vulnerabilities.

Throughout this unit you will also have an opportunity to develop some aspects of the Core Skill in *Information and Communication Technology (ICT)*, which will be useful when progressing to further study or employment.

You may wish to progress from this unit to J0HB 34 *Penetration Testing* to test the effectiveness of the firewall and its configuration.